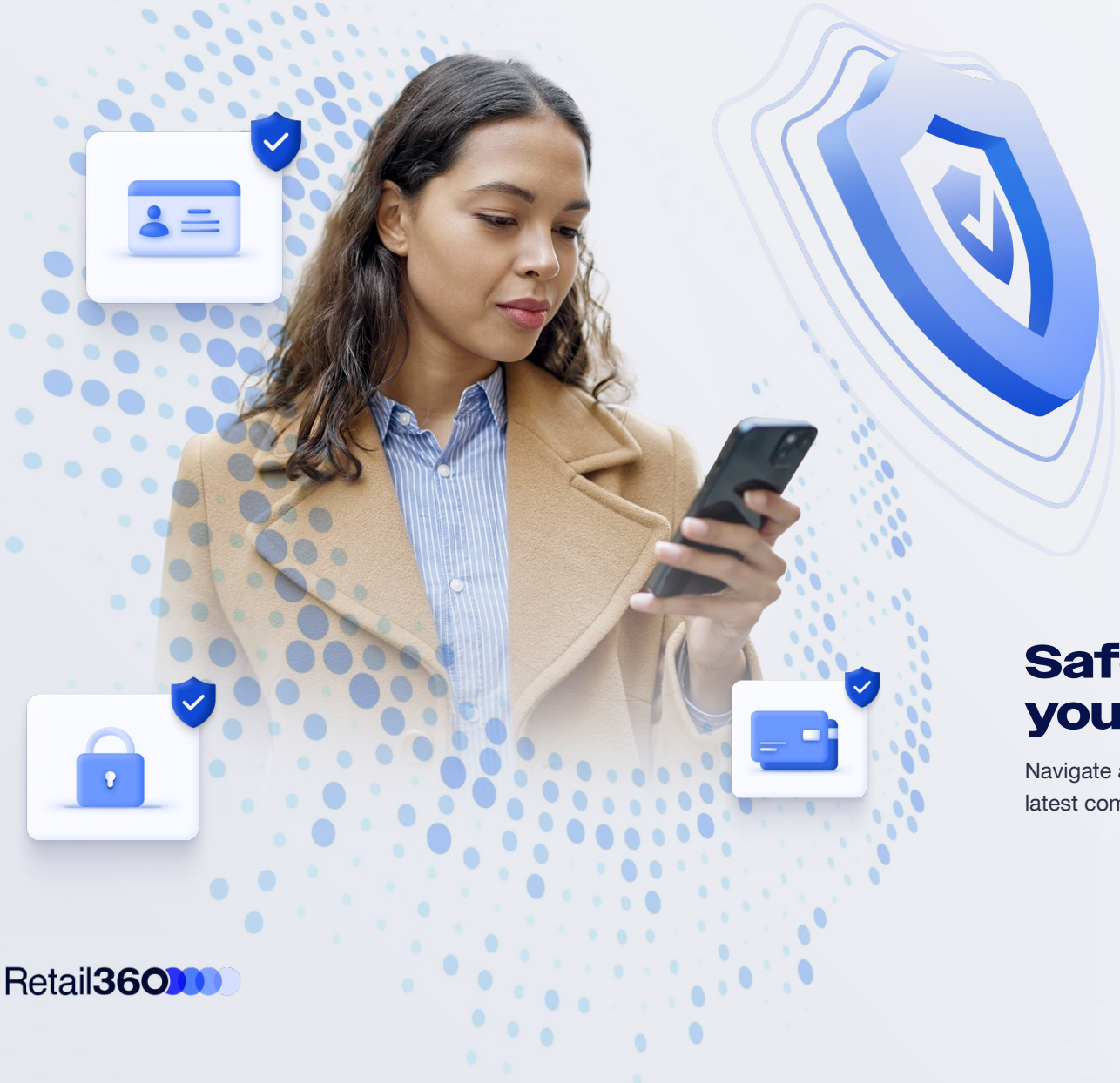
2025
Compliance Guide

Dealertrack
by Cox Automotive



Safeguarding your dealership

Navigate auto regulations and build resilience with the latest compliance insights, best practices and more.

Retail360

Table of Contents

Automotive Compliance in 2025

Gain understanding of your dealership's compliance obligations with the latest updates in consumer protection, data privacy and security regulations.

See what's new for 2025 →

Did You Know?

The FTC finalized its first rule—the Combating Auto Retail Scams (CARS) Rule—against unfair and deceptive practices by auto dealers and lenders, which is set to go into effect in late 2025 unless pending lawsuits or other challenges to the rule succeed.

Compliance Tip

With data and other security breaches on the rise, ensure you are protecting your dealership, employees, and customers from those breaches through appropriate technology and training. See more Compliance Tips

What's New for 2025

The CFPB recently announced plans to increase its monitoring of auto financing practices into 2025, particularly focusing on unwanted add-on products and hidden fees, deceptive advertising, erroneous repossessions, improper loan servicing, and inaccurate reports to credit reporting companies.

Recommended Practice

When establishing or revising your compliance program, review the CFPB's recent Supervisory Highlights for specific examples of auto dealer practices discouraged by regulators.

Breakout Sections

Compliance and your dealership in 2025

The auto industry remains stable but faces major market shifts heading into 2025. Consumer demand for cars is growing, but consumer preferences for cars are changing. For example, in the next year, more electric and hybrid cars are expected to be sold, and more car sales are anticipated to occur online instead of at dealerships. The auto finance landscape is also changing. Consumers place price as the most important factor in their car buying decisions, but car prices are still higher than average. To make up for these higher prices, auto dealers may increase incentives in 2025, particularly in financing, to entice consumers to commit to a car purchase.

Federal and state regulators will be monitoring changing auto finance practices, in particular, in 2025 to ensure consumers are being treated fairly. One of the primary federal regulators of the auto industry, the Consumer Financial Protection Bureau (CFPB), issued a report in late 2024 finding that auto loan debt currently exceeds all other consumer debt categories aside from home mortgages. As a result, the CFPB confirmed its intent to monitor auto finance practices for unwanted add-on products (e.g., payment insurance and paint protection), inconsistent contract language, improper repossessions, inaccurate reporting to credit companies, and more.

Another federal regulator, the Federal Trade Commission (FTC), has also committed to increased regulation and enforcement against unfair and deceptive practices by auto dealers in 2025. For example, the FTC finalized a new rule penalizing bait-and-switch tactics, hidden charges, and related practices by auto dealers that is slated to go into effect in September 2025 (see Topic 6). In the interim, the FTC continues to partner with state governments to bring enforcement actions against unfair and deceptive practices, resulting in costly fines and reputational harm for accused auto dealers and their owners and employees.

Moving forward, auto dealers must prioritize compliance to protect consumers from unfair and deceptive practices and to protect themselves from debilitating fines, negative press, and the administrative burdens of regulatory actions. A robust compliance program should include, among other things, appropriate resource allocation, training, monitoring, assessments, updates, oversight, and disciplinary measures. As part of their compliance efforts, auto dealers should review enforcement actions, reports, and updates issued by federal and state regulators that may address unlawful and discouraged practices, whether under new or longstanding regulatory interpretations.

When establishing or improving compliance programs in 2025, dealers must also focus on privacy and data security obligations.

Compliance Tip

Dealers must focus on privacy and data security obligations when establishing or improving compliance programs in 2025.

Federal and state regulators continue to emphasize compliance in this area. For example, at least twenty states—California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia—have enacted new data privacy and security laws, with several other states considering legislation to do the same. Topics 2 and 5 provide a detailed overview of these state laws.

Following from this regulatory outlook for 2025, the rest of Topic 1 addresses the federal and state regulatory regimes most applicable to the auto industry. Topic 1 also covers recent reports and enforcement actions issued by those regulators against auto dealers, lenders, and others for unfair and deceptive practices toward consumers. Auto dealers should consider this regulatory information when establishing and improving their compliance programs.

Consumer Financial Protection Bureau (CFPB)

The CFPB is an independent federal agency established by the Dodd-Frank Act to centralize enforcement and supervision of longstanding federal consumer financial laws and regulations, exercise authority to prohibit unfair, deceptive, or abusive practices (UDAP), and issue new regulations as it deems necessary. Auto dealers that sell or lease and service vehicles that also sell their retail installment sales contracts

to non-affiliated third parties are generally not subject to the CFPB's direct supervisory, rulemaking, or enforcement authority. Buy-here-pay-here and certain independent dealers that do not fit into the exception are subject to direct CFPB regulation. Like the federal bank regulators, the CFPB can refer a matter to the Department of Justice (DOJ) when it has reason to believe that a creditor has engaged in certain legal violations, such as a pattern or practice of lending discrimination. In some matters, it can enforce the law through its own administrative process. Recent examples of the CFPB's enforcement actions are provided in the "Recent Federal Enforcement Actions" section of this Topic.

Larger Participant Rule and Auto Leases

In 2015, the CFPB used its authority under the Dodd-Frank Act to promulgate a rule giving itself jurisdiction over nonbank "larger participants" in the auto finance space (Larger Participant Rule). Franchised auto dealers that routinely sell the retail installment sales contracts they originate to unrelated third-party finance sources are excluded from the CFPB's direct supervisory, rulemaking, and enforcement authority. However, other dealers are not as fortunate. For example, buy-here-pay-here dealers that do not sell their contracts to an unaffiliated third party are subject to CFPB oversight, as are certain independent used car dealers that do not meet the requirements for exclusion. Dealers should consider seeking advice of counsel to determine whether they are subject to CFPB jurisdiction.

One further enhancement under the Larger Participant Rule is that the CFPB has claimed jurisdiction over consumer auto leasing. Formerly, the CFPB's authority was limited to retail finance and direct loans, but the Rule clarified that traditional auto leasing is also within the CFPB's jurisdiction.

For nearly a decade, the Larger Participant Rule has provided the CFPB visibility into the practices of auto dealers. The expansion of the CFPB's jurisdiction over indirect auto finance unquestionably impacts how dealers should protect themselves from regulators with which the CFPB may be sharing information from its finance source examinations and investigations. Because of this sharing, dealers should consider the CFPB's focus on transparency and fairness to consumers in all aspects of credit transactions.

Indirect Auto Finance Guidance

In 2015, the CFPB increased its activity to enforce federal consumer credit protection laws in the area of indirect auto finance by furthering attempts to indirectly regulate auto dealers. While certain auto dealers are not subject to the direct supervisory, enforcement, or rulemaking authority of the CFPB, the CFPB sought to indirectly regulate those dealers' auto finance practices in its March 2013 Indirect Auto Finance Guidance (Guidance). The Guidance found that dealer finance participation, which the CFPB refers to as "markups," frequently discriminates against protected classes of persons under the Equal Credit Opportunity Act (ECOA), most notably minorities and women, and that finance sources that buy such paper (and who are within the CFPB's jurisdiction) can be liable for the resulting credit discrimination under a "disparate impact" theory. Disparate impact occurs when a facially neutral policy, such as a dealer marking up a "buy rate," results in a statistically significant disparity in the treatment of protected classes of persons under the ECOA when compared to those not in protected classes.

There were many questions in the industry about the legitimacy of the Guidance, starting with the CFPB's theory of credit discrimination, i.e., the "disparate impact" theory. The ECOA undoubtedly prohibits "disparate treatment," i.e., policies or practices that on their face treat protected classes less favorably than non-protected classes. But there is some question as to whether the ECOA makes "disparate impact" discrimination actionable, despite the fact that the Guidance assumes it is. Under the language of ECOA, lenders are clearly liable for their own intentional conduct. In addition, a lender can be responsible for the intentional conduct of another creditor when it knows or has reason to know of a violation. But in the Guidance, the CFPB asserted that indirect auto lenders that permit dealer participation may be liable if such compensation practices unintentionally result in disparities on a prohibited basis in their dealer-by-dealer individual portfolios and/or their aggregate portfolio.

The ECOA does not expressly prohibit credit discrimination under the "disparate impact" theory. That theory is actually derived from employment discrimination laws and works as follows:

- A creditor employs a facially neutral credit practice (e.g., a minimum income requirement);
- Application of the practice has a disproportionately negative effect on a protected class (in this example, this could be women who do not make incomes as high as men);
- If true, the creditor must show the practice meets, in a significant way, the legitimate goals of the business;
- If the creditor can so show, the burden then shifts to the regulator or plaintiff to show that the business goals can be met by means that are less discriminatory in their impact (e.g., substituting debt-to-income ratio for a minimum income requirement); there is no requirement to show knowledge or intent to discriminate by the creditor in a "disparate impact" case.

Finally, the CFPB asserted that dealer participation often has a disparate impact on women and minorities. Since an indirect auto creditor cannot collect demographic information on customers in auto finance transactions like a mortgage lender can in a mortgage transaction, the CFPB uses "proxies" to try to determine who among similarly qualified customers are in a protected class and who are not. Proxies are ways to try to guess who is in a protected class based on names and geography. The CFPB and DOJ use a proxy methodology called the Bayesian Improved Surname Geocoding (BISG) proxy, which has been heavily criticized by statisticians as overstating minorities and understating non-minorities, a conclusion the CFPB subsequently confirmed.

The BISG proxy only identifies probabilities and can also overstate disparities and the amount of alleged harm by failing to take into account non-discriminatory factors such as geography, new versus used car financing, length of loan, down payment, trade-in vehicle, credit score, and competitive factors such as meeting or beating a competing offer.

Despite these issues, many finance sources have followed the CFPB's direction to analyze, monitor, and take action against dealers whose rate participation on similarly situated customers differs, including the use of "proxies" to identify members of protected classes and compare dealer finance participation for protected classes as opposed to other customers.

The Guidance never had the force of law but illustrated the CFPB's approach, i.e., that finance sources must effectively monitor and police for discriminatory dealer rate participation on purchased contracts or alternatively compensate dealers through flat-fee pricing instead of dealer rate participation. After a wave of consent decrees enforcing the Guidance, many large finance sources sought to comply with the Guidance by requiring dealers to implement ECOA/Fair Lending policies. They also monitored buy rate participation on retail installment sales contracts of similarly qualified persons that could indicate a "disparate impact," and provided redress to impacted consumers. Most of the consent decrees also required the lenders to limit the dealer participation to specific caps if they continued to permit this form of dealer participation. Most of these consent decrees have expired.

Not surprisingly, the Guidance was very unpopular with auto finance companies and dealers. In 2017, the Government Accountability Office (GAO) accepted a request to determine whether the Guidance is a "rule" subject to disapproval under the Congressional Review Act (CRA). Under the CRA, prior to a rule becoming effective, the proposed rule must be submitted to GAO and Congress for approval. Thus, a finding that the Guidance was a "rule" under the CRA would have meant that the Guidance was ineffective because it was never submitted to GAO and Congress as required by the CRA. GAO studied this issue with the Guidance and found that it qualified as a "rule" under the CRA that had not undergone proper approvals. As a result, in Spring 2018, Congress formally repealed the Guidance.

What does all of this mean for auto dealers? Prior to 2018, this meant that your participation ability may have been limited by your lenders. However, as a result of the invalidation of the Guidance, the expiration of many of the consent decree limitations, and the CFPB's internal review of its fair

Table of Contents

lending authority, federal focus on fair lending appears to have waned for the moment, potentially allowing dealers to increase participation in lending. The CFPB continues to investigate and bring enforcement actions against discriminatory lending practices, though, and states may be bringing enhanced scrutiny to fair lending in their own examination processes.

CFPB Supervisory Highlights

The CFPB is investigating auto sales and auto lending for possible unfair, deceptive, or abusive acts and practices (UDAP) that could violate the Dodd-Frank Act and also result in finance source liability for dealer activity.

Did You Know?

The CFPB is watching how auto finance companies respond to add-on product cancellation requests for possible unfair, deceptive, or abusive acts and practices (UDAP) that could result in dealer liability.

The CFPB issued Supervisory Highlights in 2024 noting that the agency is cracking down on junk fees, which include unnecessary, unavoidable, or surprise charges that inflate costs while adding minimal value (e.g., unnecessary certification or inspection fees, service charges, convenience fees, charges for "nitrogen-filled" tires, etc.). The Supervisory Highlights also indicate that CFPB is targeting deceptive advertising, incorrect credit reporting, and improper repossessions that harm consumers. Dealers are encouraged to review the CFPB's full analysis in its Fall 2024 Supervisory Highlights Special Edition on Auto Finance: https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights-special-ed-auto-finance_2024-10.pdf. A summary of each issue covered in the Supervisory Highlights is below.

- *Misleading Origination Disclosures*. Examiners found that auto loan originators advertised marketing rates "as low as" specified APR rates to consumers who had no reasonable chance of qualifying for or being offered rates at or near that level. Examiners also found that auto loan originators' disclosures did not accurately reflect the terms of loan prepayment penalties.
- *Erroneous Repossession Activities*. Examiners found that auto loan servicers repossessed a consumer's vehicle even though the consumer made payments or obtained extensions to prevent repossession, or the consumer requested a COVID-19 related loan deferment or modification and had otherwise made timely payments. Examiners also found that servicers failed to record a valid lien on a vehicle prior to repossessing it.
- *Unlawful Servicing Practices*. Examiners found that auto loan servicers forced consumers to pay late fees by applying their auto loan payments to post-maturity loans in a different order than the order disclosed on the servicers' websites. Examiners also found that servicers failed to timely deliver vehicle titles to consumers after the consumers paid off loans or leases for the vehicle or after consumers requested the title to transfer vehicle registrations to a different state.
- *Unnecessary Add-On Products*. Examiners found that auto finance companies charged consumers for add-ons that the consumers did not agree to purchase (e.g., extended service contract, vehicle protection product, optional GAP waiver product, etc.), financed add-ons that were void because of vehicles' salvage titles, failed to identify the payees for add-ons purchased by consumers, required consumers to visit dealerships in person on multiple occasions to cancel contracts for add-ons, refused to honor consumers' contractual rights to cancel contracts for add-ons, failed to refund unearned premiums to consumers on early termination of loans, refunded incorrect amounts to consumers on early termination of loans, delayed refunds of unearned premiums to consumers, and collected loan payments from consumers who are covered by a GAP waiver that would cover the outstanding balance and then failed to reimburse those excess payments to consumers.
- *Deficient Credit Reporting*. Examiners found that auto loan furnishers reported information to credit reporting companies while knowing or having reasonable cause to believe that the information was inaccurate, failed to provide a clear and conspicuous address to consumers for notices relating to inaccurate information, and continued to furnish information after determining that the information was incomplete or inaccurate.

Table of Contents

The CFPB's Supervisory Highlights from Summer 2024 identified other unfair and deceptive practices in the auto lending space. Dealers should review the CFPB's analysis in this edition: https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-34_2024-07.pdf. A summary of each issue covered is below.

- *Improper Late Fees*. Examiners found that auto loan servicers failed to automatically debit final loan payments to consumers enrolled in automatic loan payments and neglected to provide consumers adequate notice that their final loan payments were required to be made manually rather than automatically. The CFPB required the servicers to revise "their policies and procedures to ensure that they either include the final payment in autopay withdrawals or adequately notify consumers enrolled in autopay if and when a payment is required to be submitted manually."

The CFPB's Supervisory Highlights from Spring 2024 emphasized the importance of providing accurate information to credit reporting companies. Dealers should review the CFPB's analysis in this edition, as well: https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-32_2024-04.pdf. A summary of each issue covered is below.

- *Uncorrected Information*. Examiners identified auto loan furnishers that failed to promptly correct consumers' information provided to credit reporting companies after finding out that such information was incomplete or inaccurate.
- *Uninvestigated Disputes*. The CFPB found that auto loan furnishers neglected to investigate direct disputes that did not satisfy the furnishers' additional identity verification requirements that were not required by law.
- *Inaccurate Delinquencies*. Examiners observed that auto loan furnishers reported inaccurate dates of first delinquency on applicable accounts because of coding errors.
- *Incorrect Identity Theft Reports*. The CFPB found that auto loan furnishers received identity theft reports from consumers at qualifying addresses but continued to furnish information identified in the report before knowing or being informed by consumers that the information was correct.

The CFPB's focus on auto sales, auto lending, and add-on products is not new. In its Supervisory Highlights prior to 2024, the CFPB identified instances in which auto lenders overcharged various fees, failed to refund unearned add-on product fees, double-billed consumers for collateral protection insurance (CPI) charges, misrepresented the status of requested auto loan modifications, activated starter interruption devices in vehicles when consumers were not in default, made deceptive representations during collection calls, repossessed vehicles after consumers took action that should have prevented the repossessions, and misrepresented the estimated balance of deferred loan payments, among other issues. In light of the CFPB's consistent focus on issues arising from auto lending, auto dealers should review their auto financing practices to ensure they are both accurate under financing agreement terms and authorized under applicable law.

Federal Trade Commission (FTC)

The FTC is an independent federal agency established by the Federal Trade Commission Act (FTC Act) to centralize enforcement and supervision of civil antitrust and consumer protection laws. Like the CFPB, the FTC has long investigated UDAP complaints, issued regulations in response to civil law violations, and referred criminal penalties to the DOJ.

Since 2012, the FTC has brought many deceptive advertising enforcement actions against dealers using its authority to prohibit UDAP. For example, in 2018, the FTC focused on bogus recall notices issued by dealerships. The notices warned consumers about supposedly urgent recalls with prominent language, but the FTC alleged that the dealers made no effort to limit the mailing list to consumers whose vehicles were subject to open recalls.

In another instance, the FTC initiated an action against auto dealers for falsifying consumer income information on financing applications. Specifically, the FTC alleged that the dealers inflated the consumers' financial information, prevented the consumers from reviewing the information, signed financing documents without the consumers' knowledge, used deceptive advertising that confused consumers about the financing or leasing terms,

Table of Contents

and violated the Truth in Lending Act (TILA) by failing to disclose required terms. The FTC also named the dealership owner in his individual capacity on grounds that he directed the illegal activity. The case resulted in payment by the auto dealers of more than $415,000 to the FTC and was significant in that it was the first of its kind to be brought by the FTC against auto dealers.

In May 2020, the FTC filed a complaint in New York against an auto dealer and its general manager, citing violations of the FTC Act, TILA, and ECOA. The FTC alleged that the dealer and manager engaged in unlawfully misleading and deceptive practices and discriminated against Black and Hispanic car buyers by targeting them with higher financing markup rates. In September 2020, the FTC ordered the dealer to pay $1.5 million to settle the charges. This result serves as an important reminder of enforcement actions for both federal consumer protection laws and for discriminatory practices.

Through the years, in addition to marketing, the FTC has focused on so-called "yo-yo" financing (i.e., "spot delivery") where customers were allegedly offered one finance deal in order to effectuate the purchase transaction, and then coerced into another less favorable deal after they signed their contracts. In addition, the FTC has also concentrated on dealers that allegedly "packed" unauthorized charges for aftermarket products and services into financed transactions. **Remember that the FTC does not need an actual complaint against a dealer before it can bring an action.**

Did You Know?

The FTC does not need an actual complaint against a dealer to bring an action. The FTC only needs to allege that an advertisement or practice "is likely to mislead" or that a practice is "likely to cause substantial injury" to consumers.

The FTC only needs to allege that an advertisement or practice "is likely to mislead" or that a practice is "likely to cause substantial injury" to consumers to satisfy the required legal elements of a UDAP claim.

These actions demonstrate that, as the primary federal regulator for most auto dealers, the FTC is serious about using its investigatory authority to prevent UDAP. The FTC is also authorized under the Dodd-Frank Act to promulgate rules implementing its UDAP authority as it relates to dealer activities. Based on this authority, the FTC recently finalized its CARS rule, which is set to become effective in September 2025. The CARS Rule targets bait-and-switch tactics, deceptive pricing, junk fees, hidden charges, and other conduct the FTC views as UDAP. The rule faces legal challenges, however, including a petition filed in January 2024 by the National Automobile Dealers Association and Texas Automobile Dealers Association against the FTC in the Fifth Circuit Court of Appeals alleging that the CARS Rule is arbitrary and capricious. *Nat'l Auto. Dealers Ass'n v. FTC*, Case No. 24-60013 (5th Cir. 2024). The Fifth Circuit held oral argument on the petition in October 2024 and is expected to issue its ruling in 2025, which may be appealed to the United States Supreme Court.

Also, unlike the CFPB, the FTC has issued guidelines on a variety of marketing topics, including online marketing disclosures. Guidance can also be gleaned from the FTC's enforcement actions against auto dealers and lenders. Recent examples of the FTC's enforcement actions are provided in the "Recent Federal Enforcement Actions" section of this guide.

Recent Federal Enforcement Actions

Individual enforcement actions also demonstrate federal regulators' focus on auto sales and auto lending. In the last decade, the CFPB and FTC have brought over 50 auto-related enforcement actions concerning, among other things, vehicle advertising, deceptive pricing, credit reporting, "yo-yo" financing, bait-and-switch tactics, add-on products, discrimination, and privacy and data security issues. Here are six recent examples:

- In August 2024, the FTC sued an auto dealer group and its general manager for systematic junk fee practices. The FTC alleged that the dealers and manager had been using numerous tactics to charge consumers for add-ons that they had not agreed to purchase or that they had been falsely told were required to purchase a vehicle. One such alleged tactic was "payment packing," which is a practice that

Table of Contents

involves getting a consumer to agree to monthly payments that were larger than needed to pay for the vehicle and then "packing" add-ons to the vehicle sales contract to hide the difference from the consumer.

- In August 2024, an auto dealer group and its general manager agreed to pay $2.6 million to settle a lawsuit brought by the FTC and the State of Arizona alleging deceptive pricing and discriminatory practices. The dealers allegedly advertised low prices for vehicles online and then informed consumers who visited the dealership that the advertised prices were not available. If a consumer decided to purchase a vehicle, the dealers allegedly required the consumer to also purchase unwanted add-ons, including products already installed on the vehicle. The dealers also allegedly charged Latino consumers nearly $1,200 more in interest and add-on charges than non-Latino consumers.
- In July 2024, a former online used car dealer agreed to pay $1 million to settle a lawsuit brought by the FTC. The lawsuit alleged that the online dealer failed to display warranty information near the cars posted on its website, omitted a Buyer's Guide from display on the cars, deprived customers of the option to cancel their car purchases and receive refunds, delayed delivery of purchased cars beyond an advertised delivery timeframe, and advertised that the cars had passed "multiple inspections" when they had not. In its settlement, the FTC required that the online dealer cease its deceptive advertising, document all claims about its promised shipping times, and follow all other applicable regulations the dealer was alleged to have violated.
- In January 2024, the FTC and the State of Connecticut sued an auto dealer, its owner, and several employees for deceiving consumers about prices of certified used cars, add-ons, and government fees. The dealers allegedly lured consumers to the dealership with low advertised prices that the dealers did not honor, charged consumers exorbitant fees to certify vehicles already advertised as certified, failed to actually certify the vehicles, and charged consumers for add-ons they did not know about or they were told were required to purchase a vehicle. The FTC and the State of Connecticut brought 17 counts in their complaint against the dealers, owner, and employee as a result, seeking various penalties, attorney's fees, costs.
- In October 2023, an auto dealer group and its general manager paid the FTC $1.1 million and agreed to dissolve their corporate owner entities to settle allegations regarding junk fees and discriminatory practices. The dealers allegedly charged junk add-on fees to approximately half of its customers through deception or without authorization. For example, the FTC claimed that the dealers misled consumers into purchasing GAP insurance as a required add-on even though it was optional, costing consumers increased fees and interest. The dealers also allegedly charged unwanted add-ons and larger interest rate markups to American Indian consumers at a higher rate than non-Latino white consumers.
- In August 2023, the CFPB sued an auto loan servicer for various illegal practices. Those practices included disabling cars when consumers were not in default or were in communication with the servicer about payments, failing to refund GAP insurance premiums when consumers paid off their loans early or their cars were repossessed, double-billing consumers for collateral-protection coverage, misapplying extra loan payments from consumers, and repossessing vehicles from consumers who did not qualify for repossession or had taken action to stop repossession. The CFPB sought to recover millions of dollars in compensation to consumers as well as civil penalty fines.
- In January 2023, the CFPB sued an auto lender for predatory lending schemes. The CFPB alleged that the company had misrepresented the cost of credit to defraud consumers into entering high-cost loans on used cars. Although the company complied with interest rate caps, it allegedly inflated principal balances based on consumers' projected performance under their credit agreements, sending numerous consumers into default. The company further allegedly incentivized auto dealers to mislead consumers into purchasing optional add-on products to the loans, such as vehicle service contracts, by making consumers believe the add-ons were required. The CFPB sought a civil penalty fine of $1 million per day that the lender engaged in certain illegal conduct, among other fines and damages.

Table of Contents

Transparency and consistency in advertising vehicle prices, providing consumer financing, selling add-on products and services, servicing and modifying loans, collecting debts, providing consumer disclosures, and related activities should remain a priority for 2025 and beyond.

State Attorneys General

Although federal law addresses most consumer financial services topics, states are also active in regulation. Under the doctrine of "preemption," certain federal laws, including the Federal Arbitration Act, TILA, ECOA, and FCRA will preempt and override inconsistent state laws on the same subject. However, states that have laws that are not covered by federal law, or are more restrictive than their federal counterpart, are not subject to preemption and will be enforceable by the states.

The CFPB has previously encouraged states to take the lead in enforcing consumer finance laws in the auto industry. As demonstrated by recent enforcement actions, the CFPB and FTC have coordinated with states to investigate and file lawsuits against auto dealers engaging in UDAP. Dealers should continue to monitor enforcement actions affecting the auto industry that their respective state attorneys general have recently taken. For example, in August 2024, the Arizona Attorney General collaborated with the FTC to obtain $2.6 million from an auto dealer group and its general manager for advertising deceptive vehicle prices, charging junk fees without consumers' consent, misrepresenting add-ons as required instead of optional, and discriminating against Latino customers through financing practices.

Environmental Protection Agency

The U.S. Environmental Protection Agency (EPA) continues to play an impactful role in reducing emissions, which affects the auto industry. Part of the EPA's role involves bringing legal actions against auto dealers that violate EPA regulations and related laws. For example, in August 2024, an auto dealer agreed to pay nearly $40,000 in fines to the EPA for violating the Clean Air Act by installing illegal aftermarket exhaust system modifications on vehicles to avoid having to make more complicated sensor repairs. Auto manufacturers are at risk of even heftier fines. For example, in July 2024, a multinational auto manufacturer agreed to pay nearly $146 million in fines to federal regulators after the EPA found its carbon dioxide emissions were higher than the manufacturer had stated in compliance reports.

Other Guidance

Like other companies, dealers must refrain from discriminating against the LGBTIQA+ community. In March 2021, the CFPB issued an interpretive rule clarifying that the prohibition against sex discrimination under the ECOA and Regulation B includes sexual orientation discrimination and gender identity discrimination. This prohibition also covers discrimination based on actual or perceived nonconformity with traditional sex or gender-based stereotypes, as well as discrimination based on an applicant's social or other associations.

Additional Resources

CFPB, Our Auto Finance Data Pilot (February 2023)
https://www.consumerfinance.gov/about-us/blog/our-auto-finance-data-pilot/

CFPB, Automobile Finance Examination Procedures (August 2019)
https://files.consumerfinance.gov/f/documents/201908_cfpb_automobile-finance-examination-procedures.pdf

CFPB, Supervisory Highlights
https://www.consumerfinance.gov/compliance/supervisory-highlights/

FTC, Rulemaking: Unfair or Deceptive Fees
https://www.ftc.gov/legal-library/browse/rules/rulemaking-unfair-or-deceptive-fees

FTC, The Auto Marketplace
https://www.ftc.gov/news-events/topics/consumer-finance/auto-marketplace

DOJ, Evaluation of Corporate Compliance Programs (September 2024)
https://www.justice.gov/criminal-fraud/page/file/937501/download

Table of Contents

Preparing Your 2025 Compliance Action Plan

Protect your dealership and customers by developing policies, procedures and ongoing monitoring for environmental issues, data breach incidents, and other potential threats to your dealership.

Safeguarding dealership and customer data →

Did You Know?

Twenty states have now enacted comprehensive consumer data privacy and security of consumer data laws, many of which go into effect in 2025. Auto dealers should review state laws to ensure consumer data is protected throughout the entire sales transaction process, beginning with the initial customer inquiry and continuing through data collection, processing, and storage.

Compliance Tip

Use the IRS's Energy Credits Online portal to determine whether a consumer is eligible to apply a Clean Vehicle Credit to their electric or hybrid vehicle purchase. Check out more Compliance Tips

What's New for 2025

Be prepared to comply with the FTC's new notification requirements under its amended Safeguards Rule if your dealership experiences a qualifying data breach or other security incident.

Recommended Practice

Stay updated on changes to environmental regulations for air, water, and land pollution to help your dealership avoid potential liability. See more Recommended Practices

Breakout Sections

Looking Ahead: What's Next for Auto Dealers

On the enforcement front, the presidential administration and its philosophy on regulation will likely continue to have a strong impact on the CFPB's and FTC's investigations of consumer-facing companies. The Biden administration had put in place a more aggressive CFPB leadership and several of the changes under the preceding Trump administration had been voided. Where the auto industry is concerned, the CFPB, FTC, and state regulators will likely continue to investigate auto dealerships to identify deceptive and unfair sales and financing practices related to, among other things, add-on products, spot delivery, recall notices, interruption devices, repossessions, and payment packing. **In the last few years, regulators have charged not just the dealership, but also its owners and employees when misconduct amounts to illegal business practices. This includes failing to disclose the history of pre-owned vehicles, falsifying loan documents, and misleading consumers into paying junk fees as a condition of a sales transaction.**

Did You Know?

Regulators can not only charge the dealership but even owners and employees, for misconduct and discriminatory conduct.

The FTC will likely maintain its interest in auto dealer activities, initiating new investigations and entering into consent orders with dealers currently under investigation.

On the regulatory front, dealers should be aware of new proposed and finalized rules from the FTC and CFPB, as well as new state laws governing junk fees and data privacy.

- **In May 2024, the FTC's amendments to the Safeguards Rule went into effect to require non-bank "financial institutions" to follow certain notification procedures to report to the FTC any event in which unencrypted customer information involving 500 or more consumers is acquired without authorization.**

Compliance Tip:

In the event your dealership experiences a data breach or other security incident, be prepared to follow any obligations you may have to notify the FTC.

The Safeguards Rule was finalized in 2023 and amended to include these provisions in 2024 in response to growing incidents of data breaches and other security incidents. As described more in Topic 4, given the broad definition of "financial institution," auto dealers should work with their counsel to identify obligations that may be relevant to them.

- In May 2024, the CFPB finalized its Registry of Nonbank Covered Persons Rule, which scrutinizes consumer financial products provided by nonbanks for risks to consumers. The Rule requires such nonbank entities to register annually with the CFPB regarding their use of certain terms and conditions in form contracts for consumer financial products and services. The finalized Rule, however, excludes from its application "a motor vehicle dealer that is predominantly engaged in the sale and servicing of motor vehicles, the leasing and servicing of motor vehicles, or both" and that "routinely" assigns any retail credit or leases to an "unaffiliated third-party finance or leasing source." Auto dealers should consult with their counsel to determine whether they are subject to the CFPB's annual reporting requirements.
- The CFPB is proposing an Open Banking Rule, which would require any entity that "controls or possesses covered data concerning a covered consumer financial product or service" and that has a "consumer interface" to provide consumers access to nonconfidential data about the financial product or service they are using in a machine-readable format. While the Rule is primarily aimed at banks, its terms are worded broadly enough that they could arguably apply to auto lenders who provide financial products or services to consumers and use a digital platform to interact with those consumers. The CFPB plans to review comments and issue a final Rule by the end of 2024.

- In July 2024, California's new law banning junk fees went into effect. The law requires all "mandatory fees or charges" to be included in a price when a business is "advertising, displaying, or offering a price" for a product or service. The law does not further define those terms. The law does provide, however, that auto dealers may exclude certain costs from advertised, displayed, or offered prices for vehicles, including "a tax, a vehicle registration fee, the California tire fee, an emission testing charge not exceeding $50, an actual fee charged for a certificate, a finance charge, or a dealer document processing charge or charge to electronically register or transfer the vehicle."
- In May 2024, Minnesota passed a law to ban junk fees, which will become effective on January 1, 2025. The law requires "all mandatory fees or surcharges" to be included in a price when a business "advertises, displays, or offers a price" for a product or service. The term "mandatory fee" is broadly defined as including a fee that is required for a purchase, not "reasonably avoidable" by a consumer, or that a "reasonable person" would expect to be included in the purchase price. Excluded from application of the law are any "fees authorized by law related to the purchase or lease of a motor vehicle that are charged by a motor vehicle dealer."
- **Twenty states—California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia—have enacted comprehensive data privacy and security laws.**

Did You Know?

Twenty states have enacted their own comprehensive data privacy and security laws. Be sure to review the laws of the states in which you do business to stay compliant.

Several other states are considering legislation to enact similar laws. Many of these laws become effective in 2025. Dealers should be proactive and incorporate into their 2025 compliance action plan the new state law requirements described in more detail below.

In sum, auto dealers should continue to monitor actions and consent orders involving other dealers (or analogous industries) to determine what particular conduct is disfavored by the CFPB, FTC, and state authorities. At minimum, it is clear that robust compliance policies alone are not enough. Dealers must implement, monitor, and enforce such policies. Moreover, obtaining consumer consent is often more than just obtaining a signature. Dealers must educate the consumer early in the sales process so that the consumer fully understands the product and any accompanying financing. To lessen regulatory risk, dealers can remove pre-checked boxes, avoid confusing or inconspicuous disclosures, eliminate hidden fees, and disclose any add-on products at the outset. This is explored further in Topic 7.

Policies and Procedures

As stated in Topic 12, auto dealers should implement and maintain current written policies and procedures, as well as effective systems and controls, to ensure its consumer financial product programs comply with federal consumer financial laws. To that end, **a compliance management system should be updated on an as-needed basis to address any changes in applicable law.**

Recommended Practice

Update your compliance management system as needed to address any changes in applicable law.

For guidance, the CFPB has released a comprehensive Supervision and Examination Manual and several additional guidance documents and bulletins that shed light on all of the different ways their examiners oversee the institutions and companies subject to their supervisory and examination authority. While the CFPB does not have direct examination and supervisory authority over franchised auto dealers and other select independent dealers, the financial institutions it does supervise and examine are likely to continue their pattern of assessing dealer compliance as a precondition to doing business. Implementing your own compliance management policies, processes, and procedures across the business is the best way to position your dealership for the evolving lender efforts in this regard.

State Data Safeguards and Security

Recommended Practice

> Check your internal processes and information technology systems to ensure sensitive information about your dealership and customers are safeguarded from unauthorized users

California

The California Privacy Rights Act (CPRA), a ballot initiative approved by California voters in 2020 and made effective in 2023, amends certain provisions of the California Consumer Privacy Act (CCPA). Like the CCPA, the CPRA is supplemented by regulations issued by a new privacy protection agency; however, the nature and the extent of the CPRA's regulatory mandates far exceed those of the CCPA. Specifically, the CPRA establishes a new data protection agency, the California Privacy Protection Agency (CPPA), which shares enforcement responsibility with the California Attorney General. The CPRA expands on the CCPA's requirements for covered businesses to provide California residents with greater transparency and choice regarding how businesses collect and use consumers' personal information. Covered businesses now have an affirmative obligation to respond to specific consumer rights requests, observe restrictions on certain data practices, and update their privacy notices annually to provide detailed disclosures about their data handling practices relevant to California consumers' personal information. See Topic 5 for additional information on these laws.

Colorado

The Colorado Privacy Act (CPA) became effective in 2023. The CPA requires covered businesses to provide consumers with privacy notices and certain rights, ensure personal data is subject to privacy principles, and conduct data protection assessments for the processing of personal data that presents a heightened risk of harm to consumers. The Colorado Department of Law has issued finalized rules to enforce the CPA. Importantly, beginning on July 1, 2024, the CPA started requiring covered businesses to provide consumers with a universal data collection opt-out option, so that a consumer can click one button to exercise all their opt-out rights.

Connecticut

The Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CTDPA) became effective in 2023. The CTDPA contains certain unique requirements, particularly relating to consumer consent, that are more complex than similar requirements in data privacy laws passed in other states. The CTDPA also provides a 60-day cure period for violations, but the right to cure expired on December 31, 2024.

Delaware

Delaware enacted the Delaware Personal Data Privacy Act (DPDPA) in 2023, which will go into effect on January 1, 2025. The DPDPA will provide consumers opt-out and other rights relating to their personal data. Unlike other states' laws, the DPDPA will require most nonprofit organizations and higher education institutions to comply with its transparency and disclosure obligations.

Florida

Florida enacted the Digital Bill of Rights (FDBR) in 2023, which went into effect on July 1, 2024. Unlike other states' laws, the FDBR has higher jurisdictional standards for enforcing the FDBR against entities, which allows more entities to avoid being subject to the law. These standards are aimed at regulating "Big Tech" companies instead of small and middle-market companies. The FDBR also contains unique provisions requiring a revenue threshold to be subject to the law, broadening opt-out rights, protecting children online, and prohibiting government officials from moderating content.

Indiana

Indiana enacted the Indiana Data Privacy Law (IDPL) in 2023, which will go into effect on January 1, 2026. The IDPL will provide requirements and rights substantially similar to other states' data privacy and security laws, allowing for existing data privacy compliance programs to easily adapt to the IDPL.

Iowa

Iowa enacted the Iowa Consumer Data Privacy Act (ICDPA) in 2023, which will go into effect on January 1, 2025. The ICDPA will provide requirements and rights substantially similar to other states' data privacy and security laws. However, it does not grant consumers the right to delete or correct data collected by third parties.

Kentucky

Kentucky enacted the Kentucky Consumer Data Protection Act (KCDPA) which will go into effect January 1, 2026. The KCDPA will provide requirements and rights substantially similar to other states' data privacy and security laws, allowing for existing data privacy compliance programs to easily adapt to the KCDPA.

Maryland

The Maryland Online Data Privacy Act (MODPA) will take effect on October 1, 2025. The MODPA imposes more stringent privacy standards on business than similar laws in other states including requiring a company to minimize the data it holds from the outset.

Minnesota

Minnesota enacted the Minnesota Consumer Data Privacy Act (MCDPA) which will go into effect on July 31, 2025. The MCDPA will provide requirements and rights substantially similar to the other states' data privacy and security laws; however, the MCDPA allows consumers to question automated decisions made about them via profiling.

Montana

Montana enacted the Montana Consumer Data Privacy Act (MCDPA) in 2023, which went into effect on October 1, 2024. The MCDPA provides requirements and rights substantially similar to other states' data privacy and security laws, allowing for existing data privacy compliance programs to easily adapt to the MCDPA.

Nebraska

Nebraska enacted the Nebraska Data Privacy Act (NDPA) which will go into effect on January 1, 2025. The NDPA will provide requirements and rights substantially similar to other states' data privacy and security laws, allowing for existing data privacy compliance programs to easily incorporate the NDPA's requirements.

New Hampshire

New Hampshire enacted the New Hampshire Privacy Act (NHPA) which will go into effect on January 1, 2025. The NHPA will provide requirements and rights substantially similar to other states' data privacy and security laws, allowing for existing data privacy compliance programs to easily adapt to the NHPA.

New Jersey

New Jersey enacted the New Jersey Data Privacy Act (NJDPA) which will go into effect on January 15, 2025. The NJDPA will provide requirements and rights substantially similar to other states' data privacy and security laws, allowing for existing data privacy compliance programs to easily incorporate the NJDPA's requirements.

Oregon

Oregon enacted the Oregon Consumer Privacy Act (OCPA) in 2023, which will go into effect on July 1, 2024. The OCPA is unique in comparison to other states' laws because it imposes stricter obligations, including requiring disclosures about data processing by third parties and subjecting nonprofits to compliance requirements.

Rhode Island

Rhode Island enacted the Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA), which will go into effect on January 1, 2026. The RIDTPPA will provide requirements and rights substantially similar to the other states' data privacy and security laws; however, it requires companies to secure consent before processing sensitive data.

Tennessee

Tennessee enacted the Tennessee Information Protection Act (TIPA) in 2023, which will go into effect on July 1, 2025. The TIPA will be slightly more restrictive than other states' laws, as it will include tighter jurisdictional requirements and steeper thresholds for revenue and processing. The TIPA will otherwise be substantially similar to other states' laws.

Texas

Texas enacted the Texas Data Privacy and Security Act (TDPSA) in 2023, which went into effect on July 1, 2024. Unlike other states' laws, the TDPSA has a much broader application, as it does not contain a minimum revenue requirement or a minimum number of consumers whose personal data is processed or sold for an entity to be subject to the law. The TDPSA does, however, exempt several entities from its provisions as other states do, including utility service providers and state government entities.

Utah

The Utah Consumer Privacy Act (UCPA) became effective in 2023. Fewer entities will be subject to the UCPA, though, because it requires a business to meet both a financial threshold and a data volume threshold to be subject to the law. The UCPA was also one of the first data privacy statutes to take a more limited approach to restricting uses of personal data and several other states have modeled their statutes after the approach taken by the UCPA.

Virginia

The Virginia Consumer Data Protection Act (VCDPA) became effective in 2023. The VCDPA was the first data privacy law to forego a private right of action and only allow the Virginia Attorney General to enforce the law by bringing an action in the name of the state or on behalf of persons residing in the state. Other states have followed suit and chosen to limit enforceability to the state attorney general. The Virginia Attorney General has the power to issue a civil investigative demand to any data controller or processor believed to be engaged in, or about to engage in, any violation of the VCDPA.

Financial Technology Companies

Financial technology companies—or "fintechs"—continue to disrupt the consumer financial services industry by presenting consumers with alternatives to traditional financial institutions. Rather than visiting a brick and mortar to obtain a loan, many consumers are procuring loans through online sources that do not have physical locations. We anticipate that the auto industry will continue to innovate the ways in which it serves its customers. **Fintechs may present new opportunities for dealers to connect with consumers, lenders, and other service providers.**

Compliance Tip

Look for opportunities to work with financial technology or "fintech" firms to connect with consumers, lenders, and other service providers.

We recommend that dealers continue to monitor this development as they may benefit from the changing technological landscape.

Electric Vehicle (EV) Mandates and Incentives

Regulation of vehicle emissions continue to increase in the United States. For example, as recently as March 2024, the Biden Administration boasted that it had passed the country's "strongest-ever pollution standards for cars" by finalizing national pollution standards proposed by the Environmental Protection Agency (EPA). The standards apply to cars manufactured in 2027 through 2032 and aim to reduce carbon emissions by more than 7 billion tons. Along with implementing more stringent emissions regulations, federal and state governments are encouraging auto dealers to stock and sell more electric and hybrid vehicles.

One of the primary ways in which governments promote increased EV sales is through incentives or rebates. For example, as of January 1, 2024, taxpayers can transfer their Clean Vehicle Credit to a dealer at the point of sale. The credit can be applied to the vehicle's down payment and reduce the cost of the vehicle. The dealer then handles the paperwork for the tax credit qualification with the IRS. If the taxpayer does not meet certain qualifications, however, the credit may need to be repaid. **Dealers can submit information**

to the IRS through IRS Energy Credits Online to determine the eligibility and amount of a Clean Vehicle Credit for each vehicle.

Recommended Practice

Visit the IRS's website to determine whether your customer can apply a Clean Vehicle Credit to an electric or hybrid vehicle purchase.

If the submission for tax credit qualification is approved, the dealer must provide the buyer with a copy of the IRS's approval.

Environmental Regulations

Along with stricter emissions standards, auto dealers must continue to navigate a host of new and existing environmental regulations and potential liabilities at both the state and federal level. **Understanding and proactively addressing these environmental standards can help dealerships avoid costly fines and reputational harm.**

Recommended Practice

Stay updated on changes to environmental regulations to help your dealership stay compliant and avoid potential liability.

Most of these standards apply to the dealership facilities themselves. Dealerships may need to comply with regulations related to the disposal and recycling of automotive parts and fluids, the washing of pollutants into waterways or stormwater systems, and the emission of harmful compounds into the air when painting cars or engaging in similar activities. For example, auto dealers that engage in auto body coating, painting, or paint stripping must comply with the EPA's Auto Body Rule controlling hazardous air emissions relating to those activities.

Beyond their activities, auto dealers should also consider any environmental issues presented by their facilities. For example, if a dealership facility is located on real property that has a history of contamination, the owner of the real property may be held responsible for cleaning up the contamination under the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) passed by Congress in 1980, as amended. The EPA enforces the CERCLA and can seek court orders if needed to compel private parties to engage in cleanup actions.

Create a Culture of Compliance

Establishing a culture of compliance, data security, transparency, and honesty with customers is critical to protecting your dealership.

Recommended Practice

Establishing a culture of compliance, data security, transparency, and honesty with customers is critical to protecting your dealership.

You should establish processes to document your compliance and risk assessments, deal by deal. Leveraging a digital solution that identifies which processes were completed for each deal can be invaluable if an audit or regulatory inquiry occurs. In addition, do not forget the importance of a systematic customer complaint system. Seek to resolve complaints using a consistent process with timelines and escalation procedures. The new state data privacy laws require businesses to provide certain rights within a designated period of time and allow individuals to exercise those rights regarding personal information collected by the business. **Remember that, in the long run, it may be better to resolve a dispute in favor of the customer rather than winding up on the CFPB's or FTC's online complaint database, or similarly on the radar of your state attorney general, data protection agency, or the Better Business Bureau.**

Compliance Tip

Create a clear and consistent process for resolving customer complaints to avoid legal and reputational risk.

Additional Resources

FTC, CARS Rule (December 2023)
https://www.ftc.gov/business-guidance/resources/ftc-cars-rule-combating-auto-retail-scams-dealers-guide

CFPB, Registry of Nonbanks Rule (September 2024)
https://www.consumerfinance.gov/rules-policy/final-rules/registry-of-nonbank-covered-persons-subject-to-certain-agency-and-court-orders/

CFPB, Safeguards Rule (May 2024)
https://www.ftc.gov/business-guidance/blog/2024/05/safeguards-rule-notification-requirement-now-effect

CFPB, Proposed Rule for Open Banking (October 2023)
https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/

Minnesota House Bill No. 3438 Junk Fees Ban (May 2024)
https://www.revisor.mn.gov/bills/text.php?number=HF3438&type=bill&version=3&session=ls93&session_year=2024&session_number=0

California Senate Bill No. 478 Junk Fees Ban (October 2023)
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB478

EPA, Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) and Federal Facilities (July 2024)
https://www.epa.gov/enforcement/comprehensive-environmental-response-compensation-and-liability-act-cercla-and-federal

EPA, Biden-Harris Administration Finalizes Strongest-Ever Pollution Standards for Cars (March 2024)
https://www.epa.gov/newsreleases/biden-harris-administration-finalizes-strongest-ever-pollution-standards-cars-position

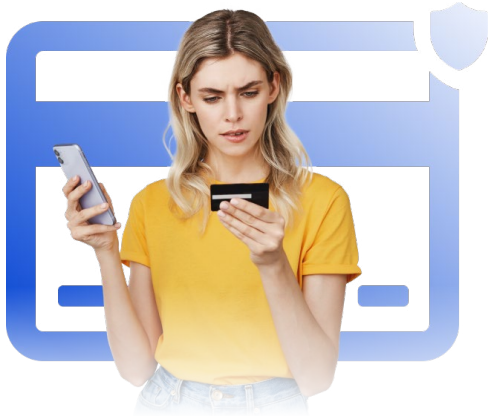
EPA, About EPA's Auto Body Rule (December 2023)
https://www.epa.gov/collision-repair-campaign/about-epas-auto-body-rule

BakerHostetler Advertising Law Blog, Minnesota Passes Junk Fee Law and California Issues FAQs (June 2024)
https://www.adventures-in-law.com/blogs/minnesota-passes-junk-fee-law-and-california-issues-faqs/

BakerHostetler Advertising Law Blog, California Junk Fees Ban (October 2023)
https://www.adttorneyslawblog.com/blogs/what-you-gonna-do-with-all-that-junk-fees/

Credit Applications, Credit Reports, and Contracts

Familiarize yourself with the many laws and regulations that apply to the credit application, reporting, and contracting process.



Train your employees to be diligent →

Did You Know?

The IRS requires the IRS/FinCEN Form 8300 to be filed electronically for reporting cash transactions over $10,000 if 10 or more other tax information statements are filed each year.

Compliance Tip

Regulators are bringing more enforcement actions against auto lenders for failure to report accurate information, or to correct previously reported information that is no longer accurate, to credit reporting companies. Make sure you are handling consumer credit information appropriately to avoid costly fines and reputational harm. See more Tips

What's New for 2025

The CFPB's Small Dollar Rule takes effect in 2025 and institutes new underwriting and credit reporting guidelines for certain lending activities. Consult your attorney to determine whether the Small Dollar Rule applies to your auto financing activities.

Recommended Practice

Consider adopting an internal fair lending policy similar to the model NADA-NAMAD-AIADA Fair Credit Compliance Policy available online here to ensure your dealership is engaging in best practices when financing car purchases. See more Recommended Practices

Breakout Sections

1. Important Laws and Regulations
   - The Fair Credit Reporting Act (FCRA)
   - The Equal Credit Opportunity Act (ECOA) and Regulation B
   - Adverse Action Notice Obligations Under ECOA and FCRA
   - Risk-Based Pricing Notices
   - Security Freeze Laws
   - Truth in Lending Act Requirements
   - State Developments
   - FTC Credit Practices Rule
   - Electronic Signatures and Records
   - Servicemembers Civil Relief Act
   - The Military Lending Act
   - CFPB Small Dollar Rule Effect on Auto Lending
   - USA Patriot Act
   - Car Buyer's Bill of Rights
   - Spot Deliveries
   - Spot Agreements
   - Federal Odometer Law
   - Online Sales
   - State Restrictions on Fees
   - State Single Document Laws
   - Cash Sales
   - Disclosure of Starter-Interrupt and/or GPS Technology
   - Failing to Obtain the Customer's Signature
2. Recommended Practices
3. Sample Adverse Action Notice

Credit Applications, Credit Reports, and Contracts

The following information is not intended to be legal advice. You should consult with your attorney to ensure that you are in compliance with applicable law.

Since the late 1960s, federal law has restricted the use of credit reports and required creditors to notify consumers of credit decisions and describe credit terms in finance contracts. The federal Consumer Credit Protection Act, passed in 1968, includes the Truth in Lending Act (TILA), the Fair Credit Reporting Act (FCRA), and the Equal Credit Opportunity Act (ECOA), as well as other laws relating to wage garnishments and debt collection practices. The 2003 FACT Act added additional consumer rights, disclosures, and protections concerning credit reports, affiliate information sharing, identity theft protection, and risk-based pricing notices to the FCRA. Title X of the 2010 Dodd-Frank Act, also known as the Consumer Financial Protection Act of 2010 (CFPA), requires additional consumer disclosures in adverse action notices. State laws also govern lease and finance transactions, limit fees and charges in connection to those transactions, and require certain additional consumer disclosures for motor vehicle finance and lease transactions.

Important Laws and Regulations

The Fair Credit Reporting Act (FCRA)

FCRA is a federal law that regulates, among other things, the access, use, and distribution of information that meets the definition of a "consumer report," including a credit score. For FCRA purposes, a "consumer report" (often informally called a "credit report") includes eligibility information contained in such reports, as well as certain information obtained from third parties, such as an employer or landlord.

FCRA requires a dealer to have a "permissible purpose" to obtain a consumer report. **A consumer's prior written consent is the best proof of a permissible purpose** and may be required to access consumer reports in a state like Vermont and may also be required under certain contracts with the credit bureaus.

Recommended Practice

| Get the consumer's written consent before obtaining a consumer report.

Most credit application forms contain language providing for such written consent. However, a dealer may also have a permissible purpose to obtain a consumer report when (i) the consumer clearly understands that he or she is initiating a transaction to purchase or lease a vehicle, and (ii) the dealer has a legitimate business need for the credit report to complete the transaction. Many dealers have reason to want a consumer report earlier in the process, in which case they must rely on written authorization from the consumer to obtain the report, as the FTC has stated that pulling a consumer report for comparison shopping purposes or for cash customers is not permitted under FCRA without the customer's prior written consent.

FCRA also requires giving the consumer an "adverse action notice" if the creditor used a credit report, in whole or in part, as a factor in denying credit to the consumer or offering the consumer credit on terms less favorable than those the consumer requested (unless the consumer accepts the less favorable terms). Adverse action notices are discussed below.

Once a creditor provides a loan to a consumer, FCRA further requires the creditor to maintain and provide accurate information to credit reporting companies in connection with the loan. The creditor must ensure that its systems, processes, and procedures used to furnish credit reporting information are regularly updated and functioning properly. If the creditor reports inaccurate information, then they may be required to pay fines, pay compensation to consumers, update their reporting systems, and/or revise their policies and procedures. For example, in July 2022, the CFPB required each of these actions of an auto financing subsidiary of an auto dealer after it furnished inaccurate information to credit reporting companies due to manual and outdated reporting systems, which lowered consumers' credit scores and reduced their access to credit.

The Equal Credit Opportunity Act (ECOA) and Regulation B

ECOA and its implementing regulation, Regulation B, prohibit auto dealers

from discriminating against applicants for credit on the basis of race, color, religion, national origin, sex, marital status, age, sexual orientation, gender identity (including discrimination based on actual or perceived nonconformity with sex-based or gender-based stereotypes), because of an applicant's associations, because an applicant receives income from a public assistance program, or because an applicant has in good faith exercised any right under the Consumer Credit Protection Act (CCPA). Certain state laws include additional protected class categories. The CFPB has entered into consent orders with several finance sources over alleged violations of the ECOA's antidiscrimination provisions. As a result, many finance sources require dealers to implement and maintain a fair lending compliance program.

If gross income, rather than net income, is used in determining a consumer's repayment ability, ECOA will generally require that nontaxable income be "grossed up" to make it equivalent to taxable income in order to avoid allegations of a disparate impact on applicants, such as those with disabilities and the elderly, both of whom are more likely than the general applicant pool to receive substantial nontaxable income. ECOA has other considerations relating to income, including, for example, that a creditor may not discount part-time income in evaluating a consumer's creditworthiness.

The Federal Reserve Board was the agency responsible for enforcing Regulation B prior to such responsibility being transferred to the CFPB. The Federal Reserve Board staff has long held the view that ECOA does not apply to a lease transaction because that transaction is not "credit" as defined by the ECOA. While some courts have taken the opposite (and in many practitioners' view, incorrect) position, most lessors in the industry treat leases as though they are subject to the ECOA as a best practice. Given the uncertainty over whether the CFPB might choose to treat leases as subject to the ECOA, doing so might be an excellent practice.

ECOA also requires that credit application forms (or scripts, as applicable) contain certain disclosures, such as the consumer's right to not reveal income from alimony, child support, or separate maintenance if the consumer does not want such income to be considered as a basis for repaying the credit obligation. Certain state laws impose additional notice requirements in credit applications. Regulation B also requires that multiple consumer applicants affirmatively state on their credit application whether or not they want to apply for joint credit.

States also enforce their own fair lending laws and regulations.

Compliance Tip

Be aware of the fair lending rules for your state - to protect your dealership against discrimination claims and violations.

For example, New York added two additional protected classes under its fair lending rules: military status and sexual orientation. The New York Department of Financial Services (NYDFS) also issued a reminder to supervised entities and sales finance companies that engage in indirect automobile lending through third parties that they must comply with New York's Fair Lending Law, including, but not limited to the development of a fair lending compliance program, despite the federal rollback. Additionally, the NYDFS guidance provides that these entities may be liable for pricing disparities or discrimination based on the dealer reserve amount.

In another example, Connecticut imposed a new requirement for sales finance companies to acquire and maintain information about the ethnicity, race, and sex of applicants for motor vehicle retail installment contracts. However, a temporary "no action" memo was issued by the Connecticut Banking Commissioner indicating that Connecticut's Department of Banking would not enforce that new law pending receipt of an advisory opinion it requested from the CFPB. Under ECOA, this type of data collection is authorized for mortgage, not auto transactions.

Adverse Action Notice Obligations Under ECOA and FCRA

Adverse action means a refusal to grant any credit or a refusal to grant credit in substantially the same amount or on substantially the same terms requested by the consumer, unless the consumer accepts a counteroffer of credit. Adverse action also means terminating an account or changing its terms in a manner unfavorable to the consumer,

except for actions taken in connection with a default or delinquency on the account. An example is unwinding or re-contracting a "spot delivery" contract on less favorable terms. Auto dealers are identified as the creditor/seller on the retail installment sales contract (RISC), despite the fact they later sell the RISC to a finance source.

ECOA mandates the following time frames for providing an adverse action notice:

Compliance Tip

Know your timeframes for Adverse Action Notice obligations under the ECOA.

- 30 days after receipt of a completed credit application concerning the approval of counteroffer to, or adverse action on an application;
- 30 days after taking adverse action on an incomplete application, unless notice is provided of an incomplete application as set forth in Regulation B;
- 30 days after taking adverse action on an existing account; or
- 90 days after notifying the applicant of a counteroffer (if the applicant does not expressly accept or use the credit offered) for notifying the applicant of the credit decision, whether favorable or unfavorable (e.g., offering credit, informing the consumer that additional information is necessary to make a credit decision, making a counteroffer, or sending an adverse action notice).

An adverse action notice is not required if the dealer denies an application by providing a counteroffer which the consumer accepts.

An ECOA adverse action notice must be in writing and, at a minimum, include either specific reasons why the credit application was denied or counter-offered, or tell the consumer how they may contact the dealership within 60 days to get the reasons along with the name, address and telephone number of the person who can provide the specific reason(s) for the adverse action. An ECOA adverse action notice must also include an antidiscrimination notice similar to the one in 12 C.F.R. 1002.9(b). There are additional state laws relating to adverse action as well.

As creditors, dealers should give adverse action notices to consumers in at least three situations:

1. When a dealer takes a credit application but does not send it to any financing source, typically because the consumer is credit-challenged;
2. When a dealer unwinds or re-contracts a spot delivery deal; and
3. When the dealer is unable to get the customer financed on terms acceptable to the dealer.

It is a common misunderstanding that a dealer can rely on a finance source's adverse action notice.

Did You Know?

A finance source's adverse action notice will not shield the dealer from liability, as it does not contain the necessary disclosures that must be given by the dealer.

In fact, a finance source's adverse action notice will not shield the dealer from liability in these instances as it does not contain the necessary disclosures that must be given by the dealer, including but not limited to naming the credit bureaus used and the federal agency that administers compliance for dealers (i.e., the FTC). Furthermore, most lenders advise dealers in their dealer agreement or their program materials that the lender's issuance of any adverse action notice is only on such lender's behalf.

The FCRA adverse action definition is more broadly drafted but includes the adverse action definition as set forth under the ECOA. Under FCRA, an adverse action notice is required when: (i) taking an adverse action with respect to a consumer, based in whole or in part on information contained in the consumer report; (ii) denying consumer credit or increase

of credit, based on information obtained from a person other than a credit reporting agency (e.g., credit worthiness, credit standing, credit capacity, character, reputation, etc.); (iii) taking adverse action based upon information, in whole or in part, received from an affiliate. Generally, a single form can be used to comply with both FCRA and ECOA adverse action notice requirements. Although, additional language is required if the dealer's decision was based in whole or in part on information received directly from a third party that is not a consumer reporting agency.

Recommended Practice

> It is the dealers responsibility to provide the adverse action notice to the consumer.

An adverse action notice must inform the consumer of the adverse action; either give up to four primary reasons for the adverse action or tell the consumer how they may contact the dealership within 60 days to get the reasons; identify any consumer reporting agency that provided a credit report or credit score used by the dealer; provide the consumer's credit score, information about the credit score, and up to four to five "key factors" that adversely affected the credit score (up to four key factors unless one of the factors is the number of recent credit inquiries, in which case up to five key factors). The notice must contain other mandatory language as well. A sample adverse action notice is attached at the end of this Topic.

If the adverse action is completely due to the credit score, the primary reasons must indicate which factors in the credit score caused the adverse action. Using a general statement like "credit score too low" as a primary reason for adverse action does not comply with ECOA.

The primary reasons for the adverse action required by ECOA are not necessarily the same as the FCRA-required "key factors" that must be disclosed to describe what most adversely affected the credit score. These "key factors" are related to the credit score only, not the consumer's overall application for credit, which may also consider other factors, for example, income and ability to repay.

If the dealer uses credit information obtained from a third party that is not a consumer reporting agency, the adverse action notice must inform the consumer and advise they may make a written request within 60 days of the notice to obtain the nature of that information. An example would be information received directly from the consumer's employer, landlord, or a private creditor.

Risk-Based Pricing Notices

Enacted in 2011, the Risk-Based Pricing Rule (RBP Rule) requires informing consumers that they received worse credit terms than other consumers because of information in their credit reports. Receipt of a consumer's credit application triggers the RBP Rule notice requirement. A creditor who uses a consumer report and provides credit to the consumer on "material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers from or through that person" either must give these customers a "risk-based pricing notice" (RBP Notice) or give them a "credit score disclosure exception notice" (CSD Notice). "Material terms" generally means the APR.

Compliance with the RBP Rule is difficult and expensive, a fact that was recognized by the agencies that wrote it and evidenced by the inclusion of the CSD Notice exception. The CSD Notice exception permits a dealer to provide all applicants for credit a disclosure of their credit score and certain other information, i.e., the date and identity of the person providing the credit score; the national distribution of credit scores among consumers under the credit scoring model used, disclosed in either a bar chart form or in language indicating where the customer falls in the national range of credit scores; and certain language disclosures about credit scores in general.

CSD Notices are easily obtained from consumer reporting agencies (e.g., Experian, TransUnion, Equifax, Credco, etc.), and should be provided to every credit applicant as soon as possible after obtaining the credit score but no later than the consummation of the transaction.

Compliance Tip:

Provide a credit score disclosure (CSD) notice to every credit applicant as soon as possible after obtaining their credit score.

If you use multiple credit scores, you must disclose the one on which you most relied. If you didn't primarily rely on one particular score, you can disclose any one of the multiple scores. If a consumer does not have a credit score, you must give that consumer a special form alternative notice stating that no score was available. Notably, the CSD Notice exception does not require disclosing the four to five "key factors" that adversely affected the credit score. The "key factors" disclosure is only required for adverse action notices.

What if your dealership doesn't ordinarily need to pull credit reports or credit scores? Your lender may still expect you to handle this requirement as the initial creditor, and this may require you to buy a credit score anyway.

Security Freeze Laws

All consumers can now freeze their credit files by contacting most consumer reporting agencies, including the three nationwide credit bureaus: Equifax, Experian, and TransUnion. If a customer freezes her credit file, you will be unable to pull her credit report (including her credit score) unless she "thaws" the credit freeze with the credit bureau. If a customer calls the credit bureau to disable the freeze, the report should be available in a relatively short amount of time. If a customer submits a written request to disable the freeze, the process could take up to several days after receipt of the request.

Truth in Lending Act Requirements

The federal Truth in Lending Act (TILA), the federal Consumer Leasing Act (CLA, a subsection of TILA), and their implementing regulations, Regulations Z and M respectively, govern disclosures of credit terms to consumers. TILA and CLA disclosures must be given prior to consummation of the transaction. TILA and state laws also contain disclosure and other requirements for credit applications and consumer credit contracts. Many state laws cap Annual Percentage Rates (APRs) and other charges, as do the federal Servicemembers Civil Relief Act and Military Lending Act discussed below. TILA and Regulation Z, and CLA and Regulation M, do not apply to credit transactions and consumer leases in excess of the then-current amount of the cap. However, it is a best practice to comply with TILA and the CLA regardless of the amount of the obligation on all credit transactions and consumer leases. A number of states require compliance with TILA on all credit transactions, regardless of the credit amount.

TILA generally treats costs of retail installment sales as either part of the amount financed (simplistically, the price of the goods or services financed by the consumer) or as a finance charge (simplistically, the cost to the consumer to finance payment of the goods or services):

- *Amount financed*. Examples of required disclosures in retail installment sales contracts (RISCs) for the cost of the goods or services financed are the amount financed and an itemization of the amount financed. The amount financed includes the cash price of goods or services purchased on credit, and non-finance charge amounts advanced by the dealer to the consumer or paid to others on the consumer's behalf, such as vehicle cost, taxes, registration fees, and sums paid to pay off credit obligations on a consumer's trade-in vehicle. The cost of insurance (credit or property) financed in connection with the transaction can be a component of the amount financed (as opposed to finance charge) if properly disclosed.
- *Finance charge*. This includes many types of charges that TILA defines as part of the finance charge and represents the cost of credit. The finance charge must be disclosed as the total dollar amount of finance charges and the cost of credit expressed as an APR in the RISC. These disclosures must be more conspicuous than any other required disclosures (such as by bolding them, outlining them in a border, using all capital letters, etc.). For examples of finance charges see Regulation Z, 12 C.F.R. 1026.4.
- *Lease Disclosures*. The CLA and Regulation M require that the vehicle's gross and adjusted capitalized cost, residual value, depreciation and amortization, and rent charges be disclosed in lease agreements.

- *Closed-Credit Disclosures*. TILA and Regulation Z also require specific disclosures concerning credit terms of the transaction (e.g. the amount financed and finance charge) that must be provided before consummation of the transaction. For additional information on the disclosures and other requirements see TILA, 15 U.S.C. 1601 et seq. and Regulation Z, 12 C.F.R. 1026.

State laws may require other disclosures and mandate that certain contract terms be conspicuous. Both RISCs and lease agreements must state the number, amounts, and timing of payments. TILA and Regulation Z also include specific rules on disclosing negative equity on a trade-in in a financing transaction. Negative equity should either be used to reduce the customer's down payment or itemized under "Amounts Paid to Others." It should not be disclosed as part of the sales price of the vehicle.

TILA requires creditors to disclose the costs of ancillary products and services that the consumer elects to purchase as part of the transaction, but that are not required in order to obtain credit. These items are typically disclosed in the Itemization of the Amount Financed on the RISC. Simply including the un-itemized cost of aftermarket items, such as vehicle etching, service contracts, rustproofing, and other items, into the cash price of the vehicle constitutes "payment packing," an activity of great interest to the FTC and state Attorneys General. **Even if an aftermarket product is permitted under applicable state and federal law, failing to disclose these items in the Itemization of the Amount Financed could subject the dealer to regulatory scrutiny and/or lawsuit.**

Compliance Tip

Every aftermarket product should be included in the Itemization of the Amount Financed.

For example, a dealer was sued in a class action alleging a TILA violation for including vehicle etching in the cash price of new motor vehicles without disclosing that it was doing so or that the vehicle etching was optional.

Creditors must disclose additional information regarding the cost of credit, including the Total of Payments (in both credit sales and loans) and Total Sale Price (in credit sales only). In addition, creditors must also disclose the security interest (typically in the vehicle), the amount of any late fees that could be imposed, and whether the consumer may prepay the obligation without incurring penalties. The disclosures also must include a contract reference directing the consumer to the contract documents for additional information about the extension of credit. These disclosures and others that could apply to the transaction, along with the finance charge, APR, amount financed, total of payments and total sale price, must be segregated from all other information and may not include any information not directly related to the disclosures.

Additionally, TILA governs disclosure of deferred down payments (also called "pick-up payments"), a practice in which the consumer agrees to make a portion of the contractual down payment at a time later than contract signing and vehicle delivery. A deferred portion of a down payment may be treated as part of the down payment if it is payable not later than the due date of the second otherwise regularly scheduled payment and is not subject to any finance charge. However, most lenders require in their dealer agreements a representation and warranty from the dealer that it has received the down payment in full prior to assigning the RISC to the lender. Thus, while TILA permits deferred down payments, a lender on the receiving end of this representation and warranty could require a dealer to repurchase a RISC for breaching it.

TILA provides several ways to disclose pick-up payments. A creditor may disclose pick-up payments either as part of the down payment or as a component of the amount financed. Other disclosure requirements may apply.

State laws also have provisions relating to deferred down payments. Some states require a separate disclosure of the deferred portion of the down payment on the RISC. Non-disclosure of the deferred portion on the face of the RISC may violate some states' laws.

TILA disclosures must reflect the legal obligation of the parties. If information necessary for the accurate disclosure is unknown, the disclosure may base the information on the best information reasonably known to the creditor and label the disclosures as estimates. In the case of a refinancing, new TILA disclosures must be provided for the refinanced transaction.

Finally, TILA also includes recordkeeping requirements. Creditors must retain evidence of compliance for two years after the disclosures are required to be made.

State Developments

Several states have enacted their own laws requiring certain disclosures for commercial non-real estate financing. To date, eight states have enacted such laws: California, Connecticut, Florida, Georgia, Kansas, New York, Utah, and Virginia. In 2023, the CFPB analyzed existing state disclosure laws in California, New York, Utah, and Virginia, and it determined that those laws are consistent with, and as a result are not preempted by, TILA. The CFPB reached this determination because the state laws extend disclosure protections to businesses seeking commercial financing, while TILA provides its protections to consumers seeking consumer financing.

Most recently, Florida, Georgia, and Kansas passed their own commercial finance disclosure laws, which each took effect in 2024. Florida and Kansas require certain disclosures from providers financing transactions exceeding $500,000, while Georgia requires them for transactions in amounts of $500,000 or less, as California and Virginia do. Connecticut's law applies to financing in amounts of $250,000 or less, Utah applies to $1 million or less, and New York more broadly applies to $2.5 million or less. Other states have considered or are considering similar disclosure laws. Auto dealers should familiarize themselves with commercial disclosure laws in their states that may apply to their financing practices.

FTC Credit Practices Rule

The FTC Credit Practices Rule has three major provisions.

First, it prohibits certain unfair contract provisions, such as making consumers assign their wages to get credit or a creditor taking a lien on household goods to secure payment.

Second, the Rule prohibits "pyramiding" of late fees, which occurs when a payment is considered late only because the payment did not include a late fee from the previous payment.

Third, the Rule also requires giving cosigners an FTC-mandated notice describing their potential liability if the consumer fails to pay. The notice must be given to and signed by the cosigner before the cosigner becomes obligated on the agreement. A "cosigner" is different from a co-buyer, co-borrower, or co-applicant because a cosigner receives no tangible benefit from the agreement but undertakes liability as a favor to the main debtor who would not otherwise qualify for credit.

On the other hand, a co-buyer (one who shares in the purchased goods), a co-borrower (one who shares in the loan proceeds), or a co-applicant do receive benefits. Therefore, they generally are not considered cosigners under the Rule, and you are not required to provide the cosigner notice to them. A classic example of a cosigner is a parent cosigning for their child's credit obligation. Many states have additional requirements for cosigner notices so check with your local attorney on the cosigner notice required in your state. Recall that when two applicants for credit apply for financing, they are required to indicate on the credit application whether or not they intend to apply for joint credit.

Electronic Signatures and Records

The federal Electronic Signatures in Global and National Commerce Act (the E-SIGN Act) and the Uniform Electronic Transactions Act (UETA) adopted by all states except New York were enacted to resolve uncertainty about whether electronic documents and signatures are as valid as paper ones. Both acts provide that electronic records and signatures have the same legal status as ink signatures and paper records. Under both, an "electronic record" is information "that is stored in an

electronic or other medium and is retrievable in perceivable form" and an "electronic signature" is "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

Neither act changes the disclosure or content requirements for documents under other law. The E-SIGN Act requires that consumers specifically consent to receiving disclosures that are required to be "in writing" electronically and provides specific requirements for obtaining such consent. Alternatively, one can provide such disclosures in paper form and avoid the consent procedure imposed by the E-SIGN Act.

Please note that because of limitations in their scope, the E-SIGN Act and UETA do not alter the documentation and signature requirements of Uniform Commercial Code Article 9, which provides the requirements for the customer to grant the creditor a security interest in the vehicle sold. Fortunately, Article 9 permits the use of electronic records and signatures to grant a security interest in substantially the same way as the E-SIGN Act and UETA would. So, the electronic records and signatures used in the customer's financing contract that satisfy the E-SIGN Act and UETA requirements will also satisfy the Article 9 requirements for the contract.

As a result, **a consumer's digital signature on an electronic signature pad linked to an electronic document or their digital signature on a tablet used to provide the documents carries the same legal enforceability as their traditional handwritten signature on a paper document. A click-through to a website can also be an electronic signature.**

Did You Know?

A consumer's digital signature carries the same legal enforceability as their traditional written signature on a paper document.

The electronic document can be stored in an electronic filing cabinet or vault and should be retained for a period of time equal to the retention period for a paper version of the same document. Under TILA, the consumer must receive a copy of the disclosures that the consumer can keep prior to the consummation of the transaction. See more in Topic 11: Recordkeeping and Destruction of Records.

The UETA was not adopted in New York. Instead, prior to the UETA, New York had already adopted its Electronic Signatures and Records Act, which established the legality of electronic signatures in New York starting in 2000. We recommend reviewing New York law for any additional requirements concerning the use of electronic signatures.

Servicemembers Civil Relief Act

Formerly called the Soldiers and Sailors Civil Relief Act, the Servicemembers Civil Relief Act (SCRA) imposes a 6-percent rate cap on pre-existing secured credit, including a vehicle credit sale or a loan, during the period of military service. These provisions apply to both the person in military service and their dependents with respect to obligations entered into by such persons before the service member was called to active-duty status.

The SCRA also allows service members to terminate pre-service automobile leases if they are called for military service of 180 days or longer. Service members who sign automobile leases while on active duty may be able to terminate an automobile lease and receive a refund of any lease amounts paid in advance if they are given orders for a permanent change of station outside the continental United States or to deploy with a military unit for a period of 180 days or longer.

A large auto lessor agreed to pay millions to settle a SCRA claim with the Department of Justice (DOJ) related to DOJ charges that the lessor failed to properly refund lease amounts paid in advance consisting of a pro rata portion of the lessee's capitalized cost reduction (minus manufacturer rebates or similar incentives, the payoff of negative equity or prior lease balances, payments for vehicle maintenance and other ancillary products, the amount of any acquisition fee, and any amounts paid for tax, title, and license). Another automobile financer agreed to a multi-million-dollar settlement with the DOJ following allegations that the financer improperly denied lease termination requests for deployed service members.

In addition, the SCRA requires a creditor to file an affidavit with the court regarding whether or not a customer is in military service before obtaining a default judgment against a customer or whether the creditor is unable to determine whether the defendant is in the military. It also permits a court to stay (delay) the repossession of a vehicle in certain circumstances. It requires a court to review and approve any repossession or termination of a lease if the service member entered into the credit sale, loan, or lease and made a payment before entering military service. The court may delay the repossession or require the creditor to refund prior payments before repossessing. It can also appoint an attorney to represent the service member, require the creditor to post a bond with the court, and issue any other orders it deems necessary to protect the service member. The law also imposes special requirements on a creditor accepting a voluntary surrender of a vehicle.

A large subprime auto finance creditor agreed to pay millions to settle a SCRA claim with the DOJ related to charges that the creditor failed to obtain court orders before repossessing motor vehicles owned by protected service members, preventing them from obtaining a court's review on whether their repossessions should be delayed or adjusted in light of their military service.

The Military Lending Act

The Military Lending Act (MLA) is a federal law that imposes limitations on the cost and terms of certain extensions of credit to service members and their dependents ("covered borrowers"). The MLA applies to "consumer credit" extended by a creditor to a "covered borrower."

For purposes of the MLA, "consumer credit" means "credit offered or extended to a covered borrower primarily for personal, family, or household purposes, and that is: (i) subject to a finance charge; or (ii) payable by a written agreement in more than four installments." There are only four narrow exceptions to this definition of consumer credit: (i) residential mortgages; (ii) any credit transaction that is expressly intended to finance the purchase of a motor vehicle when the credit is secured by the vehicle being purchased; (iii) any credit transaction that is expressly intended to finance the purchase of personal property when the credit is secured by the property being purchased; and (iv) any credit transaction that is an exempt transaction for the purposes of Regulation Z. These narrow exceptions were not clearly defined in the MLA and were left subject to interpretation.

In 2017, the Department of Defense (DOD) released guidance clarifying that whether a transaction qualifies for the purchase-money exceptions described above depends upon "what the credit beyond the purchase price of the motor vehicle or personal property is used to finance." More specifically, "financing costs related to the object securing the credit will not disqualify the transaction from the exceptions, but financing credit-related costs will disqualify the transaction from the exceptions." The DOD failed to define the term "credit-related cost," but provided two examples: Guaranteed Auto Protection insurance and credit insurance. Various trade associations immediately petitioned the DOD to withdraw its guidance, particularly due to its retroactive effect, and these items have since been excluded from the DOD's interpretation. This was a victory for service members who now have financial products to protect them from total vehicle loss. Efforts to obtain further clarification are ongoing.

Under the MLA, a "covered borrower" is a consumer, who, at the time the consumer becomes obligated on a consumer credit transaction or establishes an account for consumer credit, is a covered member or a dependent of a covered member. A "covered member" includes members of the armed forces on active duty or on active Guard and Reserve Duty, and their dependents. Dependents can include the spouse and, in some cases, a child, parent or parent-in-law, or an unmarried person in the legal custody of the military member.

The MLA provides various protections for "covered borrowers." Those protections fall into two main categories: (i) a 36% Military Annual Percentage Rate (MAPR) cap, and (ii) "other MLA terms and conditions," including oral and written disclosure requirements and certain specified prohibitions and limitations, such as a prohibition against using the title of a vehicle as security for the consumer credit obligation. The MAPR

Table of Contents

is an all-inclusive APR that eliminates some prior "finance charge" exceptions under Regulation Z. For example, the MAPR calculation must include (a) fees/premiums charged for voluntary credit insurance, debt cancellation contracts, and debt suspension agreements, and (b) fees for any ancillary products sold in connection with the consumer credit.

In order to ensure that the terms of any consumer credit transactions entered into with covered borrowers meet the requirements of the MLA, the creditor must determine the covered borrower status of every applicant for consumer credit. Though the creditor is not required to use a specific method to determine covered borrower status, the MLA Regulations do allow a safe harbor for covered borrower status determinations. In order to obtain the safe harbor, creditors must either (i) directly or indirectly (perhaps through a service provider) verify the consumer's covered borrower status through the MLA database, or (ii) verify the consumer's covered borrower status by using a consumer report obtained from a nationwide consumer reporting agency that has a statement, code, or indicator (if any) concerning the consumer's covered borrower status. Doing so, and keeping a record of the findings, provides a safe harbor from liability under the MLA's terms in such status determinations.

Violators of the MLA and its regulations are subject to draconian penalties, including $500 per violation in actual damages, in addition to punitive damages, equitable or declaratory relief, court costs, and attorney's fees.

Compliance Tip

Be aware of MLA Regulations to avoid heavy fines and even imprisonment.

Knowing violations are treated as misdemeanors, which can lead to fines or imprisonment. Also, contracts violating the MLA are void from the inception of the contract (that is, the creditor cannot collect any principal or interest under the contract).

You should seek advice of counsel to determine whether the MLA applies to your transactions. In the event it does, it is best to avoid structuring deals that enable the customer to accept cash, ensure the total cost of financing the deal does not exceed the 36% MAPR, provide customers with required disclosures, and document the sale using a contract that does not include an arbitration clause.

CFPB Small Dollar Rule Effect on Auto Lending

On October 5, 2017, the CFPB issued its final rule on Payday, Vehicle Title, and Certain High-Cost Installment Loans (Small Dollar Rule). Although the Small Dollar Rule is targeted at short-term, high-interest rate loans (e.g., payday loans), the Rule has potential consequences for the auto financing industry. The CFPB issued the final Rule in 2020. As currently written, the Rule applies to three types of consumer loans: (i) loans with a term of 45 days or less called "short-term loans," (ii) balloon-payment loans, and (iii) loans charging an APR over 36% that include a "leveraged payment mechanism," such as a debit authorization. Covered short-term loans and balloon payment loans are subject to extensive and burdensome underwriting rules and a new type of credit reporting requirement. Covered leveraged payment loans are not subject to the underwriting and credit reporting requirements, but they are subject—along with covered short-term loans and balloon loans—to new disclosures that must be given before processing certain payments and limits on the number of payment attempts.

Note that, although the Rule is written in terms of "loans," the term "loan" is defined in the Rule to include any extension of credit and, therefore, would include retail installment sales.

The CFPB provided an exemption from the Small Dollar Rule for "certain purchase money security loans." Specifically, the Rule does not apply to credit extended for the "sole and express purpose of financing a consumer's initial purchase of a good, when the credit is secured by the property being purchased, whether or not the security interest is perfected or recorded." In other words, if a consumer receives credit for the express purpose of purchasing a car, the car secures the transaction,

and the amount financed is approximately equal to, or less than the cost of acquiring the car, then the transaction is excluded from the Rule.

However, there are two important limitations on this exemption: financing ancillary products and refinancing a purchase money transaction. Concerning ancillary products, the CFPB noted that the purchase money exemption does not encompass "ancillary products that are being sold along with a vehicle," but "are not themselves the good in which the lender takes a security interest as a condition of the credit." Therefore, financing an ancillary product along with a car could mean that there's no purchase money exemption for the transaction, if the transaction otherwise meets the definition of a "covered loan."

Additionally, the CFPB expressly states in the commentary accompanying the Rule that the purchase money exemption does not extend to refinances of purchase money credit. Therefore, if an auto finance transaction involves ancillary products or refinancing, then it could be covered by the Rule if the (i) term is 45 days or less, (ii) transaction has a balloon payment, or (iii) APR is over 36% and the transaction includes a leveraged payment mechanism. Note that, besides the purchase money exemption, the Rule also contains an "accommodation" exemption for loans made by a lender who makes 2,500 or fewer covered short-term or balloon payment loans per year and derives no more than 10% of its receipts from such loans. As a result, some sellers of motor vehicles may be permitted to engage in a "de minimis" volume of covered loans, without application of the Rule's requirements to such loans.

On October 19, 2022, the Fifth Circuit Court of Appeals ruled that the CFPB's funding mechanism is unconstitutional, and as a result invalidated the Small Dollar Rule. *Comm. Fin. Servs. Assoc. of Am. v. CFPB*, 51 F.4th 616 (5th Cir. 2022). Following the Fifth Circuit's decision, the CFPB petitioned the U.S. Supreme Court for a writ of certiorari to determine whether the Fifth Circuit erred in holding that the CFPB's funding structure is unconstitutional and in vacating the Small Dollar Rule. The Supreme Court granted certiorari, heard oral argument on October 3, 2023, and issued a decision on May 16, 2024, overruling the Fifth Circuit's opinion and finding that the CFPB was acting within its authority to issue the Small Dollar Rule. *CFPB v. Comm. Fin. Servs. Assoc. of Am.*, 601 U.S. 416 (2024).

The Small Dollar Rule is now set to take effect on March 30, 2025, for all covered loans.

You should seek advice of counsel to determine whether the Rule applies to your transactions.

USA Patriot Act

The USA Patriot Act, administered by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), mandates that no U.S. person (including auto dealers) can do any business—cash or credit—with persons or entities included on OFAC's list of Specially Designated Nationals and Blocked Persons (SDN List). These are lists of persons or entities suspected of being associated with or funding terrorist organizations and other criminal enterprises. The list is frequently updated, and a searchable version of the list is published on OFAC's website: https://sanctionslist.ofac.treas.gov/Home/index.html.

For compliance with the USA Patriot Act, you must run all of your customers—both cash and credit—against the SDN List (including the names of any individuals who directly or indirectly own 50% or more of any entity that is a party to a new transaction).

Compliance Tip:

Run every customer (cash or credit) against the OFAC SDN list for USA Patriot Act compliance.

You should also run service and parts customers who make unusual orders (e.g., high quantities of materials that could be used in making an explosive device) or who otherwise seem suspicious. You may conduct the search online yourself, or you can purchase a product from a credit bureau or an identity verification service to systematically check a customer against the current SDN List.

If you get a preliminary match, OFAC lists a series of steps to determine if you have a true match or a false positive. If you believe you have a true match after following those steps, you must call OFAC at their designated number, and you cannot do business with that person unless instructed otherwise. You must report each blocked transaction to OFAC and submit an annual report of all blocked transactions using forms on the OFAC's website, including Form TD F 90-22.50, which can be found at: https://ofac.treasury.gov/ofac-reporting-system.

Car Buyer's Bill of Rights

In 2006, California passed significant legislation, known as the "Car Buyer's Bill of Rights," affecting the way dealers sell and finance the purchase of motor vehicles. Since then, several states have passed their own versions of the Car Buyer's Bill of Rights. These laws generally give consumers additional rights and may, among other things, require dealers in affected states to make additional written disclosures to consumers with respect to certain charges and aftermarket products, as well as providing standards for selling "certified" used vehicles.

You should consult with your attorney to ensure that your procedures are designed to comply with the requirements of the law of the jurisdiction applicable to the transaction.

Spot Deliveries

Spot delivery refers to the practice of a dealer placing a consumer in a vehicle "on the spot" to make a sale, prior to obtaining a finance source's approval to purchase the financing contract. The sale is made contingent upon the dealer obtaining financing for the purchase, typically by a finance source agreeing to buy a RISC signed by the consumer and the dealer. Spot deliveries are regulated in many states, and in a few states are either prohibited or significantly restricted. State regulation of spot delivery varies greatly. Many states have specific requirements for terms on which spot deliveries may be conducted, disclosures that must be provided to consumers, and the form of the spot delivery agreement. For example, a few states require that the conditions for delivery be included in the RISC, while others require the spot delivery terms to be in a stand-alone document.

Also, consider whether the applicable law addresses certain spot delivery practices, such as:

- Limiting fees for miles driven by the customer;
- Prohibiting the sale of the customer's trade-in vehicle until the deal is finalized; and
- Limiting the number of days to obtain financing approval.

Your dealership should also have procedures designed to ensure that spot deliveries are conducted in accordance with applicable law.

Failure to use appropriate documentation and procedures for spot deliveries invites lawsuits from consumers and the attention of regulators.

Compliance Tip

Consult an attorney and know your state's laws on spot deliveries. See Topic 13 for updates on recent lawsuits and enforcement actions involving improper spot deliveries.

In many states, botched spot deliveries may result in claims under state laws prohibiting unfair and deceptive acts. You should consult an attorney and know your state's laws on spot deliveries before engaging in the practice.

Spot Agreements

Except in states where the spot delivery terms and conditions are required to be in a stand-alone document, it is good practice to incorporate the spot delivery terms and conditions in the RISC. This minimizes the risk that a consumer will be able to require your dealership to honor the terms of the RISC even if no financing source has agreed to purchase the RISC. Even in states where spot deliveries are unregulated, the spot delivery terms and conditions should always be agreed upon in writing. Without a signed spot agreement, the dealer will have signed an unconditional RISC with a buyer

for the purchase and financing of a vehicle. If the dealer can't sell the RISC, the dealer is obligated to honor the deal unless it has a spot agreement demonstrating that the parties agreed that the deal could be unwound.

Generally, spot agreements permit either the dealer or the consumer to unwind the deal if the dealer cannot find a financing source willing to purchase the contract on the terms set forth in the RISC.

In the event that a sale is unwound and the dealer and the consumer elect to "re-contract" by entering into a new sale on different terms, it is generally a good practice to have the consumer sign a document that memorializes the fact that the parties have agreed to cancel the prior contract and enter into a new transaction. This helps a dealer to demonstrate that the consumer made a voluntary decision to sign the new contract. It is also a good practice to conduct another menu transaction when re-contracting an unwound spot deal and to keep all the documentation from both transactions together in one master deal jacket in case an issue comes up later.

Dealers should never backdate a new contract to the original date of vehicle delivery. This practice is likely to violate TILA disclosure requirements which mandate that finance charges can only accrue from the date of consummation. If the contract is backdated, a customer's attorney could argue that the date of consummation was the date the customer signed, meaning that the customer will have paid interest for the days between the date on the contract and the date it was consummated and, as a result, that the APR and finance charge disclosures are incorrect. Class actions have been brought against dealers who backdate new contracts on unwound spot deals.

A pattern of numerous unwinds of spot deals may give plaintiffs' lawyers or regulators grounds to claim the dealer is engaging in "yo-yo financing," which can be a deceptive trade practice under Section 5 of the FTC Act or state law. It is a good practice to monitor what percentages of your spot deals are unwound. If you see the percentage rising, investigate and train your sales and F&I officers on what types of deals you believe your lenders will buy. **A dealer should be prepared to show that the dealership made a good faith effort to get the original deal financed with multiple finance sources.**

Compliance Tip:

Be prepared to show that the dealership made a good faith effort to finance a deal with multiple finance sources.

Many of the principles applicable to spot deliveries in a sale transaction would apply to a lease transaction, though some terms and conditions of the spot delivery might change based on state law. Any forms used to document the terms of the lease spot delivery would need to reflect those changes.

Federal Odometer Law

This law requires sellers of motor vehicles to disclose to buyers in writing the odometer reading of the vehicle being sold and prohibits tampering with odometer devices. The buyer must review and sign the disclosure. For used car sales, the odometer reading at the time of transfer must be disclosed on the title. Specific additional disclosures are required by this law and other applicable regulations, plus there are recordkeeping requirements. State laws also govern registration and titling requirements, with additional requirements at the federal level.

For example, for decades the National Highway Transportation Safety Administration (NHTSA) required a "wet signature" on an odometer disclosure for sales of vehicles 10 model-years old or less. However, in September 2019, NHTSA finally allowed states to develop their own odometer disclosure forms that may use an e-signature. It is important to note that in some states, such as California, laws still prevent fully electronic vehicle sales.

Online Sales

State laws have not quite caught up with evolving online vehicle sales and financing platforms, but dealers are able to increase sales by selling to out-of-state buyers using a variety of web-based tools. When an out-of-state dispute arises, the buyer will often attempt to sue the dealer in the buyer's home state and claim that the dealer should have been licensed

in their home state and/or that the law of their home state (including those laws addressing contract disclosures, and related consumer credit requirements and limitations) applies to the transaction. This could potentially trigger scrutiny by state regulators, too. Be sure to also check your dealer agreements with your lenders. Many dealer agreements contain representations by you that the deal has been conducted entirely within your dealership, and thus may subject your deal to repurchase.

Note that one area where guidance from the states does exist in connection with online sales is advertising. Many states do have specific rules in connection with online advertising. And some states have included express provisions in their auto industry regulations to include online statements within their regulatory definitions of "advertisements" by auto dealers. It is important to consult a knowledgeable attorney on how to minimize your risks when selling to out-of-state customers through an online sale process.

State Law Restrictions on Fees

State laws also limit or restrict fees that may be charged by a dealer, especially when the vehicle purchase will be financed in a credit sale. Some fees are only applicable to credit sales (e.g., application fees, credit investigation fees, lien recording fees, etc.). State retail installment sales acts and consumer credit codes often limit or prohibit the kinds of fees that may be charged in a credit sale. Some of these fees may also be treated as a finance charge under federal law, state law, or both.

Some fees are charged in both cash and credit sales. Document preparation ("doc fees") is a good example of a fee that dealers typically charge in both cash and credit sales. As a general rule, a dealer should not charge doc fees in a credit sale unless the dealer also charges the same doc fee in a cash sale. This is because charging a doc fee only for credit sales means that the doc fee will be treated as a finance charge under federal law, and that complicates things for the dealer and any assignee of the finance contract. In many states, a doc fee that is a finance charge would be subject to rebate upon prepayment of the finance contract. In addition, the systems responsible for creating the federal TILA disclosures on a RISC will not be able to calculate the impact of the doc fee on the finance charge and APR disclosures. So, a dealer that charges a doc fee only on credit sales is likely to understate the finance charge and APR in violation of federal law, and possibly state law as well.

Even where doc fees are charged on both cash and credit sales, state law may limit the doc fee to a specific dollar amount or to a reasonable amount in relation to the actual costs of preparing and filing documentation. A great deal of litigation has occurred relating to the propriety of doc fees charged by dealers in states where no specific amount is provided by law. Know your state law on permissible doc fees and consult your local attorney if no specific amount is permitted, or the doc fees are limited to being "reasonable."

You should consult with your attorney to ensure that all fees comply with applicable state law.

State Single Document Laws

A single document rule requires that all documents, or certain documents, evidencing the sale and financing transaction between the dealer and the buyer be contained in one document. The state single document rules take varying forms. Usually, however, a state's rule will permit multiple pages. You should make certain that you know whether your state has a single document rule and how it applies to your documentation of a deal.

Cash Sales

If a customer purchases a vehicle with cash or cash equivalents in excess of $10,000, you must file IRS/FinCEN Form 8300 within 15 days after receiving the cash payment.

Did You Know?

If a customer purchases a vehicle with cash or cash equivalents in excess of $10,000, you must file IRS/FinCEN Form 8300 within 15 days.

As of 2024, the form must be filed electronically if you are filing 10 or more information returns other than Forms 8300 for the year. For this

Table of Contents

purpose, “cash” is not only currency but currency equivalents, such as traveler’s checks, cashier’s checks, bank drafts, and money orders, if they have face amounts of $10,000 or less (note that monetary instruments with a face value of more than $10,000 are not considered cash because the financial institution issuing the instrument is required to report the transaction). A personal check and a bank check representing the proceeds of an auto loan made to the customer by the bank are not considered cash or cash equivalents because they are part of an ongoing relationship between the customer and the bank. If the customer conducts a “related transaction” (another transaction within 24 hours, such as buying another vehicle for cash, or transactions more than 24 hours apart if you know, or have reason to know, that each is one of a series of connected transactions), then you must total all the cash and cash equivalent payments from both transactions for purposes of calculating whether you collectively meet the greater than $10,000 threshold for filing IRS/FinCEN Form 8300. By January 31 of the following calendar year, you must send a notice to the customer informing the customer that you filed an IRS/FinCEN Form 8300 during the prior calendar year.

The penalties for failure to comply with IRS cash reporting laws can be significant if the IRS deems it to be intentional or in reckless disregard of the dealer’s obligations. Intentional disregard is the knowing or willful failure to file. For forms required to be filed on and after January 1, 2025, merely failing to file on time subjects a dealer to a penalty of $330 per instance (i.e., a negligent violation), up to an annual aggregate limit of $1,329,000 for businesses with gross receipts not exceeding $5 million and $3,987,000 for businesses with gross receipts exceeding $5 million. Intentional disregard raises the maximum penalty to $33,220 per instance or the cash received by the dealer in the transaction, up to a maximum of $132,500. Note that the IRS adjusts the penalty amounts for inflation annually. A dealer should adopt a written policy to educate employees on cash reporting (including the definition of cash and cash equivalents), the dealer’s obligations, and how to avoid illegally structuring transactions with the person providing the cash. A dealer can also file a Form 8300 to report a suspicious transaction, even if the transaction does not meet the $10,000 threshold, if it suspects a customer is structuring cash payments in a manner intended to avoid reporting requirements. The criminal penalties for money laundering, the signs of money laundering, and the dealer’s written policy on reporting such suspicious transactions should also be a part of your compliance plans. Consider training, monitoring, and using the DMS system in the background to flag transactions based on types of funds received.

Disclosure of Starter-Interrupt and/or GPS Technology

A dealer who fails to fully disclose and obtain the consumer’s consent to install and use the starter interrupt and GPS technology for payment assurance purposes may risk violation of federal and state law. At the very least, the disclosure must clearly and concisely explain that the technology is installed on the vehicle as a condition of the extension of credit, describe how the technology will be used, and obtain the consent of the buyer to the use of the technology.

While using starter interrupt or GPS technology is legal in most jurisdictions, most retail installment contracts do not allow a creditor to impose a charge for the installation and use of the technology when such installation and use is a condition of the credit extension. In addition, regulators frown on such charges and therefore, dealers that assess charges for installation and use of the technology in these instances face potential litigation risk and regulatory scrutiny.

Consult your attorney for guidance relating to disclosure requirements, best practices, and/or legal limitations on usage.

Failing to Obtain the Customer’s Signature

If you fail to obtain a customer’s signature on a RISC, Buyer’s Order, or any other document, the dealer should not sign the customer’s name.

Recommended Practices

1. Always have proof of a "permissible purpose" to pull a consumer's credit report.

Recommended Practice

> Always have proof of a "permissible purpose" to pull a consumer's credit report.

A signed authorization from the consumer (generally on a credit application) is strongly preferred but not required (except in certain states) when both the dealer and customer understand they are close to completing a credit transaction. Most credit applications, which are usually signed by the consumer, contain language where the consumer agrees that you can access their credit report. Check your agreements to confirm whether this language is included. Finance sources usually obligate dealers to provide credit applicants a list of the names and addresses of the finance sources to which the dealer may send their credit application to avoid being deemed a consumer reporting agency under FCRA.

2. Give or send a risk-based pricing notice or credit score disclosure exception notice to every applicant for credit.

Recommend Practice

> Give or send a risk-based pricing notice or credit score disclosure exception notice to everyone who applies for credit.

You can obtain the consumer's credit score and the distribution of credit scores for the scoring model used from a credit bureau, or a third-party source such as Dealertrack. The only exception is for customers who do not have a credit score, and they should receive a separate notice for consumers without a credit score. Even if you don't typically pull credit on applicants, you may have to buy a credit score to give the credit score disclosure notice to all credit applicants to meet your obligation to your lenders. Give the notice to the consumer as soon as possible after getting the credit score information necessary to complete the credit score disclosure notice form. Keep a copy in the deal jacket.

3. Send adverse action notices when required.

Recommended Practice

> Be sure to send adverse action notices within 30 days or as noted in the Adverse Actions Notice Obligations above when they are required.

Remember to send an adverse action notice when you decline credit or when unwinding a spot deal, for example. Note that adverse action notices require inclusion of a consumer's credit score and credit score disclosures including up to four to five key factors that adversely affected the credit score if the credit score was a factor in the adverse action.

4. Consider adopting, implementing, and monitoring compliance with an ECOA/Fair Lending policy, to protect your dealership against legal penalties, fines, and lawsuits related to discriminatory lending practices.

Recommended Practice

> Consider adopting, implementing, and monitoring compliance with an ECOA/Fair Lending policy to protect your dealership against legal penalties, fines, and lawsuits related to discriminatory lending practices.

Staff training and monitoring buy rate markups can be a part of the policy. One good practice, originally developed by the Department of Justice (DOJ), is to implement a consistent buy rate markup amount for all customers and permit markdowns only, based on significant, non-discriminatory, pre-identified legitimate business reasons. The reasons should be documented in the deal jacket to demonstrate the legitimacy of the action should a finance source or regulator audit the dealer's practices. This documentation should be a purely internal document and not something to give to the customer. This approach is the foundation of the NADA-NAMAD-AIADA Fair Credit Compliance Policy and Program Compliance Form (NADA Form) which closely tracks not only the approach of the DOJ but also provides a list of the specific reasons it approved in the case settlements it entered into in 2007. You can obtain a copy of the NADA Form from NADA: https://www.nada.org/regulatory-compliance/nada-fair-credit-guidance.

Table of Contents

5. Do not charge credit customers higher prices than cash customers on vehicles or aftermarket products.

Recommended Practice

> All customers should be charged the same prices, regardless of whether they pay cash or use credit.

Be prepared to show there is no negative purchase price differential for credit as opposed to cash customers. Use a menu-selling process for aftermarket items to show you consistently offer products to all consumers at the same prices. Comply with Car Buyer's Bill of Rights and/or other applicable state law requirements for disclosures of aftermarket products.

6. If spot deliveries are permitted in your state, always use a spot agreement containing terms permitted or required by your state.

Recommended Practice

> Use the terms permitted or required by your state when creating a spot agreement for spot deliveries.

Include language that gives both you and the buyer the right to unwind or re-contract if you cannot obtain financing approval for the original contract on the terms set forth in the RISC. Your attorney should review and approve your form spot agreement for compliance with your state's laws. Track your percentage of unwound spot deals. A significant percentage can lead to claims of deliberate "yo-yo" financing by the dealership, which some courts have held to be an unfair trade practice.

7. Document the re-contracting of an unwound spot deal.

Recommended Practice

> Document the re-contracting of any unwound spot deal. Do not backdate the new contract the customer is signing.

When you re-contract a spot deal, do not backdate the new contract the customer is signing. Date the new contract on the day when both parties sign. And don't forget to give the customer an adverse action notice for unwinding the original contract.

8. Advise customers on how to quickly thaw their frozen credit files before having their credit pulled.

Recommended Practice

> Advise customers on how to quickly thaw their frozen credit files before having their credit pulled.

For customers who have placed security freezes on their credit files, have a sheet of paper available containing the phone numbers of all three national credit bureaus (Equifax, Experian, and TransUnion) for the customer to call to temporarily "thaw" their credit files so that you can pull a credit report on the customer. This will require the customer to have available the PIN issued to them by the credit bureau when they froze their credit file. It is not advisable to take the customer's PIN or offer to make the calls for the customer. If you spot deliver or sell a vehicle to a customer with a frozen credit file, proceed with extreme caution. Consider obtaining additional information, such as a pay stub, bank statement, or other evidence of the customer's creditworthiness, and be especially diligent when verifying the customer's identity. Few lenders will purchase a contract for a customer on whom they cannot pull credit.

9. Provide full disclosure and obtain the customer's consent to install and use starter interrupt or GPS technology for payment assurance purposes.

Recommended Practice

> Before installing and using starter interrupt or GPS technology for payment assurance, provide full disclosure and get the customer's consent.

Be transparent about the GPS technology and the disclosure must at minimum explain that the technology is installed on the vehicle as a condition of the extension of credit, describe how the technology will be used, and obtain the consent of the buyer to the use of the technology.

Additional Resources

Fair Credit Reporting Act and Regulation V
https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act

https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1022/

Equal Credit Opportunity Act and Regulation B
https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter41-subchapter4&edition=prelim

https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1002/

Consumer Leasing Act and Regulation M
https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter41-subchapter1-partE&edition=prelim

https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1013/

Truth in Lending Act and Regulation Z
https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter41-subchapter1&edition=prelim

https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1026/

Car Buyer's Bill of Rights - California
https://www.dmv.ca.gov/portal/car-buyers-bill-of-rights-ffvr-35/

Servicemembers Civil Relief Act
https://www.justice.gov/crt/servicemembers-civil-relief-act-summary

Military Lending Act
https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section987&num=0&edition=prelim

Risk-Based Pricing Rule
https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-640

Information about Filing IRS Form 8300 on cash deals with cash payments over $10,000
http://www.irs.gov/pub/irs-pdf/p1544.pdf

Office of Foreign Assets Control
https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

Sample Adverse Action Notice Form

The following is a sample of one form of adverse action notice appropriate for use in certain circumstances. There are a number of other model forms that may be more appropriate for a given transaction, including those provided by the CFPB: https://www.consumerfinance.gov/rules-policy/regulations/1002/c/. Consult your attorney for advice on which model form, if any, could serve as a template for your dealership.

Data Safeguards and Identity Theft Protection

Secure your dealership's and customers' information from data breaches and identity theft through internal training and technological safeguards.

Deter hackers and identity thieves with appropriate data security →

Did You Know?

More than 15,000 auto dealerships, including their customers, were affected by a cyberattack in 2024. Be sure to take steps recommended in this guide to help protect your dealership from cyberattacks in 2025.

Compliance Tip

Train your employees regularly on how to avoid common cybersecurity threat tactics, including phishing, spam, and other messages employees may receive containing harmful links or requesting sensitive information. Learn more

Watch List for 2025

Cybersecurity remains a focus of federal and state governments. In 2024, the FTC's new notification procedures under the Safeguards Rule went into effect. Those procedures require non-bank financial institutions to notify the FTC of any event in which unencrypted customer information involving 500 or more consumers is acquired without authorization. Read more

Recommended Practice

Consider using endpoint detection and response (EDR) technology to monitor cybersecurity threats to your dealership network and automatically mitigate any that arise. See more Recommended Practices

Breakout Sections

Data Safeguards and Identity Theft Protection

Identity theft and data breaches continue to be serious and ongoing issues for consumers, affecting millions each year.

Did You Know?

Identity theft and data breaches affect millions of consumers each year. Don't let them happen at your dealership.

Small to Midsize Businesses (SMB), such as auto dealerships, may face many of the same cyber security threats as larger organizations, especially when the SMB maintains sensitive information about consumers.

Should a breach happen, chances are good that the response will be costly. Businesses suffering a data breach are faced with a myriad of costs including, but not limited to, those related to systems remediation, legal, public relations, forensics, communications, regulatory, diversion of management and employee time, loss of customers, and expenses to preserve the company's name and reputation in the community.

In this Topic, we discuss laws and regulations relating to a dealer's obligations to safeguard and securely dispose of customer and employee information, and to verify customer identities. Additionally, the risks to dealers from certain forms of identity theft are changing dramatically as lenders look to dealers to repurchase contracts – even contracts that have been paid for a period of time – entered into with identity thieves.

Important Laws and Regulations

The FTC Safeguards Rule

The FTC's Safeguards Rule, which was amended in 2021 to incorporate additional information security requirements, applies to "financial institutions." This term is broadly defined to include, among other entities and activities: (i) retailers significantly engaged in financial activities (including extending credit); and (ii) automobile dealerships that, as a usual part of their business, lease automobiles on a nonoperating basis for longer than 90 days.

Thus, the Safeguards Rule requires auto dealers to ensure the security and confidentiality of their customers' personal information by using appropriate administrative, technical, and physical safeguards. The Rule also requires auto dealers to take reasonable steps to ensure that affiliates and service providers safeguard the customer information provided to them.

Under the Safeguards Rule, an auto dealer must develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards that are appropriate to the dealership's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue (Information Security Program). **The Safeguards Rule requires that the Information Security Program be designed to (1) ensure the security and confidentiality of customer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.**

Did You Know?

Dealers must implement a comprehensive Information Security Program to safeguard their dealerships.

The dealer's Board of Directors (or its highest governing authority) must approve and take responsibility for the initial Information Security Program (which includes receiving reports on the program and taking appropriate action where required). A senior officer must be appointed to be the Information Security Program manager responsible for developing, overseeing, implementing, training on, updating, and administering the Information Security Program, but the final responsibility remains with the Board of Directors or the highest governing authority.

An Information Security Program must include certain basic elements to ensure it addresses relevant aspects of a dealer's operations. Among other things, the Information Security Program must:

- Describe how the program will protect customer information – both in paper and electronic format – and protect against anticipated threats to information security;
- Designate a specific employee to implement and supervise the Information Security Program;
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks in each relevant area of operations (i.e., employee training, information systems, prevention/response measures for attacks);
- Design and implement safeguards to control risks identified in the risk assessment, and regularly monitor, test, and update them;
- Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information;
- Include a documented security incident and data breach response plan in your Information Security Program for use in the event of any irregularity or in the event any consumer information is lost, stolen, or compromised;
- Test, evaluate, and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

On December 9, 2021, the FTC published significant updates modifying the Safeguards Rule in many relevant respects, including generally:

- additional guidance on development and implementation of the required written information security program, including in the areas of access control, authentication and encryption;
- additional focus on accountability in terms of board reporting requirements;
- exemptions for entities collecting information on fewer than 5,000 consumers; and
- additional defined terms and examples.

The Safeguards Rule requires designating a single "qualified individual" to implement and oversee the information security program, who has practical knowledge appropriate to the company's business circumstances and is solely responsible for overseeing and implementing the program, including training and personnel oversight (contrasting with the prior option to designate more than one person for this function). The required written information security program must be based on periodic and documented risk assessments and risk mitigation plans, with specific additional requirements to include: (a) criteria for the evaluation and categorization of identified security risks or threats; (b) criteria for the assessment of information security, and (c) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

Security training requirements are also enhanced. All personnel must receive awareness training that is updated as appropriate in view of the risk assessment. Information security personnel must be provided training and updates that are "sufficient to address relevant security risks" and the organization must verify that key information security personnel are keeping their subject matter knowledge current.

Specific requirements have also been added for the written incident response plan. This documentation must cover: (a) plan goals; (b) internal response processes; (c) roles, responsibilities and levels of decision-making authority; (d) communications and information sharing; (e) identification and remediation of identified weaknesses in information systems and associated controls; (f) security event and response documentation and reporting; and (f) evaluation and revision of the plan following a security event.

As with the risk assessment and incident response plan, the report to the Board of Directors also has specific content requirements. The

Table of Contents

report, to be delivered at least annually, must include: (a) overall status of the security program and the organization's compliance with it and, (b) "[m]aterial matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program."

The final Rule requires a significant slate of other specific security controls, although there may be exceptions available based on compensating controls in certain cases. These controls include:

- multi-factor authentication for consumers and the covered entity's internal users;
- physical access controls for customer information repositories or systems;
- limitation of access to customer information in accordance with "need-to-know;"
- encryption of customer information, in transit and at rest;
- inventory and classification of data;
- adherence to secure software development practices (this applies both to internally developed applications and evaluation of third-party applications);
- formal management of IT changes to control security risk;
- logging and monitoring of systems to detect abuse by authorized users;
- penetration testing (at least annually) and vulnerability assessment (at least semi-annually); and
- secure disposal of customer information within two years of last use and more generally, adherence to data minimization principles.

The updated Safeguards Rule also expands the security measures required in connection with the selection of third-party service providers. Although the prior version of the rule already required selecting service providers capable of maintaining appropriate safeguards for customer information and the inclusion of contractual obligations with service providers requiring these safeguards, the final rule requires a periodic assessment of service providers based on risk in relation to the continued adequacy of their safeguards.

The timeline for compliance with the amended Safeguards Rule was staggered, with specific requirements becoming effective December 9, 2022, which was extended to June 9, 2023, when the following requirements went into effect: designating a single qualified individual responsible for the information security program; providing written reports to the Board of Directors or equivalent governing body; conducting periodic written risk assessments; implementing and reviewing specific access and authentication controls; hiring qualified employees and providing appropriate updates and training to personnel; maintaining oversight of service providers; adopting controls for disposing of consumer information; and establishing a written incident response plan.

Notification Events

In October 2023, the FTC again updated the Safeguards Rule to require non-bank "financial institutions" to report to the FTC any notification event where unencrypted customer information involving 500 or more consumers is acquired without authorization. The notice to the FTC must include: (1) the name and contact information of the reporting financial institution; (2) a description of the types of information that were involved in the notification event; (3) if the information is possible to determine, the date or date range of the notification event; (4) the number of consumers affected; (5) a general description of the notification event; and, if applicable, whether any law enforcement official has provided the financial institution with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the FTC to contact the law enforcement official. Such report is due as soon as possible, but no later than 30 days after discovery of the event and must be

provided electronically through a form located on the FTC's website, https://www.ftc.gov. This notification requirement went into effect May 13, 2024.

Employee Oversight

The FTC's consent decrees have made clear its expectation that businesses engage in certain practices as a baseline for safeguarding information. Among specific security requirements cited by the FTC were the following:

- Checking references or doing background checks before hiring employees who will have access to customer information and doing so in a way that comports with FTC guidance;
- Asking every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information;
- Limiting access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs. Very few people in your dealership need access to all customer information and you should limit permissions accordingly;
- Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.);
- Using password-activated screen savers to lock employee computers after a short period of inactivity; and
- Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device. Encrypt customer information wherever it is located.

The FTC has found that failing to have a defensible password security policy or permitting "weak" administrative passwords such as common words with no capitalization (e.g., "password"), numbers, or symbols (e.g., "12345") can constitute inadequate data security. The FTC also faulted a leading social networking provider for storing and sending passwords in plain text emails.

As reflected in the changes to the Safeguards Rule discussed above, the FTC has also focused on employee training as a key element of an Information Security Program. Dealers should train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information. Some protections may include:

- Locking rooms and file cabinets where records are kept;
- Using complex passwords and not sharing or openly posting employee passwords in work areas;
- **Encrypting sensitive customer information when it is transmitted electronically via public networks;**

  Recommend Practice

  > Encrypt sensitive customer information when it is transmitted electronically via public network such as documents containing Social Security Numbers, Date of Birth, Account numbers and so on.

- Training employees to identify and report phishing and other email cybersecurity attacks;
- Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and
- Reporting suspicious attempts to obtain customer information to designated personnel.

In addition to training employees, ensure that there is proper oversight and supervision, including:

- Developing policies for mobile devices and employees who use personal devices to make certain that those devices are secured. One way to do this is by using a Mobile Device Management (MDM) solution, which can be used to enforce mobile device policies, ensure secure communications and monitor and track activity;
- Developing policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to adhere to secure system configuration and use policies, including for example using anti-malware protection;
- Imposing disciplinary measures for security policy violations including termination of employment; and
- Triggering procedures as soon as possible, including by using automated mechanisms, to prevent terminated or departing employees from accessing customer information.

Information Systems

Information systems include hardware and software, networks, servers, operating systems and more, performing functions involving information processing, storage, transmission, retrieval, and disposal. Replace all systems that are no longer supported and make sure your antivirus, anti-malware, firewall, and other security software is up to date at all times (other kinds of software should also be updated and patched promptly). **Here are some suggestions on maintaining security throughout the lifecycle of customer information, from data entry to data disposal.**

Compliance Tip

See below for suggestions on what you should include in your dealership's plan for handling customer information.

Know where sensitive customer information is stored, both on your information systems and with service providers, and ensure that it is stored securely. Know its life cycle throughout your organization. Document this information; such documentation is often referred to as a "data map" or "data flow" diagram — the format is not important as long as it has the basic information about what data goes with what systems, and can be understood by legal and IT personnel. Make sure only authorized employees have access. For example:

- Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods;
- Store physical records in a room or cabinet that is locked when unattended;
- When customer information is stored on a server or other computer, ensure that the computer is accessible only with a "strong" password and encryption and is kept in a physically secure area;
- Place customer information on a separate secure server, including a cloud-based server. Limit permissions and require additional access requirements (multi-factor authentication) such as a randomly generated token number and additional password to be able to access the server;
- Where possible, avoid storing sensitive customer data on a computer with an Internet connection. It is a good practice to provide "read only" access to customer information and disable the ability to download customer information onto third-party devices (USBs, external hard drives, etc.);
- Maintain secure backup records and keep archived data secure by storing it off-line and in a physically secure area;
- Maintain a careful inventory of your company's computers, servers, and any other equipment on which customer information may be stored;
- Monitor employees accessing customer information in both paper and electronic format. You should review the monitoring regularly to detect any unusual spikes in activity and quickly find out the reason;
- Get a static IP address from your Internet Service Provider. This will keep your IP address from changing and enable sites like Dealertrack to only accept requests for customer information from

Table of Contents

your trusted IP address. This can be a major protection in the event employees' usernames and passwords are compromised; and

- Use a cloud-based proxy server or a software-based proxy server to prevent users from going to sites that are associated with viruses, malware, or that are otherwise insecure.

Take steps to ensure the secure transmission of customer information. For example:

- When you transmit credit card information or other sensitive financial data, make sure you are using a reasonably current encryption protocol (e.g., TLS 1.2) to secure connections, so that the information is protected in transit;
- If you collect information online directly from customers, make encrypted transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email (especially in response to an unsolicited email) or pop-up message; and
- If you must transmit sensitive data by email over the Internet, be sure to use encryption.

Do due diligence and obtain appropriate assurances from third-party service providers who have access to your customer information and make sure their standards for protection are at least as comprehensive as yours. Reserve the right to do security audits of third-party vendors for compliance with required security standards. Make sure they are obligated to provide you with prompt notice in the event they experience a security incident that could compromise your customer information or your systems (if applicable).

Dispose of customer information in a way that ensures it can't be accessed or recovered and, where applicable, consistent with the FTC's Disposal Rule (Topic 11: Recordkeeping and Destruction of Records).

Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:

- Check with software vendors regularly to get and install patches that resolve software vulnerabilities;
- Use antivirus, anti-malware, and anti-spyware software that updates automatically;
- Maintain up-to-date firewalls;
- Regularly ensure that ports not used for your business are closed; and
- Promptly pass along information and instructions to employees regarding any new security risks.

Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to:

- Know the life cycle and path of information that comes into your network. Monitor for any irregularities which may indicate an intruder has gained access to your system;
- Keep logs of activity on your network and monitor them for signs of irregular activity or unauthorized access to customer information;
- Use an up-to-date intrusion detection system, such as an endpoint detection and response (EDR) tool, to alert you of attacks;
- Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user or data being transmitted from unexpected devices in your network;
- Insert dummy accounts into each of your customer lists and monitor the dummy accounts to detect any unauthorized contacts or changes;
- Assess the vulnerability of your website and computer network to commonly known and reasonably foreseeable attacks, such as SQL injection attacks. Arrange for penetration testing by an independent security specialist or firm;

Table of Contents

- Implement simple, free or low-cost, and readily available security defenses to SQL and similar attacks;
- Use readily available security measures to monitor and control connections from your network to the Internet;
- Prevent users from downloading “P2P” file-sharing network software that can allow any network user to access other users’ data servers;
- Employ reasonable measures to detect unauthorized access to consumer information such as by keeping log events, paper file access records, and other records of persons accessing consumer information. Watch for changes in users’ access behavior. If a user’s access to customer records increases unexpectedly, quickly find out why;
- Configure systems to preclude downloading of customer information to portable media such as USB drives or external hard drives. Ideally, customer information should remain on a server with read-only access on user devices;
- Conduct regular audits of your security system and operations to determine the effectiveness of your Safeguards program and to correct any deficiencies; and
- Make customer information “read only” and not downloadable to any remote devices such as cell phones or tablets. These devices are typically harder to secure and should not have customer information retained in their hard drives.

Take steps to preserve and protect customer information in the event of a security incident or data breach in accordance with your Incident Response Plan, which must be part of your Safeguards Information Security Program. The Incident Response Plan should consider the elements identified above as required by the Safeguards Rule, as well as:

- Taking immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet but do not unplug it so you can make a forensic copy without certain artifacts being deleted when the machine is powered off. Do the same for infected or possibly infected servers;
- Preserving and reviewing files or programs that may reveal how the security event occurred;
- If feasible and appropriate, bringing in security and forensics professionals to help assess the security event as soon as possible;
- Preassigning responsibilities under the incident response program to specific individuals at the dealership so a response team can be quickly assembled and begin to take action immediately in response to an actual or suspected security event;
- Notifying consumers, regulators, law enforcement, and/or businesses in the event of a security breach:
    - Assess the state and federal laws applicable to your business. All states have laws that require consumer notification when that consumer’s personal information is compromised. The applicable triggers vary by state. Your response program should include template letters for customers in all relevant states and territories;
    - Notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm. Certain state laws require the Attorney General or other state regulator to be notified or receive copies of notices that are sent to consumers. Federal regulators, such as the FTC, may need to be notified as well; and
    - Where required, notify the credit bureaus and other businesses that may be affected by the breach.
- Employing a best practice of offering consumers whose Social Security numbers and/or driver’s license numbers are involved one or two years (depending on the consumer’s state of residence) of credit monitoring or other identity protection service at no

charge. Consumer reporting agencies from which you obtain reports may require that you do so, as do a number of states;

- Knowing the deadline by which any required notices must be sent and having a plan to meet that deadline. Some state laws have tight timeframes for when notifications to consumers and government authorities must be made;
- Testing your response program periodically and making appropriate changes; and
- Obtaining cyber security insurance to cover costs of responding to a security event. Cyber security insurance is available in forms to cover specific costs (e.g., costs to notify customers and provide credit monitoring, costs of forensics, and other consultants to identify and contain the security event) and is affordable based on the extent of coverage and policy deductibles.

Bring Your Own Device (BYOD) Risks

A critical issue is employees using their personal smartphones, tablets, and other personal devices to access nonpublic personal information of consumers through their employer networks. "BYOD" or "bring your own device" has become the shorthand expression for use of personal devices for business purposes. The benefits of BYOD often include reduced hardware costs for the company as well as greater employee satisfaction from using a single portable device for workplace and personal use. Notably, however, some states such as California may require that employers reimburse their employees for a portion of their employees' cell phone bill if the employee uses the device for business purposes. Consult your counsel for more information on those state law requirements.

However, BYOD use adds another element of security risk that should be addressed in your Safeguards Program. A comprehensive risk assessment should be conducted to assess whether employees are already using their own devices for dealership business and accessing nonpublic personal information of consumers in doing so. The risk assessment should identify the types of devices and security features available to select the best technical means for program implementation and develop the specific policies and procedures governing BYOD administration and management. A variety of mobile device management (MDM) software options are available to control devices accessing your systems. Physical control over the device should be high on the list for every dealership – the baseline assumption is that the device will be lost or stolen, or at the very least, accessible to unauthorized third parties. Placing tracking mechanisms on these devices if lost or stolen is a prudent security practice but may raise privacy concerns among employees. You should consult with your counsel concerning the use of tracking devices on an employee's personal device, as it may raise certain legal issues under state privacy laws.

Another good practice is to make it clear that combining business and personal communications on one device creates a risk of personal information being exposed when parties are in litigation.

Compliance Tip

Provide employees the information they need to weigh the risks and benefits of using their personal device for business.

Employers may, under certain circumstances, exercise the capability to wipe or erase all data remotely from any device used for business purposes – and that means the device may be wiped entirely, including personal photos and contacts. However, in some circumstances, employees should be given notice and the opportunity to preserve their personal photos and other non-business-related data prior to the device being wiped. Consult with your counsel to determine the appropriate course of action prior to erasing or wiping an employee-owned device. Dealerships also must consider various technical issues associated with its BYOD policy which may include the use of untrusted devices, wireless networks, or applications; support for multiple mobile operating systems; installation of security patches and software updates; and interaction with other systems for data synchronization and storage.

Employees may resist the implementation of security software and

Table of Contents

measures on their personal devices as well as forced encryption of customer information in transit to and from the device and at rest on the device which is a best practice. Dealerships also must detect and prevent "jail breaking" of the device where the employee circumvents the organization's security policies and measures, a practice that MDM software can make more difficult. An alternative to BYOD is to supply your employees with corporate-owned and issued devices, which gives employers greater control over and access to the device and its contents.

Record Retention and Disposal

An Information Security Program should also include a written document retention and disposal policy. See Topic 11: Recordkeeping and Destruction of Records for more information on these policies.

State Data Security Laws

States are also enacting strict data security laws that apply to all organizations that maintain information about their residents. For example, some states:

- Require the development of a comprehensive written information security program, and the encryption of all personal information stored on laptops and portable devices or transmitted wirelessly or across public networks. Employee access must be limited, and paper records must be locked up;
- Require reasonable technical, administrative, and physical safeguards to protect against unauthorized access to or use of personal information; and
- Require compliance with the Payment Card Industry Data Security Standard (PCI-DSS) for credit and debit card information and transactions.

Note that some states have enacted insurance data security laws that apply to certain businesses licensed under the insurance laws in those states. Some of these laws may also apply to financial services organizations. Typically, these data security laws require covered organizations to have minimum safeguards in place, conduct risk assessments, and notify additional regulators, such as that state's Department of Insurance or Department of Financial Regulation.

New York Department of Financial Services Cybersecurity Rule

One such law is the New York Department of Financial Services (NYDFS) Cybersecurity Rule, which may apply to auto dealers if the dealer is operating as a "sales finance company" or a "service contract provider." In New York, a dealer is a "sales finance company" if it provides financing to customers for balances of $25,000 or more. A dealer is a "service contract provider" if it is obligated under an agreement to perform repair, replacement, or maintenance of property, or indemnification for repair, replacement, or maintenance, due to a defect in materials or workmanship or wear and tear, and who is not the manufacturer or seller of the property. There may be other situations in which your dealership may need to be licensed by NYDFS and you should consult your own attorney to confirm.

The NYDFS Cybersecurity Rule applies to all entities required to be licensed by the Banking Law, the Insurance Law, or the Financial Services Law of New York ("covered entities"). Already one of the most comprehensive cybersecurity regulations in the United States, NYDFS significantly amended the Rule on November 1, 2023. The amendment, including its notification provisions, became effective on December 1, 2023, with a compliance date of April 29, 2024, for most other provisions.

One major change is that smaller companies are no longer exempt from implementing multi-factor authentication (MFA). Under the amended Rule, all covered entities must now implement MFA for all user accounts accessing any of the covered entity's information systems unless the covered entity qualifies for a limited exemption, in which case MFA must be implemented for all (1) remote access to the covered entity's information systems; (2) remote access to third-party applications, including but not limited to those that are cloud based, from which nonpublic information is accessible; and (3) all privileged accounts (other than service accounts that prohibit interactive login).

Another important change is that the Rule now explicitly requires notification to NYDFS of cybersecurity events involving the deployment of ransomware within a material part of a covered entity's information systems as well as notification to NYDFS within 24 hours of making an extortion payment, with additional information about the extortion payment required within 30 days.

The Rule also requires a covered entity to have a cybersecurity program which includes:

- Risk assessments;
- Independent audits;
- Vulnerability management;
- Access privileges management;
- Third-party service provider management;
- Asset management;
- Cybersecurity monitoring and training; and
- Incident response and business continuity and disaster recovery (BCDR) planning.

Covered entities must also appoint a Chief Information Security Officer (CISO) and senior leadership must have oversight of the covered entity's cybersecurity program.

It is important that you consult your attorney to determine which specific state laws may apply to your dealership.

Identity Theft and Fraud Prevention

Social Security Number Protection Laws

Many states have passed laws restricting the use, communication, posting, emailing, or mailing of Social Security numbers (SSNs) and other nonpublic personal information (NPI). Many of these state laws prohibit (i) denying goods or services to a person who declines to give their SSN, (ii) printing of SSNs on ID cards, (iii) communicating SSNs to the public or posting or displaying them, (iv) mailing SSNs within an envelope; and/or (v) emailing SSN or other consumer NPI in an unencrypted email. A few states require companies that collect SSNs to have policies in place to protect the SSNs.

- California's law provides a good example of prohibited activity and applies to businesses, government, and other entities. The law prohibits:
- Printing SSNs on ID cards or badges;
- Printing SSNs on documents mailed to customers, unless the law requires it, or the document is a form or application;
- Printing SSNs on postcards or any other mailer where it is visible without opening an envelope;
- Avoiding legal requirements by encoding or embedding SSNs in cards or documents, such as using a bar code, chip, or magnetic stripe;
- Requiring people to send SSNs over the Internet, unless the connection is secure, or the number is encrypted; and
- Requiring people to use an SSN to log onto a website unless a password is also used.

SSNs should be truncated in any visual or printed form and be safeguarded in electronic and paper files. Encryption of Social Security numbers and other NPI is a best practice for electronic records and mandatory in transmitting SSNs over electronic networks such as the Internet.

FTC Red Flags Rule

The Red Flags Rule requires a dealership to perform a risk analysis to develop and implement a written Identity Theft Prevention Program (ITPP) to detect, prevent, and mitigate identity theft. It is not a "one size fits all" rule. A dealer's ITPP must be appropriate to the size and complexity of the dealership and the nature of its operations.

Table of Contents

The Red Flags Rule requires lenders to monitor accounts in their portfolio (along with written-off accounts) for evidence of identity theft to attempt to detect and mitigate further identity theft. So, more lenders are examining delinquencies and written-off accounts for identity theft, even accounts that may have paid for substantial periods of time. Instead of just writing these accounts off as credit losses as they did in the past, lenders are now forcing dealers to repurchase accounts they identify as identity theft accounts, even if the identity thief has made payments for a period of time. This "back end" repurchase risk presents perhaps your biggest financial risk from identity theft. A good ITPP program will protect you, the dealer, more than anyone else.

The dealer's Board of Directors (or its highest governing authority) must approve the initial ITPP and take responsibility for it. A senior officer must be appointed to be the ITPP program manager (Program Manager), responsible for developing, overseeing, implementing, training, updating, and administering the ITPP, but the final responsibility will rest with the Board of Directors or the senior management team.

The ITPP has four basic elements:

1. First, identify potential "red flags" that might occur in your business. Red flags are patterns, practices, or specific activities that indicate the possible existence of identity theft. The Red Flags Rule lists 26 potential red flags that you must consider for your ITPP, including the receipt of an address discrepancy alert (discussed below), although not all will apply to your business. One type of red flag is where a consumer provides an ID that does not appear genuine.

2. The second element of the ITPP is to employ procedures to detect any identified red flags in your processes and transactions. An electronic identity verification service such as Dealertrack Red Flags can help you compare the customer's reported information to fraudulent databases and stolen Social Security numbers, among other red flags. Following the example of a red flag related to IDs, your ITPP would set out different processes for identity verification in person versus other methods of application. For in person, for example, you would include a practice of examining every customer's IDs (front and back) for tampering or counterfeiting. For online applications, you could leverage a third party's solution to validate the consumer's identity through a series of knowledge-based questions and answers.

3. The third element requires your ITPP to have measures to prevent and mitigate identity theft when you identify a red flag. In the ongoing example, it could be as simple as asking the customer for additional verification documents or, if necessary, declining to open the account. Your ITPP should have processes where significant and/or unresolved red flags are escalated to the Program Manager.

4. For the fourth and final element, you must update your ITPP periodically (but not less often than once per year) based upon your dealership's own experiences and new information concerning identity theft from regulators, law enforcement, and industry experts. An ITPP is a dynamic program and should be re-evaluated continually.

Employees who perform program functions should prepare annual reports to the Program Manager concerning the ITPP's effectiveness and make suggestions for improvement. The Program Manager should then use these reports and other identity theft resources to make an annual report to your Board or senior management detailing the effectiveness of the ITPP and proposing material changes. Training of employees and strict oversight of ITPP service providers who have access to your customers' data are also critical tasks that the Red Flags Rule requires. Document everything you do and keep copies of all identity-related documents (e.g., the report of the electronic identity verification service and anything the consumer gives you to prove their identity) in the deal jacket in case you are audited. Apply your ITPP to every customer.

Note that while the Red Flags Rule does not apply to cash sales, the requirements provide a wealth of information for dealers to use broadly in their business to help avoid identity theft issues and losses.

Table of Contents

Synthetic Identity Theft

Unlike traditional identity theft, where someone steals and misuses a person's actual identity, a perpetrator of Synthetic Identity Fraud (SIF) starts with a single piece of legitimate personal data (e.g., social security number) and builds a fake identity around it using false information such as an address or phone number. Detecting SIF can be challenging, as many traditional fraud models and identity verification methods are not designed to detect fake people. In addition, most people who engage in SIF build up a responsible financial history for the fake identity before becoming delinquent on payments to make the fake identity appear more like a real person.

Following both the FTC Safeguards Rule (aimed at keeping private consumer information private) and the FTC's Red Flags Rule (aimed at catching inconsistencies in credit applications) are great ways to prevent and detect synthetic identity fraud. There are several other measures dealers can take to mitigate their risk against SIF. Ensuring that full and accurate data is entered on every credit application is a great start to combating SIF. Many investigations into successful fraud purchases uncovered credit applications that were incomplete, provided limited details, or contained blatantly incorrect information. Utilizing ID authentication and verification technology to authenticate driver licenses can help to validate the individual via address verification, red flag, OFAC, synthetic fraud checks, and States' databases to verify an active license. Establishing "proof of presence," like requiring Multi-Factor Authentication, ensures applicants can immediately access their phone/email to confirm communication. Reviewing suspicious application documentation, such as forged employment verification letters, invalid proof of income information, and inconsistencies of credit report history and age, are also great ways to identity red flags for synthetic identity related fraud.

Reviewing a customer's credit report may also provide dealers a means of detecting potential SIF. Dealers should look for an unusual lack of credit history for the customer's age, information on the credit report that does not quite match up with information they have received from the customer, several hard credit inquiries in a short span of time, a rapid rise in the FICO score, and any other details that may appear suspicious. In those circumstances, the dealer should utilize both technology (additional ID verification measures) and common sense (additional inquiry with the customer about his or her explanation for the suspicious credit activity) to protect the dealership against a SIF incident. If SIF occurs at a dealership, the dealer should report the incident to the FTC at reportfraud.ftc.gov or call 1-877-ID-THEFT.

The Address Discrepancy Rule

The FCRA imposes specific obligations on users of consumer reports when an address discrepancy is identified by a consumer reporting agency. Together with its Red Flags Rule, the FTC issued a companion rule related to the address discrepancy requirements. The law requires users of consumer reports who receive a notice of address discrepancy from a consumer reporting agency to have reasonable policies and procedures in place to form a reasonable belief that the consumer report relates to the consumer about whom the report was requested. For example, there are multiple John Smiths, and the law requires you to take appropriate steps to verify that you have the consumer report for your applicant prior to taking any action based on the consumer report.

In addition, dealers who establish a continuing relationship with consumers for whom they have received a notice of address discrepancy and who routinely furnish information to a nationwide consumer reporting agency (Experian, Equifax, Trans Union), must also reasonably verify the accuracy of the address provided by such consumers and furnish the verified address to the nationwide consumer reporting agency that provided the consumer report and notice of address discrepancy.

Credit and Debit Cards: Fraud Prevention

In an effort to prevent credit card fraud, the industry has moved to credit cards with computer chips (a "chip card"). The use of chip cards requires more sophisticated card readers that can read a random code generated by the device.

As of October 1, 2015, **if you do not use a chip card reader you face the risk of being liable for a fraudulent transaction committed using a chip card.**

Did You Know?

If you do not use a chip card reader you face the risk of being liable for a fraudulent transaction committed using a chip card.

Further, the Fair Credit Reporting Act (FCRA) prohibits printing more than the last five digits of a credit or debit card number or the card's expiration date on any electronically printed card transaction receipt. Damages for doing so are $100 - $1,000 per receipt for willful violations (generally a knowing or reckless violation) with no cap on damages in a class action. MasterCard and Visa can also assess fines starting at $5,000 for the first violation and going up from there. Make sure your card processing machines are set up to not print any more than the last five numbers and do not print the card's expiration date.

Cybersecurity

Ransomware attacks have become more common and also more sophisticated, including against dealerships. For example, in June 2024, more than 15,000 auto dealerships were affected by a cybersecurity attack on a dealership software provider, which also affected their customers' sensitive information. The threat actors responsible for these incidents conduct extensive research on their targets so they can identify sensitive company information and use this information to exploit the organization. While large companies are attractive to these criminals because of the massive ransom payments they can afford, small businesses are also targets because the threat actors understand that these businesses sometimes lack the resources needed to maintain the systems and dedicate the necessary staff to ensure their data is safe. A common method used is one where the threat actor steals data before encrypting the files. This allows the threat actor to also extort the victim with threats to publicly release the information if the victim refuses to pay the demanded ransom.

There are practices in which dealerships can engage to be vigilant about protecting their information from these types of incidents. **Endpoint detection and response (EDR) is a cybersecurity technology that monitors devices connected to a network from threats and automatically responds to mitigate them.**

Compliance Tip

To protect your dealership and your customers, consider adopting endpoint detection and response (EDR) technology to help prevent data breaches.

Widespread deployment of this tool, set in enforcement mode and actively monitored, is the first step towards significantly enhancing the organization's security posture. When EDR is combined with the patching of commonly targeted devices, and a resilient backup strategy, it can allow dealerships to avoid attacks, mitigate the impact of attacks that occur, and enable restoration without the need of purchasing a decryption tool from the threat actor. Even in situations where a dealership is unable to prevent an incident from occurring, having current and complete backups can substantially reduce the overall impact to the dealership and its customers.

Recommended Practices

1. **Create a culture of security at your dealership and get senior management buy-in.**

Recommended Practice

Create a culture of security at your dealership and train your employees on the importance of safeguarding customer information.

Limit permissions to access customer information to only those persons who need access to perform their jobs; require passwords to contain letters, symbols, and numbers and be changed frequently. Know the flow of information that enters your system and monitor for any unusual data flows in or out. These may be signs that a hacker has entered your system and is compromising security. Keep logs of who accesses customer information and when they do so for both electronic and paper files. Train your employees on the importance of safeguarding customer information. Do not leave credit apps or credit

reports out in the open or in unsecured file drawers. Consider using processes that can determine if your employees are actually following the policies and procedures in your Information Security Program. Regularly review access logs of the consumer information records and follow up promptly if you see any unusual spikes in any employee or other user accessing customer files. Lock down files at night and on weekends and implement a "clean desk" policy that requires all paper documents containing customer information to be locked up when not in use.

2. Put into place an Information Security Program that details how you safeguard and securely dispose of all your consumer information.

Did You Know?

Dealers must create an Information Security Program for safeguarding and securely disposing of all your consumer information.

Include a detailed data security incident and security breach response plan in the Information Security Program. Follow FTC guidelines for Information Security Programs and know your state's law on use, communication, and display of Social Security numbers and consumer notification requirements in the event of a data breach. Avoid storing consumer information longer than is necessary or allowing access using widely known simple passwords. Make sure your dealership's Information Security Program includes detailed provisions for the secure disposal of consumer information, both paper and electronic. Train and re-train employees, perform stress tests to evaluate your systems regularly, and update provisions as required. Destroy hard drives and flash drives on computers, copiers, fax machines, and wireless devices using industry standard procedures before discarding them or trading them in for replacements. Disable USB flash memory drives. Try to store customer information only in secure central servers and preclude the ability to download it. Some states (for example, Massachusetts) require that customer information contained on laptops, tablets, cell phones, and other remote devices must be encrypted. Massachusetts and Nevada also require personal information about residents be encrypted in transmissions, which is a best practice in any event and required for credit card data transmission. Consider the adoption of EDR technology to monitor threats to your dealership network and automatically mitigate any that arise.

3. Manage user permissions to give customer information access only to those employees and service providers having a legitimate business need.

Recommended Practice

Limit customer information access only to employees and service providers with a legitimate business need.

When customer information is negligently made available for theft by outsiders, employees can and do steal customer information and sell it to identity thieves. So, it is critical that you keep event access logs of those persons who access your customer information in both paper and electronic files. Review the access logs regularly to monitor patterns of irregular activity by users. Set your system to prevent downloading or file transfers of customer information to computers, USB memory sticks, PDAs, cell phones, tablets, or other remote devices, and disable PC PSTs. If you have a credit application on your website, make sure it is encrypted and begin safeguarding and tracking access to it from the time it is completed by the consumer and securely transmitted to your dealership. Keep your antivirus, anti-malware, and firewall software up to date. If you permit employees to use their own devices to access dealership information, do a risk assessment of BYOD issues and see if it is feasible for your dealership to implement a policy to enable employees to use personal devices. If so, employ MDMS software to manage the devices. If not feasible, cease their ability to do so and require that only company-issued devices be used to access dealer databases and information.

4. Have an acceptable use policy.

Recommended Practice

Have an acceptable use policy and discourage the use of text messaging for business communications.

Table of Contents

Help control risk by adopting an "acceptable use" policy that ensures employees are not sharing their device, are adhering to strong passwords, and that any corporate-owned data is encrypted. Text messaging for business communications should also be discouraged as that information may be discoverable from the device in litigation and the use of acronyms or shorthand often leads to misunderstandings.

5. Have a pre-established plan in place to deal with data security events.

Compliance Tip

Dealers must develop a plan to deal with data security breaches.

The FTC has said that your Information Security Program must include a detailed incident and breach response and notice plan to execute in the event of any actual or suspected security event or database hack in which customer information is or may have been wrongfully accessed, whether by internal or external persons. Pre-identify a team of people to manage the response to any actual or suspected security events. The team should represent each department that might be affected by a security event or that must be mobilized to interact with the public, including legal, human resources, privacy, security, IT, communications, and, if you are publicly traded, investor relations. Part of the team's role is to analyze risks to data, data flow, and worst-case scenarios. Test your plan periodically by doing mock drills. Consult your attorney to know your state law and the laws of your customers' states of residence about when you must give notices to customers and regulators about data breaches.

6. Prepare templated customer communications in advance and consider retaining a forensics expert who can quickly capture and analyze your IT system to identify the source of an electronic breach and mitigate further losses.

Recommended Practice

Have resources ready to contact customers and quickly track down the source in the event of an electronic data security breach.

Consider channeling all third-party communications through only one person for consistency. Consult with your own legal counsel prior to releasing any statements or other communications about the incident. The steps you take in the first 48 hours after a data security event may be the most critical to mitigating the incident and minimizing losses. Those steps should be laid out in advance in your security incident response plan. That is why your plan should assign roles to incident response team members in advance so each knows their precise responsibilities and the response team can be immediately assembled. Consider retaining a third-party forensics firm prior to an incident, to expedite the investigation process in the event a potential or actual security incident occurs.

7. Do not transmit customer information over insecure channels such as unencrypted email, P2P systems, or wireless access points.

Recommended Practice

Never transmit customer information over unencrypted email, P2P systems, or wireless access points.

These are not secure media. The FTC has cited the absence of data loss prevention software and an intrusion detection system in these media as inadequate practices for an Information Security Program.

8. Run an OFAC SDN List check on every customer, cash or credit.

Recommended Practice

Run an OFAC SDN List check on every customer: cash or credit.

If you get a preliminary hit, follow the steps listed by OFAC to determine whether the hit is a "false positive." Do not do business with the customer until you are certain that they are not the person listed on the SDN List. Keep a record of OFAC checks for five years.

9. Develop a risk-based Red Flags Identity Theft Prevention Program (ITPP) and implement it consistently for all consumer credit customers and business credit customers that present identity theft risks.

Recommended Practice

> Be sure to integrate checkpoints for federal Red Flag Rule requirements into your sales process for customer identification verification.

Use your ITPP with every customer and document that you're doing so. Choose red flags that are appropriate to the size, location, and activities of your dealership. If you sell vehicles over the Internet or to customers who never physically come to your dealership, take enhanced steps to verify those customers' identities. Examine photo IDs, look at recent credit bureau activity, and use an electronic identity verification service to compare customer information against databases of fraudulent activity and to assess the customer's given Social Security number. Identify any red flags in your ITPP that these actions reveal. If you cannot readily resolve the red flags with the customer, use knowledge-based authentication "challenge" or "out-of-wallet" questions as well. Escalate problematic customers who resist requests for identity verification to your Program Manager and continue to seek additional information or ask more out-of-wallet questions. Make sure your ITPP program has a process for documenting your ITPP activities for each credit customer. Do ongoing training and periodic testing of your ITPP. Refine and update your Program as new information about identity theft comes to your attention. Don't forget about holding an annual Program review for participating employees and making an annual report to your Board of Directors and senior managers.

10. Educate your employees about the risks of identity theft and social networking attacks.

Recommended Practice

> Educate your employees about the risks of identity theft and social networking attacks.

Emails purporting to be genuine from friends, law enforcement, or trusted institutions may contain links that unload malware onto the employee's PC and network if clicked on or may trick the recipient into providing their credentials to a bad actor.

Additional Resources

FTC Business Security Guide
https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

Data Breach Response: A Guide for Business
https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

FTC's Identity Theft Website
https://www.identitytheft.gov

FTC Safeguards Rule
https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information

FTC Safeguards Rule: What your Business Needs To Know
https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

FTC announces new Safeguards Rule provision: Is your company up on what's required?
https://www.ftc.gov/business-guidance/blog/2023/10/ftc-announces-new-safeguards-rule-provision-your-company-whats-required

Department of the Treasury, information and links to the OFAC SDN List
http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

OFAC – Assessing SDN List Matches for a Customer
http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#match

Searchable OFAC List – Enter a business name to identify matches on the OFAC list
http://www.instantofac.com

FTC Consumer Information Disposal Rule
https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how

State Data Security Breach Notification Laws
http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Social Security Randomization
https://www.ssa.gov/employer/randomization.html

Protecting Customer Information

Avoid exposing your dealership to legal actions and fines by understanding your limitations on collecting and sharing information about potential and current customers.

Protect your dealership by protecting your customers' privacy →

Did You Know?

Data privacy laws in most states permit civil penalties of up to $7,500 per violation, but the maximum amount is higher in some states. For example, starting in 2025, New Jersey's maximum per violation penalty will be $10,000 for initial violations and $20,000 for subsequent violations. Limit your exposure to these penalties through appropriate data privacy protection practices.

Compliance Tip

Before sharing a customer's eligibility information with an affiliate such as your parent company or insurance company, make sure you have given the customer an opportunity to opt out of affiliate information sharing.

What's New for 2025

Nine states' comprehensive data protection laws go into effect in 2025: Delaware, Indiana, Iowa, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Tennessee. Auto dealers subject to these states' laws should learn about their obligations and incorporate them into their 2025 compliance plans. See more at Important State Laws and Regulations

Recommended Practice

Review and update your privacy notices and policies at least annually, especially when required by California or other applicable law. See more Recommended Practices

Breakout Sections

Table of Contents

Privacy and Consumer Information Sharing

Federal law and regulations limit how dealers can collect, use, and share non-public personal information (PI) as well as credit information about a person.

Did You Know?

Federal law and regulations limit how dealers can collect, use, and share non-public personal information (PI) as well as credit information about a person.

A number of laws and regulations require that dealers disclose information collection and sharing practices to potential customers before they become customers (which occurs when they receive a financial product or service from the dealer), and to consumers (persons who provide information to seek but don't obtain a credit product) prior to the time the dealer intends to collect, use, or share their information.

For example, the California Consumer Privacy Act (CCPA) imposes significant responsibilities on businesses that collect California consumers' personal information. In addition, in November 2020, California passed the California Privacy Rights Act (CPRA), which amends the CCPA and went into effect on January 1, 2023, with a 12-month lookback for the personal information in scope.

Further, all 50 states and the District of Columbia now have data breach laws with which dealers must be familiar.

Finally, the FTC has brought hundreds of privacy-related enforcement proceedings over the past 15 years. More recently, the FTC has brought enforcement cases where companies have engaged in the collection and sharing of consumer data without consumers' consent, as well as cases against businesses that fail to adequately establish and maintain sufficient information security programs and controls to prevent breaches. This Topic discusses federal and state laws and regulations relating to customer information collection, use, and sharing, and the privacy of consumer data. As used here, the word "customer" will mean both consumers and customers unless otherwise stated.

Important State Laws and Regulations

The California Consumer Privacy Act (CCPA)

(The term "Consumer" as used within this section means a natural person who is a California resident and is different from the use of the term in context of obtaining or seeking credit).

The CCPA became effective January 1, 2020 and imposes obligations on covered businesses. A company is a covered business under CCPA if it:

- Operates as a for-profit entity;
- Collects California Consumers' personal information;
- Alone, or jointly with others, determines the purposes and means of processing Consumers' personal information; and
- Does business in California.

The company must also meet one of the following three threshold criteria:

- Has annual gross revenues in excess of $25,000,000; or
- Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more Consumers, households, or devices; or
- Derives 50% or more of its annual revenues from selling Consumers' personal information.

The CCPA imposes numerous privacy and data security obligations on covered businesses. These include providing additional rights to California Consumers over the collection and use of their personal information.

Did You Know?

The CCPA gave California consumers additional rights regarding the collection and use of their personal information.

The CCPA defines personal information as any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Consumer or household. Examples include, a name, alias, postal address, unique personal identifier, IP address, email address, account name, social security number, driver's license number, Internet activity, geolocation data and other similar identifiers. Publicly available information is not personal information under CCPA.

A business will need to be able to provide California Consumers notice of the following rights and the ability to fulfill requests to exercise these rights:

- Right to know what personal information is collected about them;
- Right to know how their personal information is being used;
- Right to access a copy of their personal information;
- Right to request that a business delete the personal information that was collected from them (subject to certain exceptions); and
- Right to say no to having their personal information sold to third-parties (known as the "Do Not Sell" right.)

A covered business must respond to a Consumer request within 45 days and provide the categories of PI collected, the categories of sources from which PI is collected, the business or commercial purpose for collecting PI, the categories of third parties with whom the business shares PI, and the specific pieces of PI the business collected about the Consumer in the 12 months preceding the request.

A key CCPA compliance challenge concerns the law's broad definition of the term "sell" and the numerous obligations that apply to sales of PI.

The definition of a sale under CCPA encompasses "releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." Note that disclosures to vendors that qualify as a "service provider" as defined by the CCPA are exempt from being a "sale." Under the CCPA covered businesses are required to provide enhanced notices to Consumers of their rights through an updated website privacy notice that includes the requisite CCPA disclosures (or a separate California notice). This notice must cover online and offline (in-person) personal information collection and use. In addition, a business must distribute an internal employee privacy notice that includes the requisite CCPA disclosures to all California employees.

Businesses may also need to provide in-store notices about PI collection practices.

Compliance Tip

Auto dealers subject to California law may need to provide in-store notices to consumers about their personal information collection practices.

This is because the CCPA requires covered businesses to provide a pre-collection notice to Consumers at or before the point and time their PI is collected. This pre-collection notice must inform Consumers of the categories of PI to be collected and the purposes for which the categories of PI will be used. Further, a business can't collect more PI than necessary, and must limit the use of PI to the stated purposes, absent further advance notice being provided. This requirement applies to online and offline personal information collection and sharing. Dealers may need to provide a just in time notice for Consumers who visit their facilities if CCPA PI is being collected.

A CCPA covered business must disclose the following information regarding their PI practices in their online privacy policy (or a separate online notice) and update that information at least once every 12 months.

Recommended Practice

Auto dealers should ensure that they update their online privacy policies at least annually.

Online privacy policies and any California-specific privacy notices must include:

- The categories of PI collected about a Consumer;
- The categories of sources from which PI is collected;
- The categories of third parties with whom the business shares PI;
- The business purpose or commercial purpose for collecting and for selling PI;
- The categories of Consumer PI sold (or if not sold, the notice must disclose that fact); and
- The categories of Consumer PI it has disclosed for a business purpose (or if not disclosed for a business purpose, the notice must disclose that fact).

In addition, California-specific privacy notices must include:

- A description of the Consumer's right to not be discriminated against for exercising their rights under the CCPA;
- A description of the Consumer's right to request that their PI collected by the business from the Consumer be deleted (subject to exceptions);
- The right of Consumers to opt out of having their PI sold (and a link to the businesses' "Do Not Sell My Personal Information" web-based opt-out tool);
- Notice of any financial incentives and a clear description of the material terms of any such program; and
- Two or more designated methods for submitting Consumer rights requests.

Covered businesses are also required to update their website homepage to provide a link to their CCPA notice and a "Do Not Sell" button (if applicable). Businesses should ensure that any account registration process directs California Consumers to the California privacy notice or otherwise informs them of their rights.

There are exceptions to the "Do Not Sell" right relevant for dealers to take into consideration. The "Do Not Sell" right does not apply to:

- Vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose;
- "Vehicle information" is the vehicle information number, make, model, year, and odometer reading; and
- "Ownership information" is the name or names of the registered owner or owners and the contact information for the owner or owners.

In addition, the CCPA does not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (except for in the case of a data breach).

Overall, businesses must accurately reflect their PI practices in any posted privacy notice, determine how to address consumer rights requests, and develop a process for fulfilling a request within the required timeframe.

California Privacy Rights Act (CPRA)

Overview:

The CPRA amended and expanded the CCPA in 2020 by adding consumer rights and additional obligations around Sensitive Personal Information (PI), Children's PI, and the sharing of PI. The CPRA officially replaced the CCPA on January 1, 2023. At a high level, the newly enacted CPRA moves California privacy law closer to the EU's GDPR by providing similar rights. However, the CPRA goes further than the GDPR in certain aspects, including through a broad definition of "share" that may capture many common business practices.

Like the CCPA, it applies to "consumers" — basically to anyone in California, and "personal information" (PI), applies to all "Businesses" that process over 100,000 California consumers' PI. While the CPRA went into effect on January 1, 2023, there is a 12-month lookback as to the PI in scope.

Enforcement:

Enforcement authority is vested both in a stand-alone, well-funded data protection authority agency called the California Privacy Protection Agency (CPPA),

Did You Know?

California is the only state that uses an entire state agency (the California Privacy Protection Agency) to enforce its data privacy and security laws.

as well as with the California Attorney General, thus increasing the likelihood of an enforcement action and the repercussions for non-compliance. CPRA also removes the obligation of the government to give notice and a 30-day opportunity to cure non-compliance; provided, however, that the CPPA will have the discretion to permit a one-time cure. There will also be increased penalties for non-compliance regarding children's PI.

Key Requirements:

The CPRA adds rights in addition to the above CCPA rights, which include the following:

1. New "Do Not Share" right;
   (share is broadly defined as "making available" certain PI)
   - This requires businesses to enable the opt-out of sharing of PI (in addition to selling); and
   - It requires a link on the business' homepage titled "Do Not Sell or Share My PI."
2. Right to opt-out of processing of "Sensitive Personal Information" (broadly defined);
   - This requires a link on the business' homepage titled "Limit the Use of My Sensitive PI" that businesses will need to effectuate.
3. Right to object to automated processing of PI (such as for profiling and/or targeted ads); and
4. Right to correction;
5. Right to know all PI collected in certain circumstances (not just in the past 12 months);
6. Right for employees and personnel to exercise privacy rights (which went into effect upon the expiration of the HR exemption on January 1, 2023).

In addition to the above rights, the CPRA has additional notice and disclosure obligations, including the following:

1. Disclosure of categories of Sensitive PI collected, the purposes for collection/use, and whether it is sold or shared;
2. Disclosure of PI retention periods for each category of PI in the notice at collection; and
3. Disclosure of commitment to maintain and use certain information in de-identified form.

Table of Contents

Similar to the CCPA, the CPRA will require company-wide compliance efforts and a detailed understanding of data handling practices. As such, business may consider taking a bifurcated approach: (1) continuing with CCPA compliance and tracking; and (2) creating an internal team to identify the gaps with CPRA.

Colorado Privacy Act (CPA)

Overview:
The CPA applies to entities that conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to residents of Colorado, and that satisfy one or both of the following thresholds:

1. During a calendar year, controls or processes personal data of 100,000 or more Colorado residents; or
2. Both derives revenue or receives discounts from selling personal data and processes or controls the personal data of 25,000 or more Colorado residents.

Enforcement :
The CPA is enforceable by Colorado's Attorney General and state district attorneys, subject to a 60-day cure period for any alleged violation until 2025. Under the CPA, consumers have no private right of action. Violations of the CPA are punishable by civil penalties of up to $20,000 per violation (with a "violation" measured per consumer and per transaction) with a maximum penalty of $500,000 for related violations. The Attorney General or district attorney may enforce the CPA by seeking injunctive relief.

Key Requirements:
The CPA grants certain rights to consumers, including:

1. Right to access;
2. Right to correct;
3. Right to deletion;
4. Right to data portability;
5. Right to opt-out of sale of personal data, targeted advertising, and profiling. Businesses must provide consumers with the option to opt out through a universal opt-out mechanism;
6. Right to opt-in to the processing of "sensitive" data. Businesses must obtain consent before processing "sensitive data," which includes children's data; genetic or biometric data used to uniquely identify a person; and personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; and
7. Right to appeal. Businesses must establish an internal appeals process for consumers when the business does not take action on a request.

Businesses must respond to consumer rights requests within 45 days, (which may be extended once for an additional 45-day period) if the business provides notice to the consumer explaining the reason for the delay.

The Connecticut Data Privacy Act (CTDPA)

Overview:
The CTDPA applies to entities that conduct business in Connecticut or produce products or services targeted to Connecticut residents, and who during the preceding calendar year either:

1. Controlled or processed the personal data of 100,000 or more consumers annually, except for personal data controlled or processed solely for the purpose of completing a payment transaction; or
2. Derived over 25 percent of their gross revenue from the sale of personal data and controlled or processed the personal data of 25,000 or more consumers.

The CTDPA contains numerous exemptions, including for personal data processed or maintained relating to job applicants, employees, and in the business-to-business context.

Enforcement:
The CTDPA does not provide a private right of action. Instead, the state's Attorney General has exclusive enforcement authority. Beginning January 1, 2025, the Attorney General will grant opportunities to cure alleged violations at the Attorney General's discretion, considering the following factors: (1) the number of violations, (2) the business' size and complexity, (3) the nature and extent of the processing, (4) the substantial likelihood of injury to the public, (5) the safety of persons or property and (6) whether the alleged violation was caused by a human or technical error.

Key Requirements:
The CTDPA grants certain rights to consumers, including:

1. Right to access. Consumers have the right to confirm whether a business is processing their personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in their personal data (with some limitation);
3. Right to delete. Consumers have the right to delete personal data provided by or about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible;
5. Right to opt-out of certain data processing. Consumers have the right to opt out of the processing of personal data for purposes of (a) targeted advertising, (b) the sale of personal data, or (c) profiling in connection with automated decisions that produce legal or similarly significant effects concerning the consumer;
6. Right to opt-in to the processing of "sensitive data." The CTDPA defines sensitive data as personal data that reveals (a) racial or ethnic origin, (b) religious beliefs, (c) mental or physical health condition or diagnosis, (d) sex life, (e) sexual orientation, (f) citizenship or immigration status, (g) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (h) children's data and (i) precise geolocation data; and
7. Right to appeal denials of consumer privacy requests.

Delaware Personal Data Privacy Act (DPDPA)

Overview:
Effective January 1, 2025, the DPDPA will provide consumers opt-out and other rights relating to their personal data. The DPDPA applies to entities that conduct business in Delaware or produce products or services targeted to Delaware residents and who during the preceding calendar year either:

1. Controlled or processed personal data of 35,000 or more Delaware residents, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
2. Controlled or processed personal data of 10,000 or more Delaware residents and derived more than 20% of their gross revenue from the sale of personal data.

The DPDPA contains numerous exemptions, including for certain types of entities (e.g., government entities and entities regulated by the Gramm-Leach-Bliley Act and certain other federal laws) and types of data (e.g., protected health information under HIPAA, data processed or maintained relating to job applicants and employees, personal motor vehicle records, and consumer credit-reporting data).

Enforcement:
The DPDPA is enforceable by the Delaware Department of Justice, subject to a 60-day cure period for any alleged violation until December 31, 2025. Under the DPDPA, consumers have no private right of action. Violations of the DPDPA are punishable by civil penalties of up to $10,000 per willful violation.

Key Requirements:
The DPDPA grants certain rights to consumers, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data provided by or obtained about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible;
5. Right to obtain a list of the categories of third parties to which the consumer's personal data has been disclosed;
6. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects;
7. Right to appeal denials of consumer privacy requests; and
8. Businesses must respond to consumer rights requests within 45 days, which may be extended for an additional 45-day period.

Florida Digital Bill of Rights (FDBR)

Overview:
The FDBR provides consumers opt-out and other rights relating to their personal data. The FDBR applies to entities that conduct business in Florida, collect personal data from consumers, have an annual global revenue of more than $1 billion, and meet one of the following criteria:

1. Derive 50% of their global gross annual revenue from the sale of advertisements online;
2. Operate a consumer smart speaker and voice command service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation; or
3. Operate an app store or digital distribution platform with at least 250,000 different software applications for consumers to download and install.

The FDBR contains numerous exemptions, including for certain types of entities (e.g., government entities, nonprofits, entities regulated by the Gramm-Leach-Bliley Act or HIPAA and other federal laws, and postsecondary education institutions) and certain types of data (e.g., protected health information under HIPAA, consumer credit-reporting data, personal motor vehicle records, insurance data, data processed or maintained relating to job applicants and employees, and personal data collected and transmitted for the sole purpose of facilitating payment processing for the purchase of products or service).

Enforcement:
The FDBR is enforceable by the Florida Department of Legal Affairs and is generally subject to a 45-day cure period. Under the FDBR, consumers have no private right of action. Violations of the FDBR are punishable by civil penalties of up to $50,000 per violation.

Key Requirements:
The FDBR grants certain rights to consumers, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data provided by or obtained about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible;

Table of Contents

5. Right to opt-out of sale of personal data, targeted advertising, and profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer;
6. Right to opt-out of the collection or processing of "sensitive data," including precise geolocation data;
7. Right to opt-out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature; and
8. Right to appeal denials of consumer privacy requests.

The FDBR also contains protections for children on online platforms and restrictions on government officials moderating content.

Indiana Data Privacy Law (Indiana DPL)

Overview:
Effective January 1, 2025, the Indiana DPL provides consumers opt-out and other rights relating to their personal data. The Indiana DPL applies to entities that conduct business in Indiana or produce products or services that are targeted to the residents of Indiana and, during a calendar year, either:

1. Control or process personal data of 100,000 or more Indiana residents; or
2. Control or process personal data of 25,000 or more Indiana residents and derive over 50% of their gross revenue from the sale of personal data.

The Indiana DPL contains numerous exemptions, including for certain types of entities (e.g., government entities, entities regulated by the Gramm-Leach-Bliley Act or HIPAA, nonprofit organization, institutions of higher education, and public utilities) and certain types of data (e.g., protected health information under HIPAA, consumer credit-reporting data, personal motor vehicle records, and data processed or maintained relating to job applicants and employees).

Enforcement:
The Indiana DPL is enforceable by the Indiana Office of the Attorney General, subject to a 30-day cure period. Under the Indiana DPL, consumers have no private right of action. Violations of the Indiana DPL are punishable by civil penalties of up to $7,500 per violation, and the Attorney General may also seek injunctive relief.

Key Requirements:
The Indiana DPL grants certain rights to consumers, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and to access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to request that the controller delete personal data provided by or obtained about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible;
5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer; and
6. Right to appeal denials of consumer privacy requests.

Businesses must respond to consumer rights requests within 45 days, which may be extended for a single 45-day period.

Iowa Data Privacy Law (Iowa DPL)

Overview:
The Iowa DPL, which goes into effect on January 1, 2025, provides requirements and rights substantially similar to those of other states' privacy laws. It applies to entities that conduct business in Iowa or produce products or services for Iowa residents and, during a calendar year, that either:

Table of Contents

1. Control or process personal data of 100,000 or more Iowa residents; or
2. Control or process personal data of at least 25,000 Iowa residents and derive over 50% of their gross revenue from the sale of personal data.

The Iowa DPL contains numerous exemptions, including for certain types of entities (e.g., government entities, nonprofit organizations, institutions of higher education, and entities regulated by the Gramm-Leach-Bliley Act and HIPAA) and certain types of data (e.g., protected health information under HIPAA, consumer credit-reporting data, personal motor vehicle records, and data processed or maintained relating to job applicants and employees).

Enforcement:
The Iowa DPL, which includes a 90-day cure period, is enforced by the Iowa Attorney General. Under the Iowa DPL, consumers have no private right of action. Violations of the Iowa DPL are punishable by civil penalties of up to $7,500 per violation, and the Attorney General may also seek injunctive relief.

Key Requirements:
The Iowa DPL grants certain rights to consumers, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and to access such personal data;
2. Right to deletion. Consumers have the right to request that the controller delete personal data provided by or obtained about the consumer;
3. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically practicable; and
4. Right to opt-out of the sale of personal data.

Businesses must respond to consumer rights requests within 45 days, which may be extended for a single 45-day period.

Kentucky Consumer Data Protection Act (KCDPA)

Overview:
Effective January 1, 2026, the KCDPA applies to companies that conduct business in Kentucky or produce products or services targeted to Kentucky residents, and that satisfy one or both of the following thresholds:

1. Control or process personal data of at least 100,000 consumers per calendar year; or
2. Control or process the personal data of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of that data.

Enforcement:
Kentucky's Attorney General has exclusive civil enforcement authority for the KCDPA. The Kentucky Attorney General provides businesses with a 30-day cure period. Consequences for noncompliance with the KCDPA include civil penalties up to $7,500 per violation.

The KCDPA does not provide a private right of action.

Key Requirements:
The KCDPA establishes a number of consumer rights, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible; and

5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Businesses must respond to consumer rights requests within 45 days, which may be extended for a single 45-day period.

Maryland Online Data Privacy Act (MODPA)

Overview:
Effective October 1, 2025, the MODPA applies to businesses that conduct business in Maryland or produce products or services targeted to Maryland residents, and that satisfy one or both of the following thresholds:

1. In the preceding calendar year, controlled or processed personal data of at least 35,000 consumers; or
2. Controlled or processed the personal data of at least 10,000 consumers and derived more than 20% of gross revenue from the sale of that data.

Enforcement:
Maryland's Attorney General has exclusive authority to enforce the MODPA. The MODPA does not specify a private right of action, but also does not preclude consumers from "pursuing any other remedy provided by law." The Maryland Attorney General may at its sole discretion determine whether to grant a 60-day opportunity to cure to companies in consideration of several factors, but only until April 1, 2027.

A violation under MODPA constitutes an unfair, abusive, or deceptive trade practice under Maryland's Consumer Protection Act.

Key Requirements:
The MODPA establishes a number of consumer rights, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data.
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible; and
5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Businesses must respond to consumer rights requests within 45 days, which may be extended for a single 45-day period.

Minnesota Consumer Data Privacy Act (MCDPA)

Overview:
Effective July 31, 2025, the MCDPA applies to companies that conduct business in Minnesota or produce products or services targeted to Minnesota residents, and that satisfy one or both of the following thresholds:

1. During a calendar year, control or process personal data of at least 100,000 consumers (excluding solely for the purpose of completing a payment transaction); or
2. Process the personal data of at least 25,000 consumers and derive more than 25% of gross revenue from the sale of that data.

Enforcement:
Minnesota's Attorney General has exclusive authority to enforce the MCDPA. The MCDPA does not provide a private right of action. Companies have a 30-day period to cure violations before being penalized. This right to an opportunity to cure expires January 31, 2026. Consequences for noncompliance with the MCDPA include:

1. Civil penalties of up to $7,500 per violation;

2. For willful or knowing violations, treble damages; and
3. Reasonable expenses, including attorneys' fees.

Key Requirements:
The MCDPA establishes a number of consumer rights, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible; and
5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Businesses must respond to consumer rights requests within 45 days, which may be extended for a single 45-day period.

Montana Consumer Data Privacy Act (MCDPA)

Overview:
The MCDPA provides consumers opt-out and other rights relating to their personal data. The MCDPA applies to entities that conduct business in Montana or produce products or services targeted to Montana residents and either:

1. Control or process personal data of 50,000 or more Montana residents, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
2. Control or process personal data of 25,000 or more Montana residents and derive more than 25% of their gross revenue from the sale of personal data.

The MCDPA contains numerous exemptions, including for certain types of entities (e.g., government entities, nonprofit organizations, institutions of higher education, and entities regulated by the Gramm-Leach-Bliley Act and HIPAA) and certain types of data (e.g., protected health information under HIPAA, consumer credit-reporting data, personal motor vehicle records, and data processed or maintained relating to job applicants and employees).

Enforcement:
The MCDPA is enforceable by the Montana Office of the Attorney General, subject to a 60-day cure period until April 1, 2026. Under the MCDPA, consumers have no private right of action. The MCDPA does not specify a penalty amount for violations.

Key Requirements:
The MCDPA grants certain rights to consumers, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible;
5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer; and
6. Right to appeal denials of consumer privacy requests.

Table of Contents

Businesses must respond to consumer rights requests within 45 days, which may be extended for an additional 45-day period.

Nebraska Data Privacy Act (NDPA)

Overview:
Effective January 1, 2025, the NDPA applies to companies that conduct business in Nebraska or process or engage in the sale of personal data.

Enforcement:
Attorney General has exclusive authority to enforce the NDPA. The NDPA does not provide a private right of action. Nebraska's companies have a 30-day period to cure violations before being penalized. Consequences for noncompliance with the NDPA include:

1. Civil penalties of up to $7,500 per violation;
2. For willful or knowing violations, treble damages; and
3. Reasonable expenses, including attorneys' fees.

Key Requirements:
The NDPA establishes a number of consumer rights, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible; and
5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Businesses must respond to consumer rights requests within 45 days, which may be extended for a single 45-day period.

New Hampshire Data Privacy Act (NHDPA)

Overview:
Effective January 1, 2025, the NHDPA applies to companies that conduct business in New Hampshire or produce products or services targeted to New Hampshire residents, and that satisfy one or both of the following thresholds:

1. During a one-year period, control or process the personal data of at least 35,000 customers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
2. Control or process the personal data of at least 10,000 customers and derive more than 25% of gross revenue from the sale of that data.

Enforcement:
New Hampshire's Attorney General has exclusive authority to enforce the NHDPA. The NHDPA does not provide a private right of action. The New Hampshire Secretary of State has narrow rulemaking authority under the NHDPA to establish privacy notice requirements. Companies have a 60-day period to cure violations before being penalized, but only until January 1, 2026, after which the Attorney General may at its sole discretion determine whether to grant an opportunity to cure in consideration of several factors.

A violation under NHDPA constitutes an unfair method of competition or an unfair or deceptive act or practice under New Hampshire's Consumer Protection Act.

Key Requirements:
The NHDPA establishes a number of consumer rights, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct

Table of Contents

inaccuracies in the consumer's personal data;

3. Right to deletion. Consumers have the right to delete personal data about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible;
5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer; and
6. Businesses must respond to consumer rights requests within 45 days, which may be extended for a single 45-day period.

New Jersey Data Protection Act (NJDPA)

Overview:

Effective January 15, 2025, the NJDPA applies to companies that conduct business in New Jersey or produce products or services targeted to New Jersey residents, and that satisfy one or both of the following thresholds:

1. Control or process the personal data of at least 100,000 customers (excluding personal data controlled or processed solely for the purpose of completing a payment transaction); or
2. Control or process the personal data of at least 25,000 customers and derive revenue or receive a discount on the price of any goods or services, rom the sale of personal data.

Enforcement:

The NJDPA empowers the NJ Division of Consumer Affairs to issue regulations related to this law. The NJPDA does not provide a private right of action, with the New Jersey Attorney General retaining exclusive authority to enforce the NJDPA. Companies have a 30-day period to cure violations before being penalized, but only until July 15, 2026. A violation under NJDPA constitutes an unlawful practice under New Jersey's Consumer Fraud Act, which provides for civil fines of up to $10,000 for an initial violation and up to $20,000 for subsequent violations.

Key Requirements:

The NJDPA establishes a number of consumer rights, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible; and
5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

Businesses must respond to consumer rights requests within 45 days, which may be extended for a single 45-day period.

Oregon Consumer Privacy Act (OCPA)

Overview:

The OCPA provides consumers opt-out and other rights relating to their personal data. The OCPA applies to entities that conduct business in Oregon or produce products or services targeted to Oregon residents and who during a calendar year either:

1. Control or process personal data of 100,000 or more Oregon residents, other than personal data controlled or processed solely for the purpose of completing a payment transaction; or
2. Control or process personal data of 25,000 or more Oregon residents and derive more than 25% of their gross revenuefrom the sale of personal data.

The OCPA contains numerous exemptions, including for certain types of entities (e.g., government entities and certain financial institutions) and certain types of data (e.g., information collected, processed, sold or disclosed in accordance with the Gramm-Leach-Bliley Act and certain other federal laws, protected health information under HIPAA, data processed or maintained relating to job applicants and employees, personal motor vehicle records, and consumer credit-reporting data).

Enforcement:
The OCPA is enforceable by the Oregon Office of the Attorney General, subject to a 30-day cure period until January 1, 2026. Under the OCPA, consumers have no private right of action. Violations of the OCPA are punishable by civil penalties of up to $7,500 per violation, and the Attorney general may also seek injunctive relief.

Key Requirements:
The OCPA grants certain rights to consumers, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data provided by or obtained about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible;
5. Right to obtain a list of third parties to whom the consumer's personal data or, at the business's discretion, any consumer's personal data has been disclosed;
6. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of decisions that produce legal effects or effects of similar significance;
7. Right to revoke a previously given consent to process the consumer's personal data, which must be honored within 15 days of receiving the request; and
8. Right to appeal denials of consumer privacy requests.

Businesses must respond to consumer rights requests within 45 days, which may be extended for an additional 45-day period.

Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)

Overview:
Effective January 1, 2026, the RIDTPPA applies to companies that conduct business in Rhode Island or produce products or services targeted to Rhode Island residents and that satisfy one or both of the following thresholds:

1. Control or process the personal data of at least 35,000 customers, excluding solely for the purpose of completing a payment transaction; or
2. Control or process the personal data of at least 10,000 customers and derive more than 20% of gross revenue from the sale of that data.

Enforcement:
The RIDTPPA does not provide a private right of action. Rhode Island's Attorney General has exclusive authority to enforce the RIDTPPA. Consequences for noncompliance with the RIDTPPA include civil penalties between $100 to $500 per disclosure for each intentional disclosure in violation.

Key Requirements:
The RIDTPPA establishes a number of consumer rights, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;

Table of Contents

3. Right to deletion. Consumers have the right to delete personal data about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible;
5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer; and
6. Businesses must respond to consumer rights requests within 45 days, which may be extended for a single 45-day period.

Tennessee Information Protection Act (TIPA)

Overview:
Effective July 1, 2025, the TIPA will provide consumers opt-out and other rights relating to their personal data. The TIPA applies to entities that conduct business in Tennessee by producing products or services that are targeted to the residents of Tennessee and meet the following criteria:

1. Have $25 million or more in revenue; and
2. Either (A) control or process personal information of 25,000 or more Tennessee residents and derive more than 50% of gross revenue from the sale of personal information, or (B) during a calendar year, control or process personal information of 175,000 or more Tennessee residents.

The TIPA contains numerous exemptions, including for types of entities (e.g., government entities, certain insurers, entities regulated by the Gramm-Leach-Bliley Ac or HIPAA, nonprofit organizations, and institutions of higher education) and certain types of data (e.g., protected health information under HIPAA, consumer credit-reporting data, personal motor vehicle records, and data processed or maintained relating to job applicants and employees).

Enforcement:
The TIPA is enforceable by the Tennessee Attorney General, after issuing a notice and subject to a 60-day cure period. Under the TIPA, consumers have no private right of action. Violations of the TIPA are punishable by civil penalties of up to $7,500 per violation and treble damages for willful or knowing violations, and the Attorney general can also seek a declaratory judgement and injunctive relief.

Key Requirements:
The TIPA grants certain rights to consumers, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data provided by or obtained about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible;
5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer; and
6. Right to appeal denials of consumer privacy requests.

Businesses must respond to consumer rights requests within 45 days, which may be extended for a single additional 45-day period.

Texas Data Privacy and Security Act (TDPSA)

Overview:
The TDPSA provides consumers opt-out and other rights relating to their personal data. The TDPSA applies to entities that conduct business in Texas or produce products or services consumed by residents of the state, process or engage in the sale of personal data, and are not a small business, as defined by the U.S. Small Business Administration. The TDPSA contains numerous exemptions, including for types of entities

(e.g., government entities, entities regulated by the Gramm-Leach-Bliley Act or HIPAA, nonprofit organizations, institutions of higher education, and public utilities) and certain types of data (e.g., protected health information under HIPAA, consumer credit-reporting data, personal motor vehicle records, and data processed or maintained relating to job applicants and employees).

Enforcement:
The TDPSA is enforceable by the Texas Attorney General, after providing notice of a violation and subject to a 30-day cure period. Under the TDPSA, consumers have no private right of action. Violations of the TDPSA are punishable by civil penalties of up to $7,500 per violation and treble damages for willful or knowing violations, and the Attorney General can also seek injunctive relief.

Key Requirements:
The TDPSA grants certain rights to consumers, including:

1. Right to access. Consumers have a right to confirm whether a business is processing the consumer's personal data and access such personal data;
2. Right to correct. Consumers have the right to correct inaccuracies in the consumer's personal data;
3. Right to deletion. Consumers have the right to delete personal data provided by or obtained about the consumer;
4. Right to data portability. Consumers have the right to obtain a portable copy of their personal data to the extent technically feasible;
5. Right to opt-out of the sale of personal data, targeted advertising, and profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer; and
6. Right to appeal denials of consumer privacy requests.

Businesses must respond to consumer rights requests within 45 days, which may be extended for an additional 45-day period.

Utah Consumer Privacy Act (UCPA)

Overview:
The UCPA applies to entities that (1) conduct business in Utah or target products and services to consumers who are residents of the state, (2) have annual revenues of at least $25 million, and (3) meet one of two threshold requirements:

1. Annually control or process the personal data of 100,000 or more Utah residents; or
2. Derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of 25,000 or more consumers.

The UCPA applies only to consumer data and expressly excludes personal data collected in an employment or business-to-business context.

Enforcement:
The Utah Division of Consumer Protection may investigate consumer complaints under the UCPA and refer complaints to the Attorney General, who has exclusive enforcement authority. The Attorney General must provide businesses with written notice of an alleged violation and a 30-day opportunity to cure. The Attorney General may bring an action for uncured violations and recover actual damages to the consumer and $7,500 per violation in civil penalties. There is no private right of action under the UCPA.

Key Requirements:
The UCPA grants certain rights to consumers, including:

1. Right to access the personal data that a business processes about them;
2. Right to delete personal data that the consumer provided to the business;
3. Right to obtain a copy of the personal data, in a portable format, that the consumer provided to the business;

4. Right to opt out of the sale of personal data or processing of personal data for targeted advertising; and
5. Right to opt out of the processing of sensitive data, which includes information about racial or ethnic origin, religious beliefs, sexual orientation, citizenship or immigration status, health and medical treatment or conditions, biometric or genetic data used to identify individuals, and geolocation data.

Businesses have 45 days to respond to a request, with a 45-day extension if reasonably necessary. While businesses must handle requests free, they may charge a fee for second or subsequent requests in a 12-month period, or if certain other circumstances apply (e.g., the request poses an undue burden on the business's resources).

Virginia Consumer Data Protection Act (VCDPA)

Overview:
The VCDPA applies to entities that conduct business in Virginia or produce products or services that are targeted to residents of Virginia, and meet one of the following thresholds:

1. During a calendar year, control or process the personal data of 100,000 or more Virginia residents; or
2. Control or process the personal data of at least 25,000 consumers, while deriving over 50 percent of gross revenue from the sale of that data.

Enforcement:
The Virginia Attorney General will enforce the VCDPA by bringing an action in the name of the state, or on behalf of persons residing in the state. The Attorney General also has the power to issue a civil investigative demand to any data controller or processor believed to be engaged in, or about to engage in, any violation of the VCDPA. Any business that violates the VCDPA is subject to an injunction and liable for a civil penalty of $7,500 for each violation. The Attorney General may also recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, of any action initiated under the VCDPA.

Key Requirements:
The VCDPA grants certain rights to consumers, including:

1. Right to access their personal data;
2. Right to correct their personal data;
3. Right to request deletion of their personal data;
4. Right to obtain a copy of their personal data in a portable and easily accessible format;
5. Right to opt-out of the processing of their personal data for the purpose of targeted advertising;
6. Right to opt-out of the processing of their personal data for the purpose of profiling;
7. Right to opt-out of the sale of their personal data;
8. Right to non-discrimination for exercising rights; and
9. Right to submit a complaint about rights violations.

Important Federal Laws and Regulations

The Fair Credit Reporting Act (FCRA)

The FCRA requires a dealer to have a "permissible purpose" to access a customer's credit report or credit score.

Recommended Practice

Ensure you have proof of 'permissible purpose' to access a customer's credit report or credit score.

The FCRA also contains restrictions on sharing and using customer credit and consumer report information with both affiliated and non-affiliated companies. It requires notices to be given to customers about certain information sharing with affiliates (FCRA Privacy Notices)

and in certain cases, requires giving consumers the right to opt-out of any sharing. FCRA Privacy Notices are typically combined with privacy notices required by the Gramm-Leach-Bliley Act (GLBA) into one comprehensive privacy notice for the dealership (FCRA-GLBA Privacy Notice). See "FCRA-GLBA Privacy Notice Forms" below. The FCRA categorizes consumer credit information into two types:

1. "Transaction and experience" information: the dealer's own experience with the customer such as a customer's payment history on any credit account (for example, a service department "house" account or a customer's payment history for a buy-here-pay-here dealer account), name, address, and phone number would be a species of transaction and experience information; and
2. "Other" information: essentially anything obtained from a credit report, a credit score, or credit information about the consumer obtained from a third party (credit information).

Under the FCRA, dealers can share vehicle purchase- or lease- transaction and/or experience information with affiliates, such as sister dealerships, insurance affiliates, or a parent company, without offering an opt-out. Subject to any contractual limitations in a contract with the consumer reporting agency that provided the "credit information," dealers may share "credit information" with affiliates only if they offer consumers the opportunity to opt out of sharing that "credit information." Further, the affiliates' use of the shared information is subject to the requirements of the Affiliate Marketing Rule discussed below. The Affiliate Marketing Rule applies to all marketing based on affiliate sharing of customer information, both transaction and experience information and credit information. So, while a consumer cannot prevent sharing of transaction and experience information with a dealer's affiliates, he or she can opt out of affiliates using that information to market to them.

Dealers may share transaction and experience information with non-affiliates (unrelated companies such as sellers of non-automobile products, realtors, charities, or local merchant associations) only if the customer is given an FCRA-GLBA Privacy Notice describing the right to opt out of non-affiliate sharing of transaction and experience information, the consumer is given a reasonable opportunity to opt out, and the customer fails to opt out.

Whenever the FCRA or GLBA gives the customer the right to opt out of data sharing, the FTC has said the dealer must wait 30 days from giving the customer a privacy notice before beginning to share information. This is so the customer has time to decide whether or not to opt out up front. The 30-day rule does not apply if the customer has no right of opt out, such as when a third party is acting only as a service provider to the dealer for the customer's transaction or a joint marketer as discussed below. However, the third parties receiving such information under either the service provider or joint marketing exceptions are prohibited from using or disclosing the information for any purpose other than the one for which it was received. A dealer's disclosures to service providers and joint marketers must be stated in the FCRA-GLBA Privacy Notice.

The Gramm-Leach-Bliley Act (GLBA) and the FTC Privacy Rule (Privacy Rule)

GLBA and the FTC Privacy Rule, which implements the privacy provisions of the GLBA, provide consumers with protections on how creditors are permitted to collect, use, and share their nonpublic personal information (NPI). NPI is essentially any identifying information a dealer obtains from or about a customer in connection with a possible credit transaction. **GLBA and the Privacy Rule also require giving customers privacy notices (GLBA Privacy Notices) describing how a creditor collects, uses, and shares NPI, and giving customers rights to opt out of certain types of sharing.**

Did You Know?

GLBA and the FTC requires giving privacy notices describing how a creditor collects, uses, and shares nonpublic personal information, and gives customers rights to opt out of information sharing.

An exception to the right to opt out of third-party sharing applies and permits sharing with service providers and for joint marketing agreements with other financial companies under which the dealer and another financial

institution jointly market a different credit product such as a credit card. It is important to note that automotive dealers may often fall within the definition of a financial institution under GLBA to the extent they help consumers purchase vehicles through financing and leasing transactions.

Some states have specific requirements as well. A few examples include in Vermont, where consumers must affirmatively opt-in to both affiliate and non-affiliate sharing, and in California, where consumers must opt in before their information can be shared with a nonaffiliated third party. Note that the CCPA does not apply to personal information otherwise covered by GLBA or FCRA. This list is not exhaustive, and prior to collecting, processing, and sharing, dealers will want to consult with their local counsel.

Intersection of GLBA and CCPA

As mentioned, a large portion of the personal information collected and processed by financial institutions will be out of scope for CCPA as it falls under GLBA. The CCPA exempts information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA) and implementing regulations. It is important to note that GLBA-regulated entities are not wholly exempt from CCPA. However, the personal information collected that falls within the scope of the GLBA (or NPI) is exempt from the CCPA. For example, personal information from an individual who is not obtaining financial products or services from a financial institution, or PI that will not be used primarily for personal, family, or household purposes (such as personal information collected for targeted marketing or from a commercial client, employee, or applicant) is certainly within the scope of the CCPA.

FTC Affiliate Marketing Rule

The Affiliate Marketing Rule is an FTC regulation published pursuant to the 2003 Fair and Accurate Credit Transactions Act (FACT Act). The Affiliate Marketing Rule (AMR) prohibits a person from using consumer eligibility information received from a corporate affiliate for marketing purposes unless:

- The consumer is given a clear, conspicuous, concise written notice explaining that the person may use eligibility information about that consumer received from an affiliate to make solicitations for marketing purposes;
- The consumer is first given a reasonable opportunity and a reasonable and simple method to "opt-out," or prohibit the use of the eligibility information to make solicitations for marketing purposes; or
- The consumer has not opted out.

For purposes of the AMR, "eligibility information" means any information that if communicated, would constitute a "consumer report" as defined under the FCRA.

So, if your dealership has affiliated dealerships, insurance companies, other companies, or even a parent dealership group, the dealer must give its customers the right to opt out of the affiliates' use of any shared "eligibility" information (NPI combined with transaction and experience or credit information) to market to them.

Compliance Tip

Make sure you give your customers an option to opt out of your affiliates' use of any shared eligibility information.

The AMR notice can either be included in the dealer's FCRA-GLBA Privacy Notice or be given separately. If you use a separate Affiliate Marketing notice (such as the model "safe harbor" notice published by the FTC with the Affiliate Marketing Rule), you only need to give the Affiliate Marketing notice once every five years, not every year, as you must do for FCRA-GLBA Privacy Notices for as long as the consumer remains a customer and so long as your practices do not change. However, for consistency, it is a best practice to include the Affiliate Marketing notice in your FCRA-GLBA Privacy Notice.

Sample FCRA-GLBA Privacy forms are provided below for your review.
https://www.consumerfinance.gov/compliance/compliance-resources/other-applicable-requirements/privacy-notices/model-privacy-form/
The Affiliate Marketing Rule contains greater potential liability than does

the Gramm-Leach-Bliley Act (GLBA) with respect to customer privacy rights. While the FTC and state regulators can bring enforcement actions for failing to provide GLBA Privacy Notices, customers cannot sue directly under GLBA. However, the Affiliate Marketing Rule notice gives a customer the right to bring a lawsuit under the FCRA for any violation of the Affiliate Marketing Rule, including the right to bring a class action. Remedies include the possible recovery of up to $1,000 per violation plus attorney's fees and unlimited punitive damages for each willful violation, with presumably every individual solicitation by an affiliate being a separate violation. You, the dealer, are at risk if you fail to give the Affiliate Marketing Rule Privacy Notice or if your affiliate markets to a consumer who has opted out of affiliate marketing under this Rule.

You should consult with your attorney to ensure that your AMR notice complies with applicable law.

FCRA-GLBA Privacy Notice Forms

The Privacy Rule enables a dealer to give one privacy notice to cover the GLBA and FCRA requirements and opt-out provisions, as well as the Affiliate Marketing Rule notice requirements. **It is a recommended practice to give this FCRA-GLBA privacy notice to customers when first taking their personal information for credit (such as when they fill out a credit application or respond to an online solicitation).**

Recommended Practice

> Provide a FRCA-GLBA privacy notice to customers when you first take their personal information for credit purposes.

If a dealer maintains a credit relationship with a customer (e.g., a buy-here-pay-here dealer), the dealer must give another privacy notice to the customer annually during the term of the credit relationship. It is also a recommended practice to post the privacy notice on the dealership's website as well as to deliver a copy to consumers who come into your stores.

The FCRA-GLBA Privacy Notice should describe how the dealer collects, uses, and shares customer NPI, including information about former customers. The FCRA requires that the privacy notice must also give the customer the right to opt out of sharing credit information with affiliates and GLBA requires the right of opt out for transaction and experience information with non-affiliated third parties. A dealer can share customer information with service providers or financial institutions that are joint marketers (entities with which you share information solely to jointly market the financial product like a credit card, and for no other purpose); this is permitted by the FCRA and GLBA provided the dealer discloses this sharing to the customer in its FCRA-GLBA Privacy Notice.

The FTC and banking regulators have published model "safe harbor" FCRA-GLBA Privacy Notices written in plain English using column formats. There are six alternative forms a dealer can use, depending on whether it shares information, whether it includes the Affiliate Marketing Rule notice, and how it allows customers to opt out. Four of the six forms can be printed on the front and back side of a single sheet of 8.5 x 11-inch paper; the remaining two forms require 8.5 x 14-inch paper or two sheets of 8.5 x 11-inch paper. Using one of these six forms will provide a "safe harbor" from liability for an inadequate privacy notice. The FTC has established a page on its website to construct such a privacy notice (see references at the end of this Topic). A sample of Form 1 of the "safe harbor" notice is contained at the end of this Topic. If you have an ongoing relationship with a customer (i.e., a buy-here-pay-here) and you are sharing information, you should give an annual GLBA notice, unless you are sharing under one of the exceptions.

Certain state laws also require additional disclosures to be in privacy notices (for example, California, Nevada, and Vermont) and dealers should be aware of such state requirements. Dealers with consumers in those states should add additional disclosure language in their privacy notices.

In California, privacy notices are required to include certain disclosures in addition to the new requirements under CCPA discussed above. California's Online Privacy Protection Act ("CalOPPA") requires a person or entity that collects personal information from California residents for commercial purposes, to post a privacy policy and to comply with that policy. The law

also requires that the privacy policy disclose the categories of personal information collected and the third parties that may receive the personal information. It further obligates websites or online services ("publishers") collecting personal information to disclose how it responds to browser "Do Not Track" (DNT) signals or other consumer choice mechanisms for personal information collected over time and across third-party websites or online services. However, the law does not mandate that publishers honor or provide a specific DNT signal response. In addition, the law requires publishers to disclose whether third parties may associate tracking devices with the publisher's service that collect information about a visitor's online activities over time and across different services (e.g., other websites).

Beyond tracking and targeting disclosures, if a dealer wants to share a California customer's (note that the term customer here is defined as an individual buying or seeking household goods or services) personal information (broadly defined) with a third party (including, in most cases, affiliates) for the third party's own direct marketing purposes, then California's Shine the Light law will also apply. California's Shine the Light law requires businesses to provide customers with information regarding how and with whom their personal information is shared for third party direct marketing purposes or provide customers with the ability to opt-in or opt-out of such sharing.

Of course, the dealer's information collection, sharing, and use practices must always be consistent with what is disclosed in its privacy notices. The FTC has brought enforcement proceedings for deceptive trade practices against numerous companies including an auto dealer that did not follow the practices described in their privacy notices.

As noted above, for all privacy notices, whenever a customer has a right to opt out, you can't begin sharing their information until at least 30 days after the date you give them the privacy notice.

Did You Know?

The FTC requires you to wait 30 days before sharing a customer's information if the customer has not opted out after receiving a privacy notice.

The FTC has ruled the customer must have at least 30 days to consider whether or not they want to opt out and this 30-day waiting period applies to all opt-outs. The FCRA-GLBA Privacy Notice should give the customer a toll-free phone number, website address, or mailing address to exercise their opt-out rights. Only if the customer fails to opt out during those 30 days may information sharing for the disclosed purposes subject to the opt out thereafter begin. If a customer opts out after the initial 30-day period, promptly remove them at that time from common databases or information that is stored and recall their information from persons you have shared it with, if possible. Reserve the right to do so in your information-sharing agreements.

Additionally, courts and the FTC have ruled that privacy notices are binding contracts between a company and its customers, so a dealership's business practices must follow what is stated in its privacy notice.

Compliance Tip

A privacy notice is considered a contract with your customers, so make sure your dealership's business practices follow what is stated in your privacy notice.

The FTC has brought deceptive trade practice enforcement proceedings against companies that violated statements contained in their own privacy notices such as "we will never share any of your personal information." These proceedings show the importance of writing privacy notices using language in the present tense and not the future tense. Reserve the right to amend your privacy notice by giving the customer a revision or informing the customer that a revised privacy notice has been posted to your website. Always date your privacy notices.

The FCRA, as amended by the FACT Act and implementing regulations, contains additional privacy provisions. For example, if a dealer accepts credit or debit cards, any electronically printed card receipt that is given to the customer must truncate all but the last five digits of the card number and cannot show the card expiration date. If not, class action liability can result. Damages for doing so are $100 to $1,000 per receipt for willful violations (generally a knowing or reckless violation) with no cap on damages in a class action. MasterCard and Visa can also assess fines starting at $5,000 for the first violation and going up from there. Make sure your card processing machines are set up to not print any more than the last five numbers and do not print the card's expiration date as this has been a source of many class actions.

A dealer is also required to give identity theft victims copies of transaction documents used in connection with any identity theft incident involving the use of their identity at the dealership if the customer provides sufficient proof of their legitimate identity. Social Security numbers should also be truncated to only the last four digits on printed documents to comply with many state laws.

Other than providing consumers the opportunity to "opt out" of certain kinds of data sharing, privacy notices are not negotiable

Did You Know?

Privacy notices are not negotiable and should not be negotiated with any customer, even if the customer refuses to sign them.

and should not be negotiated with any customer, even if the customer refuses to sign the privacy notice (a customer's signature on a privacy notice is not required). The privacy notice is a statement of the dealer's privacy practices applicable to all its customers and changing it for any customer will create an impossible situation to monitor and comply. You should use one of the federal "safe harbor" FCRA-GLBA Privacy Notice forms, and the customer's signature, while a good practice to get, is not legally required.

Driver's Privacy Protection Act (DPPA)

The DPPA is a federal law restricting the release and use of personal information from state motor vehicle records. "Personal information" means information identifying an individual such as a photograph, Social Security number, or driver's license number. In general, dealers can use personal information from motor vehicle records only for limited purposes such as to verify the accuracy of information the customer provides to the dealership after obtaining the consumer's written consent to the dealer to obtain that information. The DPPA makes it illegal to obtain drivers' information for unlawful purposes or to make false representations to obtain such information. The DPPA establishes criminal fines for noncompliance, and a civil cause of action for drivers against those who unlawfully obtain their information.

Tracking Customers on the Internet

No federal law or regulation directly prohibits the use of "cookies" to track consumer behavior on a dealer's website or to track the customer's linking or proceeding to other websites after leaving the dealer's site.

However, the FTC issued its final Privacy Report in March 2012, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, indicating that Web tracking should be subject to a "Do Not Track" mechanism. The FTC has stated its support of an initiative of the Better Business Bureau in association with media and marketing companies to get companies that track consumer Web behavior to adopt a self-regulatory program that will give consumers enhanced control over the collection and use of data regarding their Web viewing for online behavioral advertising purposes. The FTC's Self-Regulatory Principles for Online Behavioral Advertising, initially published in 2009, have been adopted by many companies that track online behavior and represent a "best practice for disclosing the nature of their Web tracking and giving the consumer an opportunity to opt out." An Advertising Option Icon and accompanying language have been adopted to be displayed within or near online advertisements or on Web pages where data is collected and used for behavioral advertising. The icon links to a clear disclosure

statement regarding the company's online behavioral advertising data collection and use practices as well as an easy-to-use opt-out mechanism. The FTC has stated that privacy should be promoted at every stage of a product design and made transparent to consumers. It also has said that data should only be collected consistent with the context of a particular transaction or consumers' relationship with the company, or as required or authorized by law. Beyond that, the FTC has indicated that companies should make appropriate disclosures to consumers at "a relevant time and in a prominent manner – outside of a privacy policy or other legal document." The Chairman of the FTC summarized their position as follows: "We have proposed a 'Do Not Track' mechanism that will allow you [the consumer] to easily specify what information you want to share about your browsing behavior and have those preferences travel with you to every website you visit. Technologies to create such a system exist already."

FTC and FCC Rules on Telemarketing and Using Cell Phone Numbers

Regulators are cracking down on telemarketing and the making of unsolicited phone calls, especially to cell phone numbers.

Did You Know?

> Regulators are cracking down on telemarketing and the making of unsolicited phone calls, especially to cell phone numbers. Fines for calling or texting to cell phones can be $500 - $1,500 under the Telephone Consumer Protection Act.

According to a National Health Interview Survey available at the CDC's website, almost half of U.S. households no longer have land lines and use their cell phone as their home number, so these new rules require extreme caution when calling customers because the cost of calling or texting to cell phones can be $500 – $1,500 under the Telephone Consumer Protection Act.

Laws and regulations concerning telemarketing, email, and fax restrictions are discussed in Topic 7: The FTC: Marketing and Advertising Vehicles, and Credit Terms.

Recommended Practices

1. **Create your FCRA-GLBA Privacy Notice using the FTC's Model Consumer Privacy Online Form Builder.**

Recommended Practice:

> Use the FTC's Model Consumer Privacy Online Form Builder to create your own Privacy Notice.
>
> https://www.ftc.gov/news-events/news/press-releases/2010/04/federal-regulators-release-model-consumer-privacy-notice-online-form-builder

It explains what personal information your dealership collects, how it collects and uses the personal information, and with whom it shares the information. (See example at the end of this Topic.) Write your FCRA-GLBA privacy notice in the present tense ("We do the following") and avoid hyperbole such as "we will never share your information" or "we maintain the highest security practices." Date your privacy notice. If you share customer information with affiliates, be sure to comply with all applicable law. A best practice is to include the Affiliate Marketing Rule disclosure and notice in your model FCRA-GLBA Privacy Notice form which meets the requirements of both the FCRA's Affiliate Marketing Rule and GLBA's Privacy Rule. Alternatively, you may choose to use the "safe harbor" notice under the Affiliate Marketing Rule to send a single notice to disclose the customer's right to opt out of the affiliates' use of customers' eligibility information to market or solicit. You can then give this Affiliate Marketing notice once every five years, unlike the combined FCRA-GLBA Privacy Notice which you have to give annually for as long as the person remains your customer. If you decide to send a separate Affiliate Marketing notice, remember, you must also separately send an annual GLBA notice. (Note that if you sell a vehicle to a customer and assign the contract to a financing source, that person is no longer considered your customer for privacy notice purposes unless they have another credit relationship with your dealership.)

2. Have your privacy notices reviewed by your counsel to ensure the notices contain all of the required disclosures.

Recommended Practice:

> Have your privacy notices reviewed by your counsel.

Your privacy notices and policies should be reviewed and updated on at least an annual basis. You should also make sure that your privacy notices accurately reflect your actual information collection and sharing practices. Be careful about pooling information with affiliates or your parent company into a central database, as doing so can be considered sharing information with affiliates.

3. Confirm whether and how you share information with third parties in accordance with your current FCRA-GLBA Privacy Notice.

Recommended Practice:

> Confirm that your third-party information sharing practices are in accordance with your current privacy notice.

Many DMS providers "pull" information out of your DMS system and use it for their own purposes, and not merely to service your account. Doing so is considered third-party sharing under GLBA. If your privacy notice says, "we don't share" and your DMS provider is taking and giving access to customer information to third parties (even without your knowledge), you may be in breach of your privacy notice and face a prospective class action. Given the nature of the DMS system used by many dealers, it may be a safer practice to indicate in your FCRA-GLBA Privacy Notice that you do share and give customers the right to opt out. If possible, contractually prohibit your DMS providers from pulling customer data from your DMS system for any reason other than to service your account. Any such access to customer data for purposes that extend beyond servicing their account must be disclosed, and appropriate opt-out rights for sharing must be given in your privacy notice. Make sure to contractually require your affiliates and other entities with which you share customer information to comply with your privacy notices as well.

4. Give your FCRA-GLBA Privacy Notice to each consumer who provides you their personal information.

Recommended Practice:

> Give your FCRA-GLBA Privacy Notice to each consumer who gives you their personal information.

Provide it when the person first gives you their personal information, or soon thereafter. Clearly and conspicuously post your FCRA-GLBA Privacy Notice on your dealership website, link to it from your online credit application form (a good practice is to compel a consumer to link to the privacy notice and be forced to scroll through it before they can submit the online credit application) and give a copy to every consumer who comes into your store inquiring about financing. The FTC has an internal group that reviews company privacy notices and "mystery shops" to uncover violations.

5. Date your privacy notices so that you will always know that the version you are using is current.

Recommended Practice:

> Always date your privacy notices to ensure you are using the current version.

If you use one of the model notice forms, this dating reserves the right to change your privacy notice at any time. Put updated privacy notices on your website when you do make a change. The model "safe harbor" FCRA-GLBA Privacy Notice forms require dating your privacy notices.

6. Set up a process in your dealership to collect and manage all customer opt-outs from your customers.

Recommended Practice:

> Consistently collect and manage all customer opt-outs.

Customers have many opt-out rights. One way to manage them is to establish separate opt-out lists for each of these and use them before sharing information or conducting marketing activity as necessary.

Table of Contents

However, to simplify the process and reduce the chance for errors, keep one master list of customers who send opt-out notices to your dealership concerning any information sharing and remove all these customers from all databases that you share or use for contact purposes, including common databases within a dealership group. Having a single omnibus opt-out system is a much simpler process and will make you less likely to commit an error that could constitute a compliance violation.

7. If your dealership is engaged in online tracking for advertising purposes, you should consider use of the Advertising Option Icon and giving consumers a Do-Not-Track opt-out mechanism.

Recommended Practice:

> Alert customers if you use online tracking and give them a way to opt out.

At minimum, disclose in your Terms of Use on your website what you are doing in the way of placing cookies on users' devices and the nature of the tracking you do. Transparency in data collection and use was a priority in the FTC's Final Privacy Report released in March 2012.

8. If your dealership does business in California, you should evaluate your CCPA obligations

Recommended Practice:

> California dealerships: Find out whether you need to add the CCPA "Do Not Sell" link to your website.

and specifically whether you will need to have the CCPA "Do Not Sell" link accessible on your website.

Additional Resources

The FTC's Privacy Rule and Auto Dealers
https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-privacy-rule-auto-dealers-faqs

FTC Model Privacy Notice Online Form Builder
http://www.federalreserve.gov/bankinforeg/privacy_notice_instructions.pdf

Line-by-line instructions to complete model privacy notice — Go to page #62965
(FTC rules begin at the bottom of this page in this Federal Register notice)
http://www.gpo.gov/fdsys/pkg/FR-2009-12-01/html/E9-27882.htm

Background on the FCRA
http://epic.org/privacy/fcra/

Information on the DPPA
http://www.accessreports.com/statutes/DPPA1.htm

Information on the CCPA and CPRA
https://cppa.ca.gov/regulations/

Example of a Model Privacy Notice Form

The following is a sample of a privacy notice. This sample is for illustrative purposes only.
Consult your attorney to make certain the notice you intend to provide to your customers complies with the law.

https://www.federalreserve.gov/bankinforeg/PrivacyNotice_NoAffil_OptOut.pdf

Note:
You will also need to add any required states' notices as applicable.

Aftermarket Product Sales

When marketing and selling aftermarket products, auto dealers should be transparent about what the product is, how much it will cost, and whether it is optional for a vehicle purchase.

Engage in ethical aftermarket product sales →

Did You Know?

Some states require a separate disclosure to be given to a car buyer describing the price and the effect of certain aftermarket products on the buyer's monthly payment. Disclosure Rules for Aftermarket Sales

Compliance Tip

Monitor state laws for changing requirements that may apply to GAP or GAP-like products, including Excess Wear and Use waivers and Vehicle Value Protection agreements. See more Compliance Tips

Watch List for 2025

The FTC has finalized its Combating Auto Retail Scams (CARS) Rule against unfair and deceptive practices in auto financing and add-on product selling, which is set to take effect on September 30, 2025, pending the outcome of legal challenges to the Rule.

Recommended Practice

More states are broadening requirements applicable to voluntary protection products (VVPs), including GAP products, so be sure to consult your attorney to confirm that your practices comply with state laws applicable to your dealership. More Recommended Practices

Breakout Sections

Aftermarket Product Selling

Many dealers offer to sell aftermarket products to consumers at the time of a vehicle purchase. Typically, the products that are offered include vehicle service contracts, GAP (guaranteed auto protection) waivers and insurance, credit life and disability insurance, and other products that are generally marketed as enhanced protection of the vehicle or the customer's credit obligations. Aftermarket transactions also include products and services to accessorize a vehicle. **In recent years, aftermarket items must be disclosed separately, and a dealer must clearly disclose that their purchase is voluntary and not required to obtain financing. Many states (for example, California, Minnesota, and Pennsylvania) also have detailed regulations about how various aftermarket items must be separately disclosed to the consumer.**

Did You Know?

State laws require that specific notices be given to consumers with regard to certain aftermarket products.

Aftermarket Product Scrutiny

The FTC as well as the CFPB are actively investigating the sale of aftermarket products of all types for unfair and deceptive practices. The CFPB, at the urging of consumer advocates, has questioned the value of aftermarket products in relation to their cost and has asserted that it has authority over the sale of certain aftermarket products directly and all aftermarket products, when financed by a consumer. While the CFPB does not have authority to bring an action directly against certain auto dealers, it can bring actions against certain independent and buy-here-pay-here dealers and refer all other dealer violations to the FTC or a State Attorney General.

Since its inception, the CFPB has focused, as a top priority, on the sale and marketing of aftermarket products. Former CFPB Director Richard Cordray specifically mentioned add-on aftermarket products in his opening remarks at an auto finance field hearing in 2014, saying that by the time consumers get to the aftermarket part of the sales process, they may be invested in the car and impatient to finish up and drive it home, making them susceptible to misleading statements about the benefits of the product they are being sold.

In 2022, the CFPB issued a blog post highlighting particular concerns about "unearned" fees on GAP products charged even after an auto loan is paid off. Also in 2022, the FTC testified before the House Committee on Oversight and Reform Subcommittee on National Security that it was combating unscrupulous and predatory auto sales practices, including "payment packing" (slipping unwanted add-ons into a purchase agreement), bait-and-switch tactics, and extra junk fees that target servicemembers and the broader military community, including in relation to aftermarket products.

Consumer advocates and the CFPB have found that consumers typically have little awareness regarding aftermarket products or their costs. Further, in studies and on the CFPB online complaint portal, the CFPB indicates that consumers have a negative perception of the aftermarket sales process and sometimes even of the aftermarket product itself, although other industry data disputes this.

This Topic discusses laws and regulations concerning marketing and advertising of aftermarket products. Federal and state laws govern the methods and content of advertising and marketing as well as the disclosure of aftermarket items. The CFPB, the FTC, and state regulators are all interested in aftermarket product sales in a variety of industries and have brought enforcement actions for unfair and deceptive sales practices.

Incentives

In the wake of an employee incentive consent order against a lender, in November 2016, the CFPB issued a bulletin warning supervised financial companies that creating incentives for employees and service providers to meet sales and other business goals can lead to consumer harm if not properly managed. Dealers should monitor any incentives related to the sale of aftermarket products to ensure the programs are consistent with the supervisory bulletin. Specifically, "the strictest controls will be necessary where incentives concern products or services less likely to

benefit consumers or that have a higher potential to lead to consumer harm, reward outcomes that do not necessarily align with consumer interests, or implicate a significant proportion of employee compensation."

To minimize risk of potential harm to consumers, the CFPB recommends that entities implement a robust compliance management system that includes: (i) oversight by the board of directors or management; (ii) adequate policies and procedures; (iii) training employees on expectations for employee incentives and ethical behavior; (iv) monitoring key metrics that may indicate incentives are leading to improper behavior; (v) a manner to implement corrective action where a risk or violation is identified; (vi) a consumer complaint management system; and (vii) an independent audit. The size and scope of the compliance management system will depend on upon the size of the dealer and its business model, among other things.

Important Laws and Regulations

Disclosure Rules for Aftermarket Sales

State laws require that specific notices be given to consumers with regard to certain aftermarket products. For example, most state insurance laws require the dealer to inform customers that purchasing insurance from the dealer is not required to obtain credit and that the consumer can obtain insurance from any insurance agent of their own choice. Many state laws require clear and conspicuous disclosures concerning GAP liability and insurance in leasing transactions as well.

The Federal Truth in Lending Act (TILA) also requires this disclosure in order to keep the insurance cost from being included as a part of the finance charge.

Did You Know?

> The Federal Truth in Lending Act (TILA) also requires this disclosure in order to keep the insurance cost from being included as a part of the finance charge.

If a dealer fails to prominently disclose that the purchase of an aftermarket item is voluntary and not required for credit, the cost of the item is considered a part of the "finance charge" for TILA purposes, and the APR must be calculated to reflect that fact. A dealer must also disclose if it will retain a portion of the premium or charge.

In addition, most state laws (and, effectively, TILA and Regulation Z) expressly prohibit "payment packing," a practice whereby the dealer quotes monthly payment prices under financing plans to consumers that include the cost of optional items that the customer has not yet agreed to purchase and without disclosing to the customer that the monthly payment quote includes such optional purchases. Restated, "payment packing" describes the sales practice of deceptively increasing a consumer's credit obligation (and in turn, increasing the dealer's and creditor's profits), by padding or "packing" the amount financed through the sale of unnecessary, unrequested and/or unwanted ancillary products. Other packing practices may include overcharges to consumers eligible for GAP coverage, sales of GAP to consumers ineligible for coverage, and/or sales of GAP products that provide less or more than the coverage desired. Generally, states may regulate the practice of "payment packing" through unfair deceptive acts and practices statutes and/or unfair insurance trade practices statutes. Many of these statutes may offer a private remedy for plaintiffs seeking redress for alleged transgressions.

Additional state regulations may also require a separate disclosure to be given to the buyer describing the price and the effect on the consumer's monthly payment of each service contract, insurance product, debt cancellation agreement, theft deterrent device, exterior or interior surface protection product, and contract cancellation option. The dealer must obtain the consumer's signature on this written disclosure prior to signing the sales contract. Discrimination claims (both under common law and under anti-discrimination laws like ECOA) can be brought against a dealer if its pricing and sales practices for aftermarket products are not consistent between non-protected and protected classes of persons (for example, charging women more for the same products). While laws and regulations may not specifically require consistency in sales approaches, variations in sales practices may still trigger the possibility of being sued

under various legal theories, notably UDAP laws described in Topic 8.

In 2022, the FTC proposed the Motor Vehicle Dealers Trade Regulation Rule which is aimed at banning "junk fees and bait-and-switch advertising tactics" by auto dealers. The proposed rule would prohibit dealer add-on products that provide no benefit, require disclosures for optional add-ons, require express and informed consent to charge for any item, and impose record-keeping requirements. The 2022 proposed rule's definition is broad: "Add-on or Add-on Product(s) or Service(s) means any product(s) or service(s) not provided to the consumer or installed on the vehicle by the motor vehicle manufacturer and for which the Motor Vehicle Dealer, directly or indirectly, charges a consumer in connection with a vehicle sale, lease, or financing transaction."

The definition of "add-on product or service" from an FTC enforcement action settled in 2023 was more detailed: "any product or service relating to the sale, lease, or financing of a motor vehicle that is marketed, offered, provided, sold or arranged by a motor vehicle dealer that is not provided or installed by the motor vehicle manufacturer, including but not limited to extended warranties; prepaid or other maintenance plans; Guaranteed Asset Protection insurance ('GAP insurance'); Vehicle Identification Number (VIN) etching; vehicle service contracts; payment programs; rustproofing; undercoating; paint or fabric protection; physical items such as mud flaps or sill plates; appearance products; lease protection; tire and wheel protection; theft protection or security devices; global positioning systems; starter interrupt devices; remote starters; road service or club memberships; shuttle services; credit life, accident, disability, loss-of-income or other insurance; and debt cancellation or suspension coverage."

Thus, examples of prohibited aftermarket products include:

- Rustproofing that does not actually prevent rust;
- Theft-prevention services that lack proof that the services prevent theft;
- Nitrogen-filled tires that contain no more nitrogen than naturally exists in the air;
- GAP insurance sold to consumers with a financing balance low enough that ordinary insurance would be sufficient; and
- Extended warranties that merely duplicate coverage already provided on the vehicle.

In order to offer optional add-ons, dealers will need to disclose up-front the cash price at which a consumer may purchase the vehicle without additional add-ons. The dealer will also need to offer to close the transaction without any optional add-ons. Lastly, the proposed rule would require dealers to maintain for 24 months materially different advertisements, training materials, and marketing materials regarding vehicle price, financing, or leasing terms; materially different lists of add-on products; consumer complaints regarding add-ons; and records to establish compliance with the proposed rule.

After the close of the comment period for the Motor Vehicle Dealers Trade Regulation Rule in September 2022, the FTC declined to extend the comment period for the Rule and instead developed and announced a similar but broader proposed Rule, the Trade Regulation Rule on Unfair or Deceptive Fees, in November 2023 to impose junk fee prohibitions on businesses including but not limited to those in the auto industry. Similar to the 2022 proposed Rule, the 2023 proposed Rule prohibits "misrepresenting the total costs of goods and services by omitting mandatory fees from advertised prices and misrepresenting the nature and purpose of fees," including "misrepresent[ing] optional ancillary products as mandatory." The breadth of this proposed Rule continues to indicate the FTC's intention to crack down on deceptive practices relating to aftermarket parts sales. The comment period on the proposed Rule ended in January 2024, and the FTC held an informal hearing on the proposed Rule in April 2024. The FTC may consider finalizing the proposed Rule in 2025.

In December 2023, the FTC announced its proposed Combating Auto Retail Scams (CARS) Rule that focuses more specifically on junk fees and other

UDAP practices in the auto industry. The Rule requires auto dealers to cease misrepresenting "material" information that would affect a consumer's choice to buy a car, disclose the offering price of the car separate from optional add-ons, avoid charging a consumer for add-on products that provide no benefit to the consumer, retain all records necessary to demonstrate compliance with the Rule for at least 24 months, and stop misrepresenting dealers' affiliations with military or government organizations, among other requirements.

The FTC finalized the CARS Rule in 2024, but its implementation is delayed by legal challenges to the Rule.

Watch List for 2025:

The FTC CARS Rule is finalized and is set to take effect on September 30, 2025, depending on the outcome of legal challenges to the Rule.

In January 2024, the National Automobile Dealers Association (NADA) and Texas Automobile Dealers Association filed a petition in the Fifth Circuit Court of Appeals against the FTC alleging that the CARS Rule is arbitrary and capricious and would significantly increase dealers' costs and extend the car-buying process. *Nat'l Auto. Dealers Ass'n v. FTC*, Case No. 24-60013 (5th Cir. 2024). The Fifth Circuit held oral argument on the petition in October 2024 and is expected to issue its ruling in 2025, which may then be appealed to the United States Supreme Court. Given the ongoing lawsuit against the Rule, the U.S. House Appropriations Committee passed the Fiscal Year 2025 Financial Services and General Government appropriations bill in June 2024, which included a provision requiring the FTC to delay implementation and enforcement of the Rule until September 30, 2025, pending the outcome of the lawsuit.

In addition to the proposed and finalized rules, the FTC has been ramping up enforcement of current rules prohibiting "junk fees." The FTC recently required an auto dealer and its general manager to pay $2.6 million for misrepresenting optional or already-installed add-on products as required for consumers to purchase vehicles. The FTC also required an auto dealer group and its general manager to pay $1.1 million to settle the FTC's allegations that the dealer had added "junk fees" for add-ons after consumers declined the add-ons or confirmed the price without the add-ons present. Other FTC complaints against dealers alleged that the dealers either increased the price over what was advertised or negated any discounts the consumers negotiated through the use of add-on fees. One dealer described the add-on fees as extra fees it charged to customers for inspection, reconditioning, or certification when, in many instances, automobile manufacturers specifically prohibit dealers from charging separately for certification costs.

These rules and enforcement are not limited to the federal level. In 2024, California's new law banning junk fees went into effect. The law requires all "mandatory fees or charges" to be included in a price that is advertised, displayed, or offered by a dealer. The law also prohibits dealers from "representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another" or "representing that a part, replacement, or repair service is needed when it is not." Minnesota passed a similar junk fee ban in 2024 that will take effect in 2025. In addition, several states, including Arizona, Connecticut, and Wisconsin, have collaborated with the FTC to bring enforcement actions and obtain millions of dollars from auto dealers for charging junk fees to consumers without their consent, misrepresenting add-ons as required instead of optional, and engaging in other wrongful practices.

The enactment of junk fee bans, and initiation of related enforcement actions are expected to continue, and potentially even increase, into 2025 and beyond.

Insurance Products

In selling aftermarket products, it is critical to know how the dealership's home state characterizes certain protection products, such as GAP, debt cancellation products, and/or service contracts. In some states, these are considered "insurance,"

Did You Know?

It is critical to know whether or not your dealership's home state characterizes certain aftermarket protection products such as GAP, debt cancellation products, and/or service contracts as insurance.

which may require the dealer to be licensed by the State Insurance Department and to give the customer disclosures in a retail installment sales contract (RISC) that are different from disclosures for non-insurance products. In other states, where these products are not considered insurance, they still need to be separately itemized on a RISC or lease agreement. If all or part of the payment is paid to a third party, the itemization must indicate the identity of the third party. If true, dealers should also disclose the fact that it may retain a portion of an amount paid to a third party. Federal law requires that credit insurance and GAP coverage be initialed or accepted by the consumer in writing. This is typically done by having the consumer initial an insurance box on the retail installment sales contract or lease agreement.

State laws on how products are characterized can change. For example, prior to 1997, New York considered a service contract that covers wheel and tire damage caused by road hazards such as a blowout to be an insurance product. As such, only a licensed insurer could sell this product. However, the New York Legislature amended the State's Insurance Law to provide that a manufacturer or seller of a tire or its agent (such as an auto dealer) may offer coverage for damage to a wheel or tire from road hazards without needing an insurance license.

Both the FTC and CFPB have emphasized that transparency, understanding, and fairness are needed in the treatment of consumers related to the sale of aftermarket products. **Aftermarket products are a ripe area for consumer misunderstandings, and it is important that F&I professionals take the time to carefully explain what each product costs and the benefits it provides.**

Compliance Tip:

Aftermarket products are a ripe area for consumer misunderstandings. It is important that F&I professionals take the time to carefully explain what each product costs and the benefits it provides.

The review should include that the purchase of the product is voluntary and not required to obtain credit. Scripts and Q&As for aftermarket selling will be examined by regulators, as will any recordings of aftermarket selling sessions. Make sure yours tell a good story.

Guaranteed Automobile Protection ("GAP")

GAP is optional consumer protection that generally covers the difference between what the car is worth and what the consumer owes on the car after a total loss. There are two types of GAP protection: (1) GAP insurance; and (2) a two-party GAP waiver. Both GAP insurance and two-party GAP waiver have coverage limits, although GAP waiver typically has much higher coverage limits that often apply to both the amount owed on the financed vehicle and negative equity from a trade in vehicle that is included in the amount financed.

GAP insurance is an agreement entered into between the consumer and a third-party insurance company. It functions as insurance coverage to generally cover the "gap" between the amount a customer owes on their car and the car's actual cash value in the event of an accident. A car's actual cash value is the car's monetary value at the time of the accident, not the car's original price. GAP insurance is not available from many auto insurance companies and, when it is available, it often is limited to consumers with a qualifying credit profile who are purchasing new vehicles or used vehicles below a certain age. GAP insurance also typically does not cover negative equity from a trade in vehicle and may not cover the auto insurance company's deductible. In addition, GAP insurance must be added to coverage should a customer switch insurance companies because it does not transfer from one insurance company to another. The creditor is not a party to a GAP insurance agreement.

A two-party GAP waiver, on the other hand, is a contractual agreement between the consumer and the creditor which remains with the finance contract through maturity unless it is cancelled pursuant to the agreement. A GAP waiver is typically designed to be an addendum to the retail installment sale contract or lease. In a retail installment sale transaction, the dealer, as the initial creditor, is initially obligated on the GAP waiver. When the retail installment sale contract is assigned, the holder steps into the dealer's shoes and becomes obligated on the GAP waiver. Under a GAP waiver, the holder is obligated to "waive" the amount owned as specified in the agreement.

States typically dictate whether a creditor may sell and finance GAP. Historically, states generally permitted creditors to sell and finance GAP insurance, while only some states permitted creditors to sell two-party GAP waivers as non-insurance products. In recent years, many states have enacted GAP waiver laws or adopted regulatory positions that expressly permit creditors to sell and finance non-insurance GAP waivers. **Some states have also started regulating GAP-like products, such as Vehicle Value Protection Agreements (VVPA).**

Compliance Tip:

> Monitor state laws for changing requirements that may apply to GAP or GAP-like products, including Excess Wear and Use waivers and Vehicle Value Protection agreements.

For example, in 2024, Florida passed a new law changing its existing requirements for GAP and Excess Wear and Use (EWU) waivers, as well as extending its requirements to VVPAs. Other states are expected to follow suit.

State GAP waiver laws typically impose disclosure and other substantive requirements for offering a GAP waiver, including limitations on GAP waiver terms, cancellation, and refund requirements, and in a limited number of states, form approval requirements, licensing or registration requirements. The failure to comply with these requirements when offering a GAP waiver may, among other things, result in the GAP waiver being subject to regulation as insurance or may subject any GAP waiver charge to being treated as a finance charge.

GAP insurance and GAP waivers are also subject to regulation under federal law. TILA requires the financing agreement to include certain disclosures in order to exclude GAP charges from the finance charge. Specifically, in order for a GAP charge to be excluded from the finance charge under TILA, Regulation Z requires the following conditions to be satisfied: (i) GAP is not required by the creditor, and this fact is disclosed in writing; (ii) The fee or premium for the initial term of coverage is disclosed in writing. If the term of coverage is less than the term of the credit transaction, the term of coverage also must be disclosed; and (iii) The consumer signs or initials an affirmative written request for coverage after receiving these required disclosures. Any consumer in the transaction may sign or initial the request. If a dealer fails to prominently disclose that the purchase of GAP is voluntary and not required for credit, the cost of the item is considered a part of the "finance charge" for TILA purposes and the APR must be calculated to reflect that fact. A dealer must also disclose if it will retain a portion of the premium or charge.

Finally, when marketing and selling GAP, dealers must be mindful of complying with state and federal standards governing unfair, deceptive, or abusive acts or practices. The sale and marketing of voluntary protection products (VPPs), including GAP, have been an area of focus for government law enforcers, including the CFPB and the FTC. While the agencies have not issued any guidance to date that directly impacts the ability of a creditor to sell GAP, issues of focus include fair lending, marketing, and advertising of products, and the techniques used to sell GAP. This has resulted in enforcement actions involving deceptive claims about the benefits of GAP, failure to disclose material product exclusions, limitations, or qualifications on the benefits, violations of TILA, and billing for services not provided. Another area of potential risk with respect to GAP is high penetration rates as evidence to challenge the voluntary nature of the products. In other words, penetration rates in the high 90th percentile, while not per se evidence that the product is not voluntary, could invite heightened scrutiny around sales practices.

Most states have unfair and deceptive acts and practices statutes, and/or unfair insurance trade practices statutes, which may also govern the

sale of GAP and/or disclosures made in connection with those sales. Many of these statutes offer appealing private remedies for plaintiffs seeking redress for alleged transgressions, including "payment packing" or "packing." "Packing" describes the sales practice of deceptively increasing a consumer's credit obligation (and in turn, increasing the dealer's and creditor's profits), by padding or "packing" the amount financed through the sale of unnecessary, unrequested, and/or unwanted products. Other packing practices may include overcharges to consumers eligible for GAP coverage, sales of GAP to consumers ineligible for coverage, and/or sales of GAP products that provide less or more than the coverage desired.

To the extent GAP is marketed honestly and the cost of the GAP is transparent to the consumer, dealers can reduce these compliance risks.

Compliance Tip:

Establish a process to ensure honest and transparent marketing of GAP to help reduce compliance risk.

The National Automobile Dealers Association, in conjunction with the National Association of Minority Automobile Dealers and the American International Automobile Dealers Association, issued an optional Model Dealership Voluntary Protection Products Policy to assist dealers in offering a professional, transparent, and consumer-friendly VPP sales process. You should consult your attorney on compliance issues relating to the GAP or other VPP products you offer.

Recommended Practices

1. **If you conduct direct marketing of aftermarket products, scrub your target lists for persons who have excluded themselves.**

Recommended Practice

Regularly scrub your aftermarket products direct marketing target lists to remove anyone who has opted out or unsubscribed.

You should keep a separate list of consumers who opt out of telemarketing, faxes, and email, and be sure to not use auto dialers or prerecorded telemarketing messages unless you first obtain the customer's written signed consent to receive auto-dialed or prerecorded calls or texts at a designated number with such consent containing language that "I understand that this consent is not a condition of purchase or credit." Adequately scrub telemarketing lists of phone numbers against the FTC's National Do Not Call Registry (www.donotcall.gov), your state's Do Not Call list, and your dealership's list of persons who have asked not to be called. The Association of National Advertisers (www.ana.net) also maintains "do not contact" lists that you can scrub your lists against. If you are telemarketing, get assurances from vendors on exclusions of persons listed on federal and state Do Not Call lists and double-check against state Do Not Call lists, as well as your own dealership's list of customers who have asked not to be called. If you are calling or texting for marketing purposes using an auto dialer or prerecorded message, getting a prior written signed consent with the above language is required or a penalty per call can be assessed. For additional information see Topic 10.

2. **Understand the state law concerning a dealer's ability to disclaim warranties.**

Recommended Practice

Understand state laws concerning your dealership's ability to disclaim warranties.

Make sure it is clear in the service contracts you sell whether you have "entered into" the service contract, in which event you cannot disclaim implied warranties under the Magnuson-Moss Warranty Act (MMWA) discussed in Topic 7: The FTC: Marketing and Advertising Vehicles, and Credit Terms. Service contracts and insurance contracts to cover the obligations can be structured in a number of different ways, each of which has different tax and liability issues. Two examples are "retro" policies and "reinsurance" policies. In "retro" policies, a portion of the customer premiums is sent by the dealer to an insurer who deposits it into an account to pay claims. When contracts expire or at predetermined times, the dealer receives a portion of the earned premiums. In reinsurance policy

programs, the dealer sends a fixed amount to an insurance company who in turn cedes the amount to a reinsurance company that may be affiliated with the dealer. The insurer offsets claims payments against sums paid to the reinsurance company. When National Warranty went bankrupt, reinsurance companies were deemed to own the reserves, which remained available for customer claims. Retro accounts were considered part of National Warranty's bankruptcy estate and not available to satisfy consumer claims. State insurance laws also contain requirements for insurance and reinsurance for service contracts. Review how your service contracts are structured and insured with your lawyer and accountant.

3. **Charge the same price for each product and each grouping of prducts.**

Do not surcharge credit customers, as the surcharge is considered part of the "finance charge" under TILA and must be calculated into the APR and disclosed in the RISC.

4. **Use consistency in selling aftermarket products in the F&I office.**

Recommended Practice

> Don't skip required steps in the F&I product presentation process. Failure to provide consistent options and full disclosures will put your dealership at risk for fines and penalties.

Understand what is legally required by your state's law and prepare scripts, FAQs, and presentations that fairly and honestly state what the product is and how much it will cost.

5. **Monitor and adjust your menus, presentation scripts, and practices to address consumer feedback and your CSI scores.**

Recommended Practice

> Adjust menus, presentation scripts, and practices in response to consumer feedback and CSI scores.

Adapt your menu and aftermarket product selling to consider changes in the law or unintended consumer negative reaction. Train and test your employees, and regularly audit their performances.

6. **Ensure any incentive programs are developed and monitored such that they are consistent with the CFPB bulletin on incentives. Review and understand the CFPB bulletin on incentive programs.**

Recommended Practice

> Develop and monitor any incentive programs to be consistent with the CFPB bulletin on incentives.

Apply robust controls where incentives concern products or services that may be less likely to benefit consumers or that have a higher potential to lead to consumer harm, reward outcomes that do not necessarily align with consumer interests, or implicate a significant proportion of employee compensation.

7. **Ensure that any aftermarket products comply with applicable federal and state law.**

Recommended Practice

> Make sure the aftermarket products you sell comply with federal and state law.

Consult with your local attorney to confirm that your disclosures and consumer-facing agreements comply with applicable law.

Additional Resources

FTC, CARS Rule (December 2023)
https://www.ftc.gov/business-guidance/resources/ftc-cars-rule-combating-auto-retail-scams-dealers-guide

FTC, Proposed Rule on Unfair or Deceptive Fees (October 2023)
https://www.federalregister.gov/documents/2023/11/09/2023-24234/trade-regulation-rule-on-unfair-or-deceptive-fees

FTC, Proposed Rule on Motor Vehicle Dealers (July 2022)
https://www.federalregister.gov/documents/2022/07/13/2022-14214/motor-vehicle-dealers-trade-regulation-rule

Minnesota House Bill No. 3438 Junk Fees Ban (May 2024)
https://www.revisor.mn.gov/bills/text.php?number=HF3438&type=bill&version=3&session=ls93&session_year=2024&session_number=0

California Senate Bill No. 478 Junk Fees Ban (October 2023)
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB478

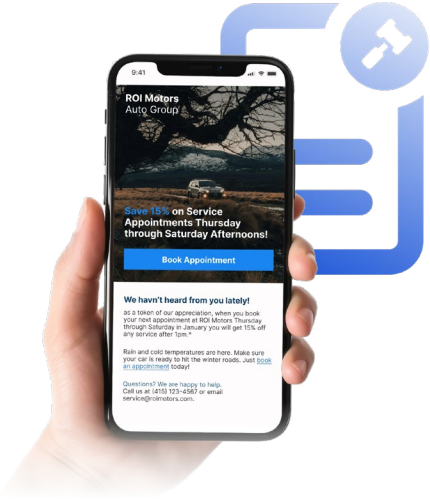
NADA, Voluntary Protection Products: A Model Dealership Policy
https://www.nada.org/regulatory-compliance/voluntary-protection-products-model-dealership-policy

Auto Finance News, Auto Lenders, Dealers Duplicating Aftermarket Compliance Efforts (March 2024)
https://www.autofinancenews.net/allposts/compliance/auto-lenders-dealers-duplicating-aftermarket-compliance-efforts/

Marketing and Advertising Vehicles and Financing

Many enforcement actions by the CFPB and FTC result from advertisements by auto dealers. Find out what information to include—and not to include—in your advertisements to avoid legal actions and fines.

Learn how to keep your marketing and advertising compliant →



Did You Know?

The FTC prohibits use of the word "free" in describing a product if that product is sold with another product or service as to which the price is arrived at through bargaining. See more about Other Advertising Guidelines

Compliance Tip

If you use an online influencer to promote your dealership or related products or services, ensure the influencer does not make any advertising claim that you could not also make. See more about Online ("Digital") Advertising

Watch List for 2025

The CFPB and FTC are cracking down on misleading advertisements, deceptive pricing, and improper online listings by auto dealers and intend to continue doing so into 2025. Learn about applicable laws and regulations in this Topic to ensure your advertisements and listings satisfy regulators.

Recommended Practice

Review your advertisements for any misleading or missing pricing information that could become the subject of a regulatory action. See more Recommended Practices

Breakout Sections

Table of Contents

Marketing and Advertising Vehicles and Financing

The Federal Trade Commission (FTC) has enforcement authority over false or misleading advertising and other wrongful activity under the authority of Section 5 of the FTC Act to prevent unfair, deceptive acts and practices (UDAP). Within the past few years, the FTC has revved up its enforcement of deceptive auto dealer advertising, starting with "Operation Steer Clear" in January 2014 and continuing with "Operation Ruse Control" in March 2015, in which the FTC partnered with 32 law enforcement agencies to bring hundreds of enforcement actions.

More recently, the FTC finalized its Combating Auto Retail Scams (CARS) Rule, which targets, among other things, misrepresentations by auto dealers in advertisements, pricing, financing, add-on products, and more. Specifically, the Rule "(i) prohibits motor vehicle dealers from making certain misrepresentations in the course of selling, leasing, or arranging financing for motor vehicles, (ii) requires accurate pricing disclosures in dealers' advertising and sales communications, (iii) requires dealers to obtain consumers' express, informed consent for charges, (iv) prohibits the sale of any add-on product or service that confers no benefit to the consumer, and (v) requires dealers to keep records of certain advertisements and customer transactions." The CARS Rule becomes effective on September 30, 2025, pending the outcome of legal challenges brought against the rule discussed in Topics 1 and 6.

The FTC can identify enforcement targets in many different ways. Although the agency does not need to receive consumer complaints to initiate an investigation, complaints sometimes trigger a closer look. In the case of auto dealers, many investigations arise from FTC staffers looking for problematic ads on the Internet. Another federal agency on the lookout for potential enforcement targets is the Consumer Financial Protection Bureau (CFPB), particularly with regard to auto financing. In its Fall 2024 Supervisory Highlights, the CFPB called out auto loan originators for advertising marketing rates "as low as" specified APR rates to consumers who had no reasonable chance of qualifying for or being offered rates at or near that level.

In this Topic, we discuss laws, regulations, and regulatory enforcement actions concerning marketing and advertising of vehicles and credit products, as well as best practices dealers should follow. Federal and state laws govern the methods and content of advertising and marketing in any medium of communication, both offline and online, including the internet and social media.

Basics of Deceptive Advertising

A deceptive practice is typically defined as a representation, omission, or other practice that is likely to mislead consumers acting reasonably under the circumstances in a material way. An act is deceptive where (i) a representation, omission, or practice misleads or is likely to mislead the consumer; (ii) a consumer's interpretation of the representation, omission, or practice is considered reasonable under the circumstances; and (iii) the misleading representation, omission, or practice is material. A practice can even be deceptive if it is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the FTC may consider established public policies as evidence to be considered with all other evidence.

Deception usually occurs through written or oral promotional messages (often referred to as "representations" or "claims") but can also occur in other ways.

Examples of deceptive practices include, but are not limited to the following:

- Misleading price claims;
- Sales of systematically defective products without adequate disclosures;
- **Bait-and-switch techniques;**

Did you know:

Online car "bait-and-switch" ads have been considered deceptive when they lure customers in with an advertised sale price that is claimed to no longer be available after the customer has already begun the car buying process.

Table of Contents

- Failure to perform promised services;
- Failure to meet warranty obligations; and
- Failure to disclose material limitations of an offer.

If the appearance of the product or the nature of the product itself conveys a misleading message, it can be deceptive. Simply selling a vehicle conveys the message that the vehicle is fit for its intended purpose (driving), even if the seller says nothing about its capabilities. Advertising, promotional materials and other disclosures should be tailored to the sophistication of the target audience. In considering whether advertising is deceptive, the FTC considers the entire advertisement, transaction, or course of dealing to determine how reasonable consumers would be likely to respond. Many factors may be considered in determining how a reasonable person would respond to a claim or practice.

To that end, the FTC may consider:

- How clear is the representation?
- How conspicuous is the qualifying information?
- How important is the omitted information?
- Do other sources of the omitted information exist?
- How familiar is the public with the product or service (i.e. car or aftermarket product)?

You should consult with your attorney for specific guidance, but the following is a practical guide to help you draft your marketing materials.

Claims Conveyed by the Advertisement

In determining whether an advertisement is deceptive, an advertiser must first understand what messages the ad is likely to convey to reasonable consumers. To do that, the advertiser must consider the ad as a whole and the "net impression" it creates. Even if everything stated in the ad is true, it can create an overall message that is deceptive. Advertisements may convey both express and implied claims. An express claim is one that states a fact directly, while an implied claim is one that literally says one thing but suggests something else. Advertisements often can be subject to multiple interpretations, some of which are true and some not. **An advertisement can be deceptive if any one reasonable interpretation is false or misleading, even if other interpretations are accurate, and even if the advertiser didn't intend for the advertisement to be perceived that way.**

Did You Know?

An advertisement can be considered deceptive even if your dealership didn't intend the interpretation that makes it appear false or misleading.

Note that "reasonable" does not mean sophisticated or highly educated.

Materiality of the Claims

Claims that are likely to influence consumers' decisions about whether to buy a product or service, or about how they use it, are considered material. The FTC often presumes that certain types of claims are material, including express claims and claims about a central feature of the product, the product's cost, or its safety. Keep in mind though that most claims are likely to be considered material, unless they are clearly "puffery" – claims that are so broad and fanciful that consumers do not take them seriously (for example, "world's best car").

Substantiation of the Claims

In addition to claims that are false or misleading, it is deceptive to make a claim about an objective feature of a product or service without having competent and reliable evidence to substantiate the claim at the time it is made. This is the case even if it later turns out that the claim was true. The type and amount of evidence that is necessary depends on the type of claim made. For example, a dealer that wants to advertise that it has the "lowest prices in the county" should survey the prices for the relevant comparison at the other dealerships in that county.

Deception by Omission

An advertisement can be deceptive not just for what it says, but also for what it does not say, that is, if it omits material information that is necessary to dispel a misimpression that the advertiser created. This usually arises in situations where there are significant qualifications, limitations, conditions, or restrictions on an offer. For example, it is deceptive to advertise financing at a particular rate without disclosing (when such is the case) that the rate may adjust upwards. Note that a disclosure is appropriate to qualify a claim, not contradict it. It is deceptive to claim one thing in the headline or text of an ad, while saying the opposite in a fine-print footnote. Moreover, a deceptive advertisement cannot be "cured" by providing the truth in a later communication with the consumer.

Making Effective Disclosures

All advertised terms must be "clear and conspicuous." If a disclosure is not made clearly and conspicuously, it is the equivalent of not making the disclosure at all. The FTC has identified the four P's for making effective disclosures: Prominence, Proximity, Placement, and Presentation.

Prominence

A disclosure must be large enough and sufficiently contrasting with the background such that ordinary consumers will notice and read it. The FTC does not state a required or minimum type size for disclosures, but there are state laws that require a minimum of 8- or 10-point type. Depending on the layout of the advertisement and the importance of the information, however, type size larger than 8- or 10-point may be necessary or appropriate. Disclosures should be distinguished from the background of the ad by using a contrasting color, bolding it, and/or putting the disclosure within a border. Asterisks next to qualified terms should be at least 50% the size of the qualified term's print size.

Proximity

Disclosures should be located close to the terms being qualified. A small footnote at the bottom of the page or image is generally not sufficient. Nor is putting the disclosures on another page of a brochure or another screen or page of a website not close to the qualified term or referring consumers to another location entirely to see the material terms (such as "see dealer for details"). In digital advertising, if hyperlinks are used to direct the consumer to the disclosure, they must be prominently displayed and clearly labeled to convey the importance and nature of the information. Information essential for consumers to understand the offer should not be disclosed through a hyperlink.

Placement

The location of the disclosure within the advertisement must be such that ordinary consumers would notice it. Small print asterisks or footnotes, even those next to the qualified term, do not meet this standard. Referring consumers to another document or location, such as "see dealer for details," is generally unacceptable.

Presentation

Language should be in "plain English." It should not scroll across media or be of such detail and depth that the average consumer would not likely read or understand it. There should be no distracting elements in the ad that compete for attention with the disclosure. The disclosure should be presented unambiguously and in short phrases. Oral disclosures in radio or audio media must be in a volume and cadence that a reasonable consumer can hear and understand.

Disclosures made in online or social media advertising present some unique challenges. This topic is discussed below.

Deceptive Advertising Examples

The following are a few examples of deceptive advertising by a dealer:

- Marketing a program where the consumer's outstanding debt on a trade-in vehicle would be paid off, no matter how much the consumer owed, but in reality, the dealer either financed the "negative equity" or required it to be paid off by the customer in cash.

- Failing to disclose that “dealer discounts” and “internet prices” would require customers to qualify for other discounts that were not generally available (e.g., military member, recent college graduate, etc.), and that even with these other discounts, the consumer would wind up paying a higher price for the vehicle than advertised.
- Advertising biweekly payment plans claiming that the plan would save consumers money on their financing by shortening the duration of the financing and thus lowering total interest paid, but the marketing materials fail to disclose that the fees charged for participating in the program outweigh any potential savings.

In 2016-2017, the FTC announced a series of settlements with auto dealers regarding advertising of used vehicles subject to unaddressed open recalls. In these cases, the FTC asserted that it was deceptive for dealers to advertise that used vehicles offered for sale were subject to a rigorous inspection when that inspection process did not identify and repair open recalls. The FTC argued that “rigorous inspection” claims constituted an implied representation that the vehicles were not subject to any unaddressed recalls. The FTC further claimed that such implied representations were likely to mislead reasonable consumers if the vehicles offered for sale were, in fact, subject to open recalls. These settlements required the dealers to supplement any inspection claims with a clear and conspicuous disclosure that vehicles offered for sale, even those that the dealer inspected, may be subject to an open recall. This disclosure also needed to explain how consumers could determine whether a particular vehicle offered for sale had any unrepaired recalls.

In 2018, the FTC settled a lawsuit against nine auto dealers in which they agreed to pay over $3.5 million in redress to consumers allegedly harmed by the dealers because they failed to disclose required information clearly and conspicuously in their advertising

Compliance Tip

Avoid potentially millions of dollar in fines by using clear and conspicuous disclosures in advertising.

and otherwise used deceptive and unfair sales and financing practices, deceptive advertising, and deceptive online reviews.

In 2020 the FTC initiated enforcement action over deceptive mailers. The mailers were designed to look like COVID-19 stimulus-related materials and instructed recipients to claim their stimulus benefits in person at a particular address, which turned out to be a lot hosting a car sale. Other mailers contained matching numbers indicating that the recipient had won a valuable prize that had to be claimed at a particular car dealership. However, small print on the back of the mailer disclosed that the recipient had not, in fact, won a prize yet and that there was a 1-in-52,000 chance of winning. Also, in 2020, the FTC sued a dealership in part because it failed to honor advertised sale prices, changed the sales price on paperwork in the middle of the sale without informing the customer, and misrepresented to customers that they were required to pay extra reconditioning and warranty fees to purchase “certified” vehicles.

In 2023, the FTC obtained a judgment of almost $1 million against vehicle parts manufacturers for advertising that their parts were “Made in USA” and “proudly designed, developed and manufactured in Lexington, North Carolina,” when that was only partially true. Most parts had been made and/or assembled in Taiwan before shipment to the manufacturers. In its final order against the manufacturers, the FTC stated that only products for which “final assembly or processing,” “all significant processing,” and the making and sourcing of “all or virtually all ingredients or components of the product” is completed in the United States can be advertised as being “Made in USA” without clear and conspicuous qualifications. This indicates that the FTC will scrutinize similar location claims made by dealers in their ads, as well.

More recently, in 2024, the FTC collaborated with the State of Arizona to require an auto dealer group and its general manager to pay $2.6 million back to consumers for engaging in bait-and-switch tactics by advertising low prices for vehicles online and then informing consumers who visited the dealership that the advertised prices were no longer available. The FTC brought an actions for similar reasons against

Table of Contents

another auto dealer in collaboration with the State of Connecticut. The FTC also obtained in 2024 a $1 million settlement from a former online used car retailer resulting from the retailer's deceptive online listings for cars. For example, the retailer would advertise that cars had passed "multiple inspections," when they had not, and would advertise certain delivery dates for cars and then fail to deliver on the advertised dates.

Finally, as detailed in Topic 6, in 2025, dealers may see new disclosure requirements that further expand the definition of deceptive advertising. The FTC has proposed a rule that, if finalized, may take effect in 2025 to require dealers to disclose what add-ons the consumer need not purchase, the total amount of payments required for a purchase or lease, and whether alternative financing options will increase the total amount the consumer will pay. The CARS Rule, which is expected to take effect in September 2025, provides similar mandates to auto dealers. Dealers should consult with their attorney to stay current on all state and federal disclosure requirements.

Dealer Advertising Practices to Avoid

The FTC is aggressively challenging deceptive dealer advertising. Below is a non-exclusive list of "don'ts" that the FTC and others have indicated dealers should avoid:

1. **Deceptive pricing. This is where the dealer makes misleading statements or omits material information about the price or terms of an offer.**

Recommended Practice

Review your advertisements for any misleading or missing pricing information that could become the subject of a regulatory action.

It is deceptive to state a price when that price excludes other significant fees and charges, unless the fees and charges are clearly and conspicuously disclosed. For example, a dealer luring prospective buyers onto the lot by advertising vehicles at a specific low price. But the advertised price is valid only after a $5,000 down payment, details of which are buried in a small-font footnote.

2. **Deceptive teaser payments.** This is where the dealer advertises interest rates that are only in effect for a short time, after which they increase substantially. For example, prominently advertising a new vehicle for $99 per month, but failing to disclose that after the first two payments, the payment amount increases to $525 for the remaining 70 months of the financing term.

3. **Undisclosed balloon payments.** This is where advertisements state a low monthly payment without clearly and conspicuously disclosing a large "balloon" payment at the end of the loan term. A balloon payment is one that is more than two times the regular periodic payment.

4. **False "$0 down" leases or sales. Claims that consumers can lease or finance for "$0 down" are a particular area of concern with the FTC.**

Did You Know?

Advertisements claiming "$0 down" to lease or finance a vehicle are a particular area of concern for the FTC.

If there are undisclosed fees or other charges due up front associated with the sale or lease (such as an acquisition fee or doc fees), or another requirement such as a particular credit score in order to obtain the no-down-payment treatment, the FTC may consider a $0 down claim to be deceptive.

5. **Hidden rates.** Claims of a low APR when the rate changes over time, or when most consumers won't qualify for that rate, can be deceptive unless these facts are clearly and conspicuously disclosed. For example, advertising a "0% APR for 60 months" promotion when the rate only applies if customers bought a new car for up to a certain dollar amount. Critically, Regulation Z and Regulation M set forth specific requirements concerning advertising credit. For additional information see "Credit Advertising" below.

6. **Bogus promotions or sweepstakes.** Dealers should not use so-called promotions or sweepstakes that are not genuine to bring customers to the showroom. FTC and state laws also require extensive disclosures in advertising contests or sweepstakes. This is discussed in more detail in

"Sweepstakes" below. An example is when a dealer mails out scratch-off sweepstakes cards to promote car sales, where every card scratched off indicates that the consumer is a winner, yet no one is awarded a prize.

Credit Advertising

TILA and Regulation Z, which apply to closed-end credit transactions, and the Consumer Leasing Act and Regulation M, which apply to consumer leases, all contain advertising requirements relating to credit terms. Under both Regulation M and Regulation Z, all disclosures must be made clearly and conspicuously. Further, Regulation Z permits creditors to state only those terms that actually are or will be arranged or offered by the creditor. If an advertisement states a rate of finance charge, it must state the rate as an "annual percentage rate," using that term.

Regulation M states that an advertisement for a consumer lease may state that a specific lease of property at specific amounts or terms is available only if the lessor usually and customarily leases or will lease the property at those amounts or terms.

Advertising the following "triggering terms" about closed-end credit requires additional disclosures:

- Down payment;
- Number of payments or period of repayment;
- Payment amount; or
- The amount of any finance charge in a credit sale.

If any of these terms are used, the advertisement must include the following terms:

- The down payment;
- Terms of repayment which reflect the repayment obligations over the full loan term, including any balloon payment; and
- The "annual percentage rate" or "APR" and whether the rate is subject to increase.

Similarly, for consumer leasing, if a lessor includes the following terms in an advertisement, they are considered "triggering terms":

- Any lease payment; or
- The capitalized cost reduction or other payment due prior to or at lease signing (or that no payment is required), or by delivery if delivery occurs after consummation.

If the advertisement includes any of these triggering terms, then the advertisement must also include the following disclosures:

- A specific reference that the advertised transaction is a lease;
- The total amount due at lease signing or by delivery if delivery occurs after consummation;
- The number, amounts, and due dates or periods of scheduled payments;
- Whether a security deposit is required; and
- A statement that an extra charge may be imposed at the end of the lease term where the lessee's liability (if any) is based on the difference between the residual value and its realized value at the end of the lease term.

Additionally, if an advertisement for a lease provides a percentage rate in an advertisement, the rate may not be more prominent than any of the required consummation disclosures (with the exception of the notice stating that "this percentage may not measure the overall cost of financing this lease" required to accompany the rate), and the lessor may not use the term "annual percentage rate," "annual lease rate," or equivalent term.

There are different rules for open-end credit. Both Regulation Z and Regulation M contain special rules for catalog and electronic advertisements, as well as television and radio advertisements.

You should consult with your local attorney to ensure that your advertisements comply with applicable law.

State Laws and Regulations

State laws on unfair and deceptive acts and practices are often even stricter than Section 5 of the FTC Act, and many State Attorneys General have guidelines for vehicle advertising in their state in both traditional and online media.

You should check with your attorney to make certain you comply with applicable state laws and rules.

Prescreening

You can "prescreen" a list of leads or even a single lead under the Fair Credit Reporting Act (FCRA). Prescreening is governed by the FCRA and involves giving a credit bureau a list of credit criteria for the credit bureau to produce a list of consumers meeting the criteria. (Under the "prescreen of one" model, the credit bureau applies the credit criteria to a single consumer and indicates whether or not the consumer meets them.) **FCRA requires dealers to make a "firm offer of credit" to these consumers, which the creditor is obligated to honor, provided the consumers continue to meet the prescreen criteria and meet any additional post-screen credit criteria as well as provide any required collateral.**

Did You Know?

FRCA requires auto dealers to honor any firm offer of credit made to prescreened consumer.

FCRA requires specific "clear and conspicuous" disclosures that must be included in the prescreen mailing, including conspicuously disclosing to the consumer how to opt out of further prescreening. The CFPB has issued a FCRA rule regulating the content and format of these disclosures, and the rule includes models that offer a compliance safe harbor. Dealers should apply the models for the most reliable approach to compliance with these disclosure requirements.

Prescreening differs from preapproval inquiries in that a consumer who meets the prescreen criteria must receive a firm offer of credit. Additionally, prescreening is generally initiated by the creditor, whereas preapprovals are generally initiated by the consumer. Persons who do not pass the prescreen criteria do not need to receive adverse action notices unless they otherwise affirmatively apply for credit and are declined.

A Wrinkle on Prescreening: "Trigger Leads"

Trigger leads are products created and sold by credit bureaus. Recall from Topic 3 that a consumer must provide his or her consent to have his or her credit report pulled as part of the loan application process. When the credit report is pulled during the loan application process, other competing lenders are notified that the consumer is shopping for credit. The credit bureaus do not communicate the consumer's name and contact information (usually a cell phone number) to the prescreen client until another auto dealer pulls the customer's credit report. In other words, one creditor's inquiry to a credit bureau regarding a consumer "triggers" the bureau to provide prescreened lead information about that consumer to a competing creditor. At that point, the prescreen/"trigger lead" client (typically a lender or another auto dealer in partnership with the lender) will call the customer on the customer's cell phone and attempt to induce them away from the original dealership that pulled the credit report. That inducement must be a valid firm offer of credit under FCRA because the trigger lead process is a form of prescreening. Often, the client will offer this inducement by claiming to offer better purchase or financing terms on the vehicle or aftermarket products. Some customers have been called on their cell phones while still in the original dealer's F&I office.

There is some general uncertainty as to the propriety of the trigger lead process in the context of indirect auto finance under federal and state law. The FTC has stated that the practice can be beneficial to consumers because

it can help them more easily identify other terms and loan offers. Although the FTC's guidance was issued in the mortgage context, it reasonably follows that the agency would look favorably on the practice in the auto lending context. While there have been efforts to ban trigger leads legislatively, no effort has yet been successful as of the date of this publishing.

To be sure, dealers should consult with legal counsel before participating in a trigger lead campaign.

Prequalifying Customers

Dealers can use their websites to market credit terms and prequalify customers even before taking a full credit application. Whether a prequalification is treated as merely an inquiry, or a credit application depends on what you communicate to the consumer. Please note that the distinction between inquiries and applications in the prequalification context is complicated and fact specific.

A consumer can securely provide personal information (e.g., name, address, birth date, Social Security number) over a secure webpage (an https page or by using encrypted data transfer) and give consent allowing the dealer to access their credit report, including their credit score, for prequalification purposes.

If a dealer responds by indicating the types of credit programs offered for which the consumer may qualify and how the consumer can submit a complete credit application, the prequalification process could be treated as an inquiry, which could subsequently trigger risk-based pricing or adverse action notice requirements. You can also communicate to the consumer that your dealership has many credit programs available and that you need additional information from the consumer to be able to pre-qualify them for one of the programs. Either way, suggest that the consumer come to the dealership or call your online sales manager.

If the dealer responds that there are no programs for which the consumer can qualify, then the dealer may be considered as having made a credit decision instead of treating it as an inquiry. In that case, the dealer would be required to send the consumer an adverse action notice. If you respond with information that indicates the consumer qualifies for specific financing, you have also made a credit decision and must provide the Risk-Based Pricing Notice or alternative Credit Score Disclosure Notice.

Dealers should work with legal counsel to ensure that their communications with consumers in the prequalification process do not inadvertently cross over from an inquiry into a credit application.

Sweepstakes

Sweepstakes or "games of chance" present additional challenges and are regulated principally by state laws and the FTC. Sweepstakes are comprised of the giving of a prize to a winner who is selected through an element of chance. To avoid a state law violation, sweepstakes must not require the giving of consideration in order to enter or win. To do this, a sweepstakes must give consumers the right to enter without making a purchase (such as by mailing in a postcard) or without requiring a substantial amount of the entrant's time or effort to participate. Sweepstakes can have a method of entry that requires payment, but only if there is a free alternative method of entry. Keep in mind that some states also prohibit or restrict prize promotions that require the entrant to attend a sales pitch, so it is best practice to consult an attorney familiar with your state's prize promotion laws.

For example, it would be a state lottery law violation to run a sweepstakes that is open only to consumers who purchased or leased vehicles. Instead, the sweepstakes should also be available without a purchase or lease by mailing in a postcard or filling out an entry form online. Some states require registration with state entities and bonding for certain consumer sweepstakes.

Before running and advertising a sweepstakes, you must have a full set of official rules setting forth details such as the method of entry, entrant eligibility, method of determining the winner, prizes, and odds of winning.

Recommended Practice

> Before running or advertising a sweepstakes, prepare a full set of official rules explaining the method of entry, entrant eligibility, method of determining the winner, prizes, and odds of winning.

The official rules also typically contain standard legal provisions such as releases, disclaimers, governing law, etc. The official rules form a contract between the sweepstakes sponsor (oftentimes the dealer) and the entrants. The official rules and all promotional materials must state that no purchase is necessary to enter and that making a purchase will not improve the chances of winning a prize. In addition, promotional materials should include a set of "abbreviated" official rules and should direct viewers to where they can find the full set of official rules. The sweepstakes provider must provide a notification system that allows consumers to have their names removed within 60 days from the mailing lists of that provider. In addition, the provider must report to the IRS the number of prizes received by certain winners.

Dealers that use prize promotions should consider seeking advice from an attorney familiar with the laws of the states where the sweepstakes will be conducted or with the appropriate government agencies in those states, because those laws can be complex. Attorneys can also help draft or review the official sweepstakes rules to ensure their compliance with applicable state laws.

Online ("Digital") Advertising

The use of digital media to promote businesses and their products is increasing at a rapid rate, and federal and state law enforcement agencies have responded accordingly. The most important thing to know is that **the same basic compliance rules that apply to other forms of advertising also apply to digital advertisements.**

Did You Know?

> The same basic advertising compliance rules also apply to digital advertising.

For example, representations must be true and substantiated and must include clear and conspicuous disclosures when necessary to dispel any misleading impression created by the ad.

The different characteristics of the Internet and the devices used to access it can create unique compliance concerns and make effective online media disclosures especially challenging, as the user experience can vary widely depending on the consumer and type of device. As in other media, online disclosures must be prominent and proximate to the claims or terms they are qualifying. Note: this can be very difficult to do on a mobile device with a small screen. In March 2013, the FTC issued an update to its Dot Com Disclosures guide to making effective online disclosures. The FTC emphasized that consumer protection laws apply equally to all advertising, regardless of the medium used, and include digital and social media. Disclosures required to avoid deception or otherwise comply with the law must be presented in a clear and conspicuous manner, and space constraints do not relieve the advertiser of this obligation.

In terms of prominence and placement, advertisers should be creative in using color, size, and graphics to make the disclosure more readily noticeable. Material disclosures should not be buried in long paragraphs of scrolling text, in the website's "terms and conditions," or in footnotes. They should be on the same screen as the claim they are qualifying and should be as close to the claim as possible. Generic statements such as "see below" are insufficient, especially if the consumer must scroll to see it. In some cases, it may be acceptable to use hyperlinks to take the reader to a separate page containing the disclosure, but only if the link itself is clear and prominent, takes the reader directly to the disclosure, and is labeled to explain the nature of the information and its importance (such as, "Click here to learn more about options you can purchase"). But hyperlinks cannot be used to communicate disclosures that are "an

Table of Contents

integral part of the claim." For example, disclosures about added fees and costs that consumers must pay to purchase the product should be in close proximity to the price claims and not on a separate screen or page.

Any elements of the ad that detract from the effective communication of a disclosure should be removed or altered. Pop-up disclosures typically do not comply because many consumers block pop-ups. A disclosure should be made in the same manner as the claim it qualifies and may need to be included each time the claim is presented. The content of the disclosures should be clear, simple, and straightforward. The test for whether a disclosure is effective is whether consumers can actually read, perceive, and understand it. Rapidly scrolling pages of text are likely to fail the test for acceptability.

For example, the FTC issued a complaint against an online lender in connection with its lack of prominent disclosures regarding fees because the company used methods such as pop-ups, scrolling, and fine print to qualify the nature of the fees. The FTC's complaint asserted that the fee disclosures were not clear and conspicuous and that this constituted a deceptive act or practice. In addition to the challenges posed by making disclosures on electronic devices, the FTC has identified three other major issues with online and social media advertising:

- **Native Advertising ("sponsored content")**. Promotional messages that blur the lines between advertising and "editorial" content are common on the Internet but may be deceptive. The FTC has issued an enforcement policy statement on "deceptively formatted advertisements," defined as promotional messages that are integrated into and indistinguishable from non-promotional content, such as news, featured articles, or product reviews. The policy statement states that advertising and promotional messages that are not readily identifiable as such are deceptive because they are likely to mislead consumers into believing the messages are independent and impartial.

  In these situations, the advertiser must clearly and conspicuously disclose that the embedded message is an advertisement, for example by putting the phrase "PAID ADVERTISEMENT" at the top of the message.

- **Deceptive Endorsements/Testimonials/Customer Reviews**. Endorsements, testimonials, and customer reviews are a hot topic at the FTC. Importantly, all endorsements/testimonials/customer reviews should reflect the honest opinions, beliefs, and experiences with using the advertiser's products or services. In addition, whenever there is a "material connection" between the advertiser and the person making the endorsement or providing the testimonial/review, that material connection must be disclosed. A "material connection" can be any of the following: monetary payment; the offering of an incentive such as a coupon, discount, or sweepstakes entry; providing free product; an employment or contractor relationship; and a family relationship. The type of disclosure will depend on the type of material connection. For example, someone paid to promote the advertiser will typically include #ad in the post or will state #freegift if the advertiser provides a free product. However, if one of the advertiser's employees posts about the advertiser's products (or about competitors' products), the disclosure would typically look something like #[advertiser]employee. The FTC's Guides Concerning the Use of Endorsements and Testimonials in Advertising ("FTC Endorsement Guides"), which set forth these rules, are described in more detail below.

- **Online Influencers**. The FTC has indicated that it will continue to monitor the use of online influencers for compliance with the FTC Endorsement Guides. Specifically, the FTC will assess whether the influencer made an appropriate material connection disclosure. The FTC may pursue enforcement action against both the influencer as well as the advertiser. If you engage influencers, it is important to have an agreement in place and to train the influencer on "do's" and "don'ts." You should monitor the influencer's posts to make sure the requisite disclosures are made and reach out to the influencer for corrective action in the event of

noncompliance. And remember, **the influencer cannot make any advertising claim that the advertiser cannot make itself.**

Compliance Tip

If you use an online influencer to promote your dealership or related products or services, ensure the influencer does not make any advertising claim that you could not also make.

As with the use of endorsements/testimonials/customer reviews, this is another area of importance for the FTC.

Social Media Advertising

Social media sites allow dealers to connect with consumers through consumers' principal means of staying in touch with friends, colleagues, and companies with whom they share an interest or have a relationship. Increasingly, advertisers are using social media to disseminate commercial messages, and government regulators are actively monitoring social media to look for deceptive practices in connection with those messages. The suggestions for advertising practices described above, including those described as part of the FTC's Dot Com Disclosures guide, should be reviewed to help advertisers make effective online disclosures.

Advertisers on social media must make sure that (i) their claims are truthful and substantiated, (ii) all required disclosures are clear and conspicuous, and (iii) advertising content is clearly distinguished from non-commercial content.

Compliance Tip:

Advertisements on social media must include:

- Truthful and substantiated claims;
- Clear and conspicuous disclosures; and
- Distinguishment from non-commercial content.

Several of the FTC's deceptive advertising cases have addressed social media advertisements. The ads came to the FTC's attention as a result of FTC staffers searching the Internet and finding the ads on sites such as YouTube.

Any dealership that plans to launch a social media presence, or whose employees have access to and use such sites, should adopt a Social Media Policy. The policy should place reasonable limits on employees' use of social media in a way that can be tied to the dealership. Relatedly, if the dealership has its own social media accounts, policies should be set for who can access/post from those accounts and what they can/cannot say.

FTC Endorsement Guides

In 2009, the FTC issued revised guidelines on the use of endorsements and testimonials in advertising. The FTC Endorsement Guides include the following:

- There are several kinds of endorsers, including experts providing their expert opinions about the advertised product, consumers relating their experiences with the product (commonly referred to as "testimonials"), and organizations that may grant some sort of certification or approval. On the other hand, individuals who are merely spokespersons and are not purporting to provide their own opinions or experiences are not covered by the FTC Endorsement Guidelines. Nor are bloggers or others who go on review websites and provide their opinions, so long as they are not connected in any way with the advertiser;
- Endorsements must reflect the honest opinions, beliefs, or experiences of the endorser. Any claims made by the endorser beyond this must be true and substantiated. In other words, if the claim would have been deceptive if made directly by the advertiser, it is deceptive when made by the endorser;
- Endorsements may not be presented out of context or reworded in a way that distorts the endorser's opinions or experiences. If the endorser is presented as a user of the product, he or she must have actually used it; and

- The experiences related in consumer testimonials must reflect the typical, or representative, experience of consumers generally. If they do not, the advertiser must clearly and conspicuously disclose what the typical experience is. A disclosure like "results not typical" or "results may vary" is not sufficient.

If there is a material connection between the endorser and the advertiser that might affect the weight or credibility of the endorsement, that connection must be disclosed clearly and conspicuously. A material connection could include the payment of compensation or providing free products to the endorser, for example, an endorser who touts her experiences with the product on a social networking site in exchange for free product or payment of money.

Other Advertising Guidelines

The FTC has published additional advertising guidelines that often apply to dealers. One example concerns the use of the word "free" in advertising. **The FTC prohibits use of the word "free" in describing a product if that product is sold with another product or service as to which the price is arrived at through bargaining.**

Did You Know?

The FTC prohibits use of the word "free" in describing a product if that product is sold with another product or service as to which the price is arrived at through bargaining.

FTC guidelines also warn that it is deceptive to advertise a discount unless the price is less than the regular price of the product. For example, an advertiser cannot raise the regular price of a product and then advertise a discount on that inflated price. Statements such as "repossession sale," "fleet liquidation," "end-of-lease sale," or other unusual sale circumstances must be true in fact. If a vehicle is advertised at "factory invoice" or the like, the terms must represent the dealer's ultimate total vehicle cost, including any holdbacks or manufacturer incentives. Advertisements for a particular product need to include a disclosure if there are limited quantities of that product available. And advertisers should not engage in "bait and switch" advertising.

State Advertising Laws and Regulations

Almost all states have laws specifically prohibiting misleading advertising. The state standards summarized in this section are for example purposes only. This section does not provide a comprehensive review of all state laws regulating advertising. An example of a relevant regulatory scheme is Florida, which prohibits any statement known or which could have been ascertained to be untrue or misleading and which was made with the intent or purpose of selling goods or services. Mississippi lists a series of phrases that are deemed to be untrue including "everybody financed," "no credit rejected," "name your own monthly payments," and a statement that no other dealer gives a greater allowance for trade-ins.

A number of state laws give consumers a right to sue for misleading advertising and specifically provide that a consumer can recover attorney's fees and punitive damages. Other states specifically prohibit using any unexplained abbreviations in dealer advertising that are not commonly understood and lists FTB, A/R, TOP, POF, and DOC as examples.

The advertising requirements for dealers are different in each state. The Attorney General and state Motor Vehicle Department websites are two good resources to find rules and regulations concerning what activities are permissible and impermissible for auto dealer advertising. Attorney General websites usually publicize enforcement actions brought against auto dealers for deceptive trade practices, including deceptive advertising. Many State Attorney General offices publish specific guidelines for auto dealer advertising in their respective states, as well.

For example, **many states prohibit a dealer from selling a vehicle at a price higher than an advertised price even if the consumer has not seen the advertisement.**

Did You Know?

Many states prohibit a dealer from selling a vehicle at a price higher than an advertised price even if the consumer has not seen the advertisement.

Table of Contents

In some states, this rule will not apply if the advertisement provides clearly and conspicuously that the consumer must bring in or at least mention the advertisement to get the advertised price. A number of states also have laws governing advertising of rebates. There are states that require a disclaimer that dealer participation may affect consumer cost when a dealer must contribute to the cost of an incentive in order to participate in a manufacturer or distributor incentive.

You should check all your advertising against your state guidelines as well as the FTC's rules and guidelines. In the present environment of aggressive enforcement, it is a best practice to have your local attorney review all advertising. It is also important to have staff that track advertised vehicle prices to ensure that all price listings regardless of where posted reflect the most up-to-date prices.

Important Laws and Regulations

FTC Used Car Rule

The FTC Used Car Rule (the "Rule") requires auto dealers to prominently post a "Buyer's Guide"

Compliance Tip

Used cars must be displayed with a Buyer's Guide that includes warranty and other consumer information.

in plain view on all used vehicles before they are offered for sale. The Rule defines a "used car" as any car that has been driven more than necessary to move it or for road testing prior to delivery to a consumer. This would include many "demo" models used for customer test drives. The Buyer's Guide must disclose whether the vehicle is being sold "as is" or with a warranty. State law governs the legal requirements for disclaiming warranties and will determine whether a dealer must use the "As Is – No Dealer Warranty" or "Implied Warranties Only" version of the Buyer's Guide. If the vehicle is sold with a written warranty, the Buyer's Guide must state the general terms of the warranty, including whether it is full or limited; the duration of the coverage; the specific systems covered (engine, transmission, etc.); a list of parts or systems not covered if necessary for clarity (e.g., a battery); what percentage of repair costs the dealer will pay under the warranty; an explanation of how the customer gets warranty service; and whom to see about complaints.

The Buyer's Guide must also tell consumers that (1) oral promises are difficult to enforce and that consumers should get all promises in writing, (2) the major mechanical and electrical systems on the car that are covered by the warranty, (3) the major problem areas that consumers should look for, (4) that they should ask to have the car inspected by an independent mechanic before they buy, and (5) that they should obtain a vehicle history report and check for open recalls at the government website: www.nhtsa.gov. If a used car transaction is negotiated in Spanish, the dealer must post a Spanish language Buyer's Guide. In addition, the English version of the Guide must advise Spanish speakers, in Spanish, to ask for the Spanish version. The Buyer's Guide becomes part of the sales contract, and the disclosures cannot be contradicted orally or in writing. In addition to the Buyer's Guide, the dealer must provide a separate warranty document, unless the dealer is not selling the used vehicle with its own warranty. The Buyer's Guide is not a warranty document. The Buyer's Guide also includes a non-dealer warranties section for a dealer to disclose whether the original manufacturer's warranty, manufacturer's used vehicle warranty, or other used vehicle warranty applies. A dealer may also disclose whether a service contract is available to purchase in this section.

The FTC is actively monitoring dealers' compliance with the Used Car Rule. In 2018, the FTC, working jointly with 12 partner agencies in seven states, conducted the first compliance sweep of car dealerships since the Rule was amended. Following the sweep, the FTC notified the inspected dealerships of the inspection results and indicated that dealerships not displaying the revised Buyer's Guide can expect follow-up inspections to ensure that they have brought themselves into compliance. More recently, in 2024, the FTC brought an enforcement action against a former online used car dealer for failing to display a Buyer's Guide in the used cars listed on the dealer's website.

The Used Car Rule applies in all states except for a few that have enacted their own state law provisions, such as Maine and Wisconsin, that require notices with additional disclosures for used car sales.

Magnuson-Moss Warranty Act

The Magnuson-Moss Warranty Act (MMWA) is a federal law that requires manufacturers and sellers to disclose information about warranties given with the sale of a product. A warranty is a statement or representation, express or implied, about the character or quality of the goods sold. Express warranties result from statements or affirmations made about a product that the buyer relies upon in deciding to purchase. The MMWA covers written express warranties. Implied warranties derive from state law and automatically attach to the vehicle from the sale, such as an implied warranty of merchantability, which is a promise the vehicle will perform in a manner fit for its usual and ordinary purposes.

The MMWA requires any written warranty to be clearly and conspicuously labeled as “full” or “limited,” to be described in a single, easy-to-read document, and to state any qualifications to the warranty (such as the consumer performing scheduled maintenance) with the full warranty terms available. At a minimum, the document must describe who is making the warranty; when the warranty begins and ends; what is covered and what is not; what the warrantor will do if there is a problem; and how the consumer can obtain warranty service. It must also indicate that the consumer may have additional rights under state law and contain the following specific disclosures: “This warranty gives you specific legal rights, and you may also have other rights which vary from state to state. Some states do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you.” If a dealer sells the customer its own service contract within 90 days of the vehicle sale (as opposed to the consumer purchasing a service contract from a third party), the dealer cannot disclaim any implied warranties, but the duration of implied warranties can be limited under certain circumstances.

A common misconception concerns the concept of a warranty versus an “extended warranty” or service contract. For a new car, a warranty is included in the vehicle price, and it provides the customer a right from the manufacturer to obtain certain repair services that must be adequately described under MMWA. Manufacturer warranties do not cover aftermarket products such as dealer-added equipment. Some vehicle manufacturers permit transfer of unexpired warranties to subsequent purchasers, and state laws restrict or limit any charges that can be imposed for doing so. Used car dealers can also provide warranties for the vehicles they sell, but a dealer cannot charge a customer for a warranty; it must be included in the cost of the vehicle. If the customer pays separately for additional coverage or an “extended warranty,” that is a “service contract.”

An “extended warranty” is somewhat of a misnomer. Any product that provides for repair or servicing of the vehicle after the original manufacturer’s (or seller’s) warranty expires and for which the customer pays an additional charge is generally deemed to be a “service contract,” not a warranty. Service contracts can be sold directly by the dealer or by a third party. They do not extend the manufacturer’s warranty obligation but give the consumer a contractual right against the seller of the service contract in the event of a breakdown or service need. Under MMWA and state law, a consumer’s legal rights and remedies will be different for warranties and service contracts.

Some states require implied warranties in any vehicle sale. Other states permit “as is” sales of used cars. Used car warranties and the availability of a manufacturer’s warranty must be disclosed in the Used Car Buyer’s Guide discussed earlier in this Topic.

In 2015, President Obama signed the E-Warranty Act, which does away with a requirement that has been on the books since passage of the MMWA that compelled manufacturers to include warranty terms on a single printed document on or within packaging of products costing more than $15.

The E-Warranty Act instead permits, but does not compel, manufacturers to avoid the requirement by directing consumers to their websites to find the terms and conditions of their consumer warranties.

Recommended Practice:

Direct customers to your website for terms and conditions of consumer warranties rather than only providing customers with a paper copy.

Pursuant to the FTC's rules implementing the E-Warranty Act, which took effect in 2016, if a warrantor or seller opts to post warranty terms electronically, the warrantor or seller must: (i) provide consumers the Internet address of the website where the warranty terms can be reviewed; (ii) provide a non-Internet based method, such as a phone number or mailing address, for consumers to request the warranty terms; upon request, the warrantor must provide the warranty terms promptly and free of charge; (iii) ensure that all required warranty terms are posted in a clear and conspicuous manner and that any limitation on implied warranties appears in close proximity to the location where the text of the warranty terms begin; and (iv) ensure that warranty terms remain accessible to the consumer on the warrantor's website.

FTC Warranty Rules

Two additional FTC rules, the Consumer Product Warranty Rule (Warranty Rule) and the Rule Governing Pre-Sale Availability of Written Warranty Terms (Pre-Sale Availability Rule), specify language for warranties, require that warranties be displayed in close proximity to the vehicle, and mandate that the full warranty terms be made available to consumers upon request before they buy. State laws, such as the California and Minnesota Car Buyer's Bill of Rights, provide minimum requirements for dealers to be able to use the term "certified" (or any similar term) in connection with a used car sale, and require other warranty and used car disclosures, as well.

Recommended Practices

1. **If you conduct direct marketing, periodically scrub your target lists for persons who have excluded themselves from the means of communication you intend to use (telemarketing, faxes, and email).**

Recommended Practice

Periodically scrub your direct marketing target lists to remove people who do not wish to be contacted via the means of communication you plan to use.

You should keep a separate list of consumers who opt out of telemarketing (calls and text messages), faxes, and email, and be careful before using an auto dialer or prerecorded message to obtain the appropriate consents from the party you are calling or texting. This consent must include specific disclosures and comply with specific content requirements. Adequately scrub telemarketing lists of phone numbers against the FTC's National Do Not Call Registry, your state's Do-Not-Call list, and your dealership's list of persons who have asked not to be called. The Association of National Advertisers (www.ana.net) also maintains "do not contact" lists that you should scrub your lists against. If you are telemarketing, get assurances from vendors on having obtained customer consents and exclusions of persons listed on federal and state Do-Not-Call lists, then double-check against Do-Not-Call lists, as well as your own dealership's list of customers who have asked not to be called. The class action liability potential under the TCPA makes this a critical area for you to be compliant. Also, note that many State Attorneys General and Motor Vehicle Departments have their own rules or guidelines for advertising motor vehicles.

2. **Advertisers must ensure that any express or implied claims made in their advertisements are truthful and substantiated.**

Recommended Practice

Make sure any express or implied claims made in your advertisements are truthful and substantiated.

Remember that every statement in an ad can be literally true, but if its net impression is misleading, the ad is deceptive. Be able to prove the truth of every statement made or implied in your advertising and consider your advertising's net impression. For example, if you are advertising sales of repossessed or off-lease vehicles, be prepared to show that substantially all of the vehicles meet those criteria. If your ad says "factory authorized," be prepared to produce the written "factory authorization" that supports that statement. Be wary of advertisements promising credit to subprime borrowers (e.g., "bankruptcy not a problem").

3. **Don't stack rebates to advertise the price of a vehicle. Rebates that are available to the general public can be itemized as deductions from the MSRP.**

Recommended Practice

> Don't stack rebates to advertise the price of a vehicle.

You can show additional conditional rebates separately from the vehicle pricing and those should be itemized along with a clear and conspicuous explanation of the qualifications for each. Note that state laws also govern the advertising of rebates such as the California and Nevada laws referenced above. If an advertisement would mislead consumers in the absence of additional information, the disclosure of that information must be "clear and conspicuous." Advertisers should apply the four P's of effective disclosures – prominence, presentation, placement, and proximity – as a starting point. The FTC has stated that if a disclosure is not made clearly and conspicuously, it is the equivalent of not making the disclosure at all. Avoid putting required disclosures in fine print or in a color that blends into the background or in pop-ups on websites. Use plain English and don't use abbreviations not commonly understood by the public. Fast-talking TV or radio disclaimers are also problematic. The CFPB specifically has cited fast-talking telemarketers as part of a deceptive selling process.

4. **If you use an advertising agency, try to get the agency to indemnify you if the ads it produces lead to litigation or an FTC or Attorney General action.**

Recommended Practice

> Try to get any advertising agency you use to indemnify you from litigation or regulatory action.

It is a best practice to have your attorney review all your contracts with advertising agencies, influencers, or other advertisers before execution, as well as review all your advertisements before publication.

5. **Use caution when promoting your products in digital media, to ensure disclosures remain clear, accurate, and compliant across all devices or platforms.**

Recommended Practice

> Use caution when promoting your products in digital media, to ensure disclosures remain clear, accurate, and compliant across all devices or platforms.

Remember that advertising online must be considered from the perspective of all devices that will be used to view it, including cell phones and tablets., so make all disclosures are clear and conspicuous regardless of how they are displayed.

6. **Be sure to disclose any material connections between you and an endorser of your product, including if the endorser is receiving monetary or other compensation.**

Recommended Practice

> Be sure to disclose any material connections between you and an endorser of your product, including if the endorser is receiving monetary or other compensation.

If you engage online influencers, be sure to have an agreement in place, train the influencer on “do’s” and “don’ts,” monitor the influencer’s posts for compliance, and require corrective action in the event of noncompliance

7. Adopt a social media policy in accordance with the guidelines described above and in consultation with your attorney or compliance professional.

Recommended Practice

Adopt a social media policy in accordance with the guidelines described above and in consultation with your attorney or compliance professional.

Make sure that your social media policy protects against improper disclosure of company or consumer information but does not inhibit the employee from making appropriate posts.

8. The FTC’s website, www.ftc.gov, and State Attorney General websites provide a great deal of information on auto dealer advertising guidelines.

Compliance Tip:

Look for auto dealer advertising guidelines at ftc.gov and your state attorney general’s website.

Checking those websites to see recent enforcement proceedings involving auto dealer advertising can also be helpful.

9. Understand the state law concerning a dealer’s ability to disclaim warranties.

Recommended Practice

Be sure you understand state law regarding a dealer’s ability to disclaim warranties.

Make sure it is clear in the service contracts you sell whether you have “entered into” the service contract, in which event you cannot disclaim implied warranties under the MMWA discussed in this Topic. Service contracts and insurance contracts to cover the obligations can be structured in a number of different ways, each of which has different tax and liability issues. Two examples are “retro” policies and “reinsurance” policies. In “retro” policies, a portion of the customer premiums is sent by the dealer to an insurer who deposits it into an account to pay claims. When contracts expire, or at other predetermined times, the dealer receives a portion of the earned premiums. In reinsurance policy programs, the dealer sends a fixed amount to an insurance company who in turn cedes the amount to a reinsurance company that may be affiliated with the dealer. The insurer offsets claims payments against sums paid to the reinsurance company. State insurance laws also contain requirements for insurance and reinsurance for service contracts. Review how your service contracts are structured and insured with your lawyer and accountant.

Additional Resources

FTC, Advertising Consumer Leases (January 2024)
https://www.ftc.gov/business-guidance/resources/advertising-consumer-leases

FTC, Advertising FAQ's: A Guide for Small Business (January 2024)
https://www.ftc.gov/business-guidance/resources/advertising-faqs-guide-small-business

FTC, Advertising and Marketing on the Internet (January 2024)
http://business.ftc.gov/documents/bus28-advertising-and-marketing-internet-rules-road

FTC, Dealer's Guide to the Used Car Rule (January 2024)
http://business.ftc.gov/documents/bus13-dealers-guide-used-car-rule

FTC, Businessperson's Guide to Federal Warranty Law (March 2018)
https://www.ftc.gov/tips-advice/business-center/guidance/businesspersons-guide-federal-warranty-law

FTC, Answering Dealers' Questions About the Revised Used Car Rule (September 2017)
https://www.ftc.gov/business-guidance/resources/answering-dealers-questions-about-revised-used-car-rule

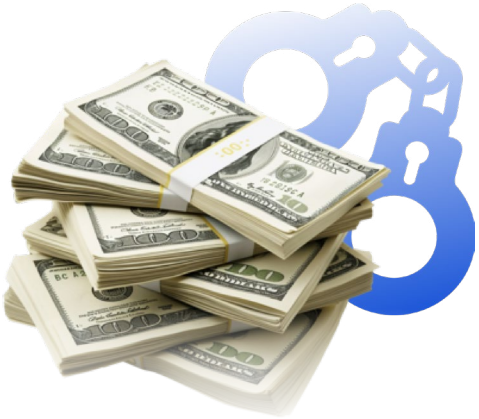
Federal Reserve, Consumer Compliance Handbook: FTC Act Section 5 (December 2016)
www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf

Auto Dealer Today, Social Media Guidelines for Dealerships (July 2012)
https://www.autodealertodaymagazine.com/310057/social-media-guidelines-for-dealerships

Digital Advertising Alliance, Self-Regulatory Principles for Online Advertising
http://www.aboutads.info/principles/

Unfair and Deceptive Practices (UDAP) Laws

Establishing ethical conduct toward customers can save your dealership time and money that might otherwise be spent addressing complaints, recovering from bad reviews, or even defending against legal actions for unfair, deceptive, and abusive trade practices (UDAP).



Adopt a culture of fairness and honesty toward customers →

Did You Know?

Regulators may bring enforcement actions against your employees, and not just your dealership or general manager, for UDAP violations. Learn more

Compliance Tip

Public reviews or ratings about your dealership or your products and services should be posted by customers and not by you or your employees. Learn more

What's New for 2025

Set to take effect in 2025, pending legal challenges, the FTC's CARS Rule prohibits broad categories of UDAP in the auto industry, including auto pricing or financing misrepresentations, unclear offering price disclosures, and unwanted add-on charges. Auto dealers should familiarize themselves with the CARS Rule to avoid legal actions and penalties for practices considered UDAP under the Rule. Learn more

Recommended Practice

Make sure your advertising on social media or online follows the same UDAP laws and regulations applicable to any other advertisements. More Recommended Practices

Breakout Sections

1. Important Laws and Regulations
   - Section 5 of the FTC Act
   - Unfair Trade Practices
   - Deceptive Conduct
   - Abusive Practices
   - State UDAP Laws
   - Criminal Liability for Deceptive or Unfair Dealer Practices
2. Recommended Practices
3. Additional Resources

Unfair and Deceptive Acts and Practices (UDAP) Laws

UDAP laws are designed to protect consumers from unfair and deceptive trade practices in the marketplace, including false or misleading advertising. They cover any merchants of goods and services generally, not just auto dealers. These laws were originally passed to ease the legal burden for proving common law fraud. The original UDAP law is Section 5 of the Federal Trade Commission (FTC) Act, which prohibits unfair and deceptive acts and practices. However, the FTC Act does not afford consumers any private right of action, and many practices require the FTC to first obtain an enforcement consent order prior to seeking the up to $51,744 per violation penalty that the Act permits if the consent order is violated.

Under Section 5 of the FTC Act, an act or practice is unfair when:

Did You Know?

The FTC considers an act or practice to be unfair when it is likely to cause substantial injury to consumers that they cannot reasonably avoid and it is not outweighed by its benefits.

- It causes or is likely to cause substantial injury to consumers;
- The injury is not reasonably avoidable by consumers; and
- The injury is not outweighed by countervailing benefits to consumers or to competition.

A substantial injury typically takes the form of monetary harm, such as fees or costs paid by consumers, because of the unfair act or practice. However, the injury does not have to be monetary; emotional or other impact and other more subjective types of harm may constitute a substantial injury. Injury can be substantial if it causes a small harm to a large number of people or a severe harm to a small number of people. An injury also does not need to have already taken place. It is sufficient that a practice is likely to cause substantial consumer injury in order to be actionable.

An injury is not reasonably avoidable by consumers when an act or practice interferes with or hinders a consumer's ability to make informed decisions or to take action to avoid that injury. Injuries caused by transactions that occur without a consumer's knowledge or consent are also not reasonably avoidable. Injuries that can only be avoided by spending large amounts of money or other significant resources also may not be reasonably avoidable.

Finally, to be unfair, the injury must not be outweighed by offsetting consumer or competitive benefits that the practice also produces. Offsetting benefits may include lower prices for consumers or the wider availability of products or services. The cost to the company of removing the injury is also a consideration.

An act or practice is deceptive when:

Did You Know?

The FTC considers an act or practice to be deceptive when it is likely to mislead a consumer, is material to their decision, and their interpretation of it is reasonable under the circumstances.

- The act or practice misleads or is likely to mislead the consumer;
- The consumer's interpretation of the act or practice is reasonable under the circumstances; and
- The misleading act or practice is material (generally significant enough to cause consumer harm).

Most deception cases involve some form of communication to consumers — whether it be an advertisement, a sales technique, or a contractual provision. The initial inquiry for deception concerns whether the communication is misleading to consumers. To determine whether a communication is misleading, the totality of the circumstances is considered. This includes both express and implied claims or representations about a product or service, as well as deceptive omissions from communications.

The meaning of a communication is determined from the perspective of a "reasonable" consumer. It does not mean someone who is highly sophisticated or educated, but where a communication is directed at a particular audience, the inquiry focuses on a reasonable member of that group. Whether an act or practice is material concerns the importance of the information to consumers. A material misrepresentation or omission is one which is likely to affect a consumer's choice or conduct regarding a product or service.

All 50 states and the District of Columbia have also enacted their own state UDAP laws. In addition to these laws authorizing Attorney General actions, **many state UDAP laws give consumers a private right of action to obtain injunctions and recover actual damages, court costs, and attorney's fees.**

Did You Know?

Most states only allow their governments to bring legal actions under UDAP laws, but some states also allow consumers to file UDAP lawsuits.

Many of the laws also permit recovery of statutory, punitive, or treble damages as a deterrent to deceptive or unfair business conduct. Some state UDAP laws permit a consumer to bring a lawsuit as a private Attorney General. Most state UDAP laws allow class actions, as well.

This Topic discusses auto dealer liability risks for UDAP practices under the FTC Act, the Dodd-Frank Act, and state UDAP laws. As these laws are a "catch all" for bad conduct, they present a substantial risk for a variety of misdeeds in selling vehicles to, or financing vehicles for, consumers.

Important Laws and Regulations

Section 5 of the FTC Act

Section 5 of the FTC Act prohibits "unfair methods of competition and unfair or deceptive acts and practices in or affecting commerce" against consumers. Enforcement authority is vested in the FTC, and the FTC has not hesitated to use its authority, most recently for lax data security practices that it considers to be an unfair act or practice, and for deceptive dealer advertising as discussed in Topic 7. The FTC can bring an administrative enforcement action and, depending on the nature of the violation, bring a court action to seek injunctive relief or damages. States look to FTC lawsuits on UDAP violations or consent decrees as precedent for their own state UDAP actions.

Recent FTC enforcement actions for UDAP violations include: actions against auto dealer groups and dealerships for charging more junk fees to customers of certain minority races or ethnicities, actions against auto dealers for misleading customers into believing optional add-on products (e.g., GAP insurance, payment insurance, and paint protection) were required with a vehicle purchase, and a settlement with an auto dealer software company that failed to implement reasonable security measures to prevent a breach of client data. States are also collaborating with the FTC to bring UDAP actions against dealers engaged in illegal activity in their state. For example, in 2024, the Arizona Attorney General worked with the FTC to obtain $2.6 million from an auto dealer group and its general manager for using bait-and-switch tactics through deceptive advertising and discriminating against Latino customers when offering auto financing.

Unfair Trade Practices

The FTC has stated that "unjustified consumer injury is the primary focus of the FTC Act." As noted above, the FTC's standard for "unfairness" is: (i) whether the practice creates a substantial consumer injury; (ii) whether the injury exceeds any offsetting consumer benefits or competitive benefits; and (iii) whether the injury was one that consumers could not reasonably have avoided. The FTC considers "deceptive" practices to consist of any material representation, omission, or practice that is likely to mislead a consumer, as examined from the perspective of a reasonable consumer. An "unfair" practice may not be "deceptive," and some deceptive practices may not be unfair. The legal standards are independently applied.

The FTC may also consider public policy in determining whether an act or practice is unfair, but it may not solely rely on public policy in making its determination. The FTC has also been given a streamlined process

to issue new rules and regulations for auto dealers' unfair and deceptive trade practices by the Dodd-Frank Act. Previously, the FTC had to conduct detailed studies and hold hearings under procedures contained in the Magnuson-Moss Warranty Act and demonstrate that the prohibited act was "prevalent" in the industry. Now, the FTC merely needs to publish proposed regulations for a comment period and then can adopt final rules or regulations after reviewing the comments without having to make the prior showing that the regulated practices are "prevalent."

One authority has indicated that the lead time for the FTC to enact unfair or deceptive practice regulations against auto dealers has been reduced from approximately seven years to one year. In 2011, the FTC conducted a series of roundtable hearings on dealer auto finance practices, and the agency continues to investigate practices like spot deliveries, with the intent to use its new streamlined authority to restrict or limit improper dealer practices or require more transparent disclosures to consumers. The FTC's recent finalization of the CARS Rule in 2024 is an example of its commitment to regulate UDAP in the auto industry. **Until the CARS Rule becomes effective in 2025, pending current legal challenges against the Rule, the FTC will continue following the CFPB's general practice of "regulating by enforcement," which means bringing enforcement proceedings against dealers who are engaging in an unfair or deceptive practice, thereby putting other dealers on notice that the practice violates the FTC Act.**

Compliance Tip

The FTC and CFPB primarily regulate UDAP in the auto industry through enforcement actions, so auto dealers should monitor recent enforcement actions to learn which practices to avoid.

Deceptive Conduct

Most auto dealer deceptive conduct involves failure to make required disclosures (e.g., triggered terms under TILA or the CLA when a dealer advertises a payment amount), written or oral misrepresentations, or omissions of both in advertisements and in personal dealings with a consumer.

Did You Know?

Most auto dealer deceptive conduct involves failure to make required disclosures, written or oral misrepresentations, or omissions of both in advertisements and communications.

The issue is whether the act or practice is likely to mislead a consumer, rather than whether it actually misleads the consumer. The FTC considers all of the facts and circumstances of a transaction in order to reach this conclusion. The FTC has focused on deceptive dealer advertising over the past decade, including its 2014 Operation Steer Clear and its 2015 Operation Ruse Control targeting dealer ads. In 2020, the FTC released a staff report on the car buying and financing experience, as well as the results of an auto buyers study, highlighting consumer concerns throughout the entire buying and financing process. In 2024, the FTC released multiple Supervisory Highlights analyzing misleading advertising of APR rates and improper disclosures of loan prepayment penalties by auto dealers, among other issues.

The FTC has pursued numerous deceptive practice claims against auto dealers. For example, FTC regulations set forth restrictions on advertising practices it considers to be deceptive, such as "bait and switch" advertising and advertising discounts from MSRP when few to no sales below MSRP take place in the dealer's geographic area. Another deceptive practice is "rebate stacking," where multiple rebates available only to select groups (military, recent college grads, first time car buyers, etc.) are advertised together to calculate a vehicle price, even though few, if any, consumers will qualify for all of them.

The FTC has brought complaints against dealers for misrepresenting the down payment in lease and financing transactions; failing to disclose fees and security deposits; advertising that vehicles had passed multiple inspections when they had not; selling vehicles with known defects that consumers were not able to determine (e.g., selling new vehicles with paint defects likely to cause rust, odometer rollbacks, and other concealment of conditions on used vehicles); selling vehicles that are subject to an open recall while advertising a rigorous pre-sale inspection; discriminating against certain protected classes of potential buyers (such as buyers of a

Table of Contents

particular race or religion); and payment packing. The FTC has indicated that advertising the fuel economy of vehicles can also trigger liability.

The FTC has further taken the position that no item can be advertised

Compliance Tip

Don't use the word "free" in your advertising without knowing the limitations.

as "free" when the primary item being sold (such as an automobile) is subject to a negotiated price. In fact, the FTC has issued an entire regulation on when the word "free" can be used in advertising without being deceptive. The regulation applies to all businesses, not just to auto dealers, and provides that "all the terms, conditions and obligations upon which receipt and retention of the 'Free' item are contingent should be set forth clearly and conspicuously at the outset of the offer" to avoid misleading consumers. 16 C.F.R. § 251.1. Since 2012, the FTC has brought more than 30 deceptive practice enforcement actions against dealers. Four involved dealers who advertised that they would pay off a customer's trade-in balance even if the customer was "under water." At least five enforcement actions involved dealers advertising prices and discounts that were either not available to all consumers or that were deceptive in terms of being available only on higher-priced, "loaded" vehicles. Other actions are discussed earlier in Topic 7, including deceptive pricing, concealment of terms, and making the advertised terms available on only a small number of vehicles.

The FTC is becoming very watchful of dealer advertising, especially online and on social media.

Recommended Practice

Ensure you are following applicable laws and regulations with your online and social media advertisements.

For example, the FTC requires disclaimers or qualifications to be displayed "clearly and conspicuously" and in close proximity to the advertised language they qualify.

The term "advertising" should also be viewed broadly. In 2016, the FTC brought a UDAP enforcement action against an auto dealer for posting fake positive reviews about the dealership on social media, which the FTC found to be deceptive advertising. Each of the enforcement actions brought by the FTC involved consent orders that can last up to 20 years, and many of the consent orders may be followed by class action lawsuits for state UDAP claims, as FTC consent orders can provide a roadmap to plaintiffs' lawyers.

The FTC also recently finalized its CARS Rule aimed at banning bait-and-switch advertising tactics by auto dealers.

Watch List for 2025

The CARS Rule is expected to take effect in 2025 to prohibit broad categories of UDAP in the auto industry.

Expected to take effect in September 2025, unless pending legal challenges against the Rule succeed, the Rule would prohibit dealers from making deceptive advertising claims to lure in prospective buyers regarding vehicle cost, terms of financing, availability of discounts and rebates, actual availability of cars advertised, and other aspects. **The Rule would also prohibit auto dealers from causing reviews or ratings of their dealerships or related products or services to be posted that are not "unbiased, independent, or ordinary consumer reviews or ratings."**

Compliance Tip

Reviews or ratings posted online about your dealership or your products and services should be posted by your customers and not by you or your employees.

The FTC continues to regularly exercise its UDAP authority and in novel ways. For example, the FTC charged a dealership group with falsifying consumers' income and down payment information on vehicle financing applications and misrepresenting financial terms in vehicle advertisements. This was the first time the FTC had brought such an income falsification claim. The FTC also brought a challenge against dealership employees, rather than just the dealership or general manager, for deceptive practices in advertising and sales of used cars.

In addition, the FTC continues in its more traditional pursuits of advertising and disclosure violations, including recall notices used as a tool to increase business.

Did You Know?

Regulators may bring enforcement actions against your employees, and not just your dealership or general manager, for UDAP.

In fact, in a public statement, the FTC warned consumers about fake recall notices from car dealerships and provided tips for checking the veracity of such notices. The FTC is expected to continue focusing on UDAP violations by auto dealers and lenders in the coming years.

Abusive Practices

Similar to Section 5 of the FTC Act, the Dodd-Frank Act prohibits unfair and deceptive acts or practices and gives the CFPB rulemaking and enforcement power to that end. However, it differs in that it also prohibits "abusive" acts or practices. Specifically, Section 1031 of the Dodd-Frank Act provides that abusive practices include practices that materially interfere with the consumer's ability to understand a term or condition of the product or service or take unreasonable advantage of a consumer's lack of understanding, inability to protect their interests, or their reasonable reliance on the credit provider (dealer) to act in the consumer's interests. Unlike unfairness but similar to deception under the FTC Act, abusiveness under the Dodd-Frank Act requires no showing of substantial injury to establish liability.

The CFPB can only bring its enforcement actions against independent and buy-here-pay-here auto dealers. While the CFPB does not have authority to enforce "abusive" trade practice violations against franchised auto dealers, the same conduct that the CFPB would consider to be "abusive" may support a private UDAP action under state law against franchised auto dealers. **Honesty and transparency in the sales and F&I processes are perhaps the best defense to a claim of an unfair, deceptive, or abusive practice.**

Recommended Practice:

Honesty and transparency in the sales and F&I processes is the best defense against UDAP claims.

Section 1042 of Dodd-Frank extends this UDAP enforcement authority to State Attorneys General and other regulators. Already, several State AGs have brought civil actions involving creditors other than auto dealers.

The CFPB published a manual in 2012 explaining its authority under the Dodd-Frank Act and describing its guidelines for determining whether a particular practice is unfair, deceptive, or abusive. The manual also provides examples of past actions that the CFPB or FTC have determined to be UDAP violations, including deceptive "$0 down" advertisements by auto leasing companies. In 2022, the CFPB updated the manual to broaden its authority to address discriminatory conduct in particular as an unfair practice, even if the practice did not violate the Equal Credit Opportunity Act. The CFPB removed those updates in 2023 following a ruling by a Texas federal district court that the CFPB could not broaden its authority in this manner. The CFPB has appealed this decision to the Fifth Circuit Court and awaits a ruling, expected to be issued in early 2025. *Chamber of Commerce v. CFPB*, No. 23-40650 (5th Cir.). If the district court's decision is reversed, the CFPB may reinstate its broad authority to target practices it believes to be discriminatory.

The FTC and CFPB signed a memorandum of understanding in December 2012 to share information and coordinate their supervisory and enforcement efforts against UDAP among their respective regulated entities. The FTC partnered with 32 law enforcement agencies in the U.S. and Canada to implement Operation Ruse Control, a crackdown on perceived deception and fraud in auto sales. Collectively, they brought over 185 actions against auto dealers. Both the FTC and the CFPB have signed similar memoranda of understanding with State Attorneys General.

State UDAP Laws

State UDAP laws are not uniform. A number of states apply different tests for "unfairness" or "deception" than the test used by the FTC. Many enumerate specific practices deemed to be unfair. Others use differing standards that include: (i) whether the practice, even if not previously considered unlawful, offends public policy under any state authority; (ii) whether it is unconscionable, unethical, immoral, oppressive, or unscrupulous; and (iii) whether it causes substantial injury to consumers. In particular, state standards for "unfairness" may include a lower threshold for liability than the FTC's unfairness standard.

Many state UDAP laws also cover online or out-of-state transactions if a resident of the state is adversely affected. You should be aware that State Attorneys General are very liberal in using UDAP laws to bring claims against auto dealers. Private lawsuits, especially class actions, present another risk under state UDAP laws. Examples of suits brought against dealers include:

- Misrepresentations about the vehicle's fuel efficiency, safety features, and warranty;
- Payment packing;
- Retaining amounts of itemized sums listed as "amounts paid to others" on retail installment sales contracts without disclosing that the dealer may retain part of the funds;
- Concealing negative equity in the cash price of a vehicle;
- Violating the FTC's Used Car Buyer's Rule which requires a Used Car Buyer's Guide to be affixed to the window of each used vehicle offered for sale or lease (remember that a federal law violation is automatically a UDAP violation under many state UDAP laws);
- Hiding the cost of an "etch" product in the vehicle's sale price; and
- Imposing extra charges when customers who leased cars attempted to exercise their right to purchase at a previously determined price.

UDAP plaintiffs may not be bound by contractual limitations of liability or merger clauses, or contributory negligence, and they often do not have to prove reliance on the act or practice. Also, arbitration clauses may not apply depending on state law and how the clauses are drafted. Courts have ruled as well that it is not a good defense that the seller acted in good faith under the advice of counsel. Unlike the FTC, most state courts adopt the least sophisticated consumer standard for assessing whether a practice could be unfair or deceptive and do not use a "reasonable consumer" standard.

State UDAP laws are written very broadly and courts have held that they are to be liberally construed in favor of the consumer.

Compliance Tip

Familiarize yourself with state UDAP laws with provisions broader than federal UDAP law that may apply to your dealership.

This puts conceivably any selling or financing practice at risk from an enterprising plaintiff's lawyer who finds a disgruntled consumer. As a "catch-all" for dealer misconduct, state UDAP laws offer consumers a powerful weapon in many states. State Attorneys Generals continue to bring UDAP claims against dealers for a variety of allegedly unfair and deceptive practices, often relating to the advertising and disclosures made by the dealer. One state even filed a complaint against a dealer's lender for facilitating perceived deceptive practices by the dealer in the selling of inoperable vehicles by providing financing for the vehicles.

Criminal Liability for Deceptive or Unfair Dealer Practices

Criminal violations have been brought against auto dealers in extreme situations when their conduct has met the requirements of criminal fraud and related criminal statutes under federal or state law. A federal statute makes it a felony to make a knowing and willful misrepresentation to a federally insured financial institution. Under this statute, indictments have been brought and dealers have paid criminal fines, or been imprisoned, for defrauding banks in order to obtain financing. The federal odometer tampering statute has been a basis for indictments against dealers, as well. Altering vehicle titles and documentation

to reflect the inaccurate mileage only compounds the crime, and the Department of Justice has indicted dealers for doing so.

Recommended Practices

1. **Adopt a dealership code of conduct emphasizing honesty and transparency with customers and train all your employees on it.**

Recommended Practice

> Adopt a dealership code of conduct emphasizing honesty and transparency with customers, and train all your employees on it.

While you can't specifically prohibit every possible practice your employees should not do, you can establish a set of principles and guidelines to govern employee conduct. Your employees have to know how you want your business to be conducted, and each employee should sign an affirmation that they understand and will comply with the code of conduct to reflect well on your dealership. Your code of conduct and training should contain specific standards of behavior that exemplify the principles embodied in the code of conduct. Enforce your code of conduct by reviewing deal files, listening to customers, and stressing the importance of proper behavior. Make employees understand shortcomings and why it is necessary to immediately correct them. Make compliance with the code of conduct a part of decision-making regarding compensation.

2. **Know your state's law on the amount of "doc fees" a dealer can collect. If the law permits such a fee, but does not prescribe a specific amount, be sure you can reasonably defend your "doc fees" in relation to your cost of preparing documents and titling work for vehicles you sell.**

Recommended Practice

> Be prepared to defend the legality of your "doc fees" and how reasonable they are in relation to what it costs for you to prepare documents and handle titling.

Many states permit "reasonable" doc fees but do not give any guidance on what constitutes "reasonable" for this purpose. And other states have limits on the amount and type of fees that can be charged and require disclosures in connection with their imposition.

3. **Make sure your advertising and other communications with customers are true and accurate and clearly state the terms of any offer you are making.**

Recommended Practice

> Make sure that all your advertisements and communications with customers are true and accurate and clearly outline the terms of any offers you present.

Many dealerships get into trouble when their advertising goes beyond simple puffery. Advertising drives customers through your doors, but you still need to stand behind promises and offers you make in that advertising. Likewise, you need to make sure you are transparent about the required terms of the offer to avoid claims that you deceived the public.

4. **Establish a consumer complaint resolution process and include timelines for a quick and efficient resolution.**

Recommended Practice

> Establish and keep track of a consumer complaint resolution process that includes timelines for quick and efficient resolution.

Keep track of your complaints and note any trends. For example, if a number of consumers complain that they did not know they were being charged for an aftermarket product, consider improving your communication strategies so that consumers only purchase the products they intend. Where disputes cannot be resolved through complaint resolution, try to establish an informal mediation process with your consumers either with a neutral officer at the dealership or through a local association, such as your regional auto dealer association, or a mediation company. Many problems can be resolved by an effective

mediator prior to litigation or arbitration if the dealer and customer are at an impasse. A consumer complaint process is an integral element of a Compliance Management System. Consult your local attorney on the possible use of arbitration clauses and class action waivers if mediation or informal efforts to resolve disputes are unavailing. Arbitration and class action waivers are discussed in Topic 9: Arbitration and Mediation.

5. **Have an attorney or compliance professional conduct periodic compliance audits and "mystery shopping" at your dealership to identify areas that might support UDAP violations.**

Recommended Practice

> Engage a legal expert to regularly perform compliance audits and conduct 'mystery shopping' at your dealership to uncover potential Unfair or Deceptive Acts or Practices (UDAPs).

Remember that in many states a violation of any federal consumer protection law or regulation (e.g., failing to publish a Spanish-language Used Car Guide on a used vehicle that was negotiated for sale in Spanish, failing to provide an adverse action notice when declining to provide financing, etc.) is an automatic violation of a state's UDAP laws. Promptly correct any deficiencies identified by using appropriate staff training to avoid repetition or other conduct that may lend itself to being an unfair or deceptive trade practice. Remember to adhere to your dealership's code of conduct and train your employees frequently.

Additional Resources

Federal Reserve, Consumer Compliance Handbook:
FTC Act Section 5 (December 2016)
http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf

FTC, CARS Rule (January 2024)
https://www.ftc.gov/business-guidance/resources/ftc-cars-rule-combating-auto-retail-scams-dealers-guide

FTC, Dealer's Guide to the Used Car Rule (January 2024)
http://www.business.ftc.gov/documents/bus13-dealers-guide-used-car-rule

FTC, Examination Procedures for UDAP Violations (June 2022)
https://www.fdic.gov/regulations/compliance/manual/7/VII-1.1.pdf

FTC, Guide Concerning Use of the Word "Free"
and Similar Representations (April 2012)
https://www.ftc.gov/legal-library/browse/rules/guide-concerning-use-word-free-similar-representations

CFPB, UDAAP Manual (September 2023)
https://files.consumerfinance.gov/f/documents/cfpb_unfair-deceptive-abusive-acts-practices-udaaps_procedures_2023-09.pdf

CFPB, Policy Statement on Abusive Acts or Practices (April 2023)
https://www.consumerfinance.gov/compliance/supervisory-guidance/policy-statement-on-abusiveness/

CFPB, Consumer Complaint Hotline
https://www.consumerfinance.gov/complaint/

CFPB, Symposium on Abusive Acts or Practices (July 2019)
https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-abusive-acts-or-practices/

16 C.F.R. § 251.1 (Using the Word "Free" in Advertising)
http://www.law.cornell.edu/cfr/text/16/251.1

Arbitration and Mediation

Arbitration and mediation are alternatives to litigation that can resolve individual disputes more efficiently but can also lead to mass arbitration filings by numerous individuals. Learn about legal developments that can help your arbitration and mediation provisions to remain enforceable and result in efficient dispute resolution.

Assess the terms of your arbitration and mediation provisions →

Did You Know?

Arbitrations brought by 25 or more consumers against the same company may be considered a "mass arbitration" subject to the American Arbitration Association's new mass arbitration rules. Read more

Compliance Tip

To protect the enforceability of your arbitration provisions, make sure the provisions are easy for the other party to access, read, and understand the contract. Read more

What's New for 2025

Some arbitration organizations enacted new comprehensive mass arbitration rules in 2024 that could quell the growing trend of mass arbitrations in 2025 and beyond. Be sure to review the new rules with your attorney to determine how to help protect your dealership from mass arbitrations. Read more

Recommended Practice

Ensure your arbitration provisions state that they adopt new mass arbitration rules and reserve your right to consolidate any mass arbitration action. See more Recommended Practices

Breakout Sections

Arbitration and Mediation

This Topic discusses recent arbitration-related rulemaking activities, federal arbitration laws, and the types of arbitration clauses that may be stricken by courts as unconscionable and unenforceable in the aftermath of the *Concepcion* decision by the U.S. Supreme Court.

Overview of Arbitration and Mediation

Arbitration and mediation offer alternative methods for auto dealers and consumers to resolve their disputes instead of resorting to litigation in courts.

Compliance Tip

Make sure you understand the difference between arbitration and mediation.

Both methods are typically favored by dealers as being more efficient, cost-effective, and private than traditional litigation. Arbitration is a private proceeding in which a dispute is decided by a private individual or panel of individuals under a set of agreed-upon rules instead of through a lawsuit. Arbitrators are given wide discretion under arbitration rules and do not tend to strictly follow legal precedent in making their decisions. Arbitrators issue binding judgments that may be later enforced in court, and grounds to challenge those judgments through appeal are very limited.

Mediation is a private proceeding in which an individual selected by the parties facilitates negotiations between the parties to guide them toward a mutual resolution. Mediation is often faster and more informal than arbitration. Rather than issue binding decisions, mediators help parties to agree on terms of their own binding settlement agreement, which may later be enforced in court. Generally, dealers may prefer to negotiate issues directly with consumers, then mediate the dispute if negotiations are unsuccessful, then consider arbitration if the dealer has an applicable arbitration agreement with the consumer. Each of these alternative dispute resolution methods may offer a more efficient and effective resolution than traditional litigation.

Indeed, there are three key rulings, actions, and changes that have reshaped the industry's approach to arbitration and mediation. They are:

- **Section 1028 of the 2010 Dodd-Frank Act**: The guidance from the Dodd-Frank Act directed the Consumer Financial Protection Bureau (CFPB) to conduct a study on consumer arbitration and report to the U.S. Congress concerning the use of mandatory pre-dispute arbitration in contracts for consumer financial products, including retail installment credit agreements.
- ***AT&T Mobility v. Concepcion*, 563 U.S. 333 (2011)**: This ruling by the U.S. Supreme Court preempted state laws prohibiting contracts from disallowing class action remedies.
- **American Arbitration Association (AAA)**: **AAA now requires you to annually register your arbitration language for approval by the AAA for compliance with its "Consumer Due Process Protocol" and pay a fee. Each dealer must make its own filing and pay its own fees.**

Did You Know?

The American Arbitration Association (AAA) now requires you to annually register your arbitration language for approval and pay a fee.

Section 1028 of the Dodd-Frank Act

In enacting the Consumer Financial Protection Act of 2010, aka, Dodd-Frank Act, Congress directed the CFPB to conduct a study on the use of mandatory pre-dispute arbitration clauses ("Arbitration Clauses") in contracts for consumer financial products and services and report back with its findings. Accordingly, the CFPB issued its arbitration study in March of 2015. The study focused on Arbitration Clauses containing provisions through which consumers waive their right to make class action claims, either in court or by arbitration. The study concluded that Arbitration Agreements with these class action waivers restrict consumers' ability to obtain relief for disputes. The report found that, in the consumer finance markets studied, very few consumers individually seek relief through arbitration or the federal courts, while millions of consumers could be eligible for relief each year

through class action claims. It also found that such Arbitration Clauses did not result in the reduction of pricing to consumers. The study concluded that class actions provide consumers with a better chance for relief than arbitration, although their statistics arguably did not support that conclusion.

After an October 2015 hearing, the CFPB indicated it was inclined to issue a rule that would prohibit Arbitration Clauses containing class action waivers and did so on July 10, 2017. In addition to banning class waivers, the final rule required companies to report data concerning individual or class arbitrations to the CFPB, including the nature of the claims and their resolution. Under the final rule as published, the CFPB would both analyze and publish the reported claims and resolutions on its website. Once the final rule went into effect, it would operate to override court decisions that have upheld the use of Arbitration Clauses with class action waivers in contracts for consumer financial products and services.

Shortly after the final rule was published, the U.S. House of Representatives voted to exercise its authority under the 1996 Congressional Review Act (CRA) to reject agency rulemaking by passing a joint resolution disapproving the final rule. In a 51-50 late-evening vote on October 24, 2017, in which Former Vice President Pence cast the deciding vote, the Senate also passed the joint resolution and sent it to the White House for the President's signature.

The CRA's original purpose was to allow Congress the opportunity to undo so-called "midnight regulations" promulgated under an outgoing administration. Prior to 2017, it had been successfully used only once to overturn a Department of Labor Rule relating to ergonomics in 2001. The joint resolution was signed by President Trump on November 1, 2017, to overturn the arbitration rule. That was the 15th time the CRA had been successfully used in 2017 alone and the first time in history it was used to strike a final rule published during a current administration.

The import of Congress using its CRA authority to overturn a rule is that the promulgating agency is prohibited from reissuing the rule in substantially the same form or issuing a new rule that is substantially the same, "unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." **This means the CFPB may not reissue its arbitration rule, issue another rule banning class waivers in Arbitration Clauses, or issue another rule requiring reporting on arbitration actions and results, unless specifically authorized by Congress at some future date.**

Did You Know?

The CFPB is barred from issuing any rule banning class action waivers in arbitration clauses.

Following the House's exercise of its authority under the CRA, the U.S. Supreme Court decided to shed some light on class action arbitration. In *Lamps Plus, Inc. v. Varela*, 139 S. Ct. 1407 (2019), the Court found that an arbitration agreement's silence as to class actions does not, without more, permit a party to pursue class action arbitration.

AT&T Mobility v. Concepcion, 563 U.S. 333 (2011)

In the 2011 case *AT&T Mobility, LLC v. Concepcion*, the U.S. Supreme Court ruled in a 5-4 decision that arbitration agreements in standard form consumer financial services contracts that waive the right to pursue a class action are enforceable, and that the Federal Arbitration Act (FAA) preempted a California court ruling to the contrary. The case involved a large number of consumers, each of whom had been overcharged by a small amount of money (approximately $30) that made it otherwise unattractive for any consumer to bring an individual action. Each consumer's contract provided for mandatory arbitration and a waiver of any right to bring or participate in a class action. Based on these circumstances, the Federal Ninth Circuit Court of Appeals in California had ruled that the class action waiver was unconscionable, and was therefore unenforceable, under California consumer protection statutes that rely on private causes of action for enforcement.

The FAA provides that arbitration agreements are "valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." Even so, the Supreme Court reversed the Ninth Circuit's decision, noting that California's law stood as obstacles to the intent of Congress, as expressed in the FAA, of favoring arbitration where the parties have agreed to it as part of a contract. The Court also held that class action waivers are not inconsistent with the intent of Congress or the FAA, noting that "[a]rbitration is a matter of contract, and the FAA requires courts to honor parties' expectations." The Supreme Court further ruled that "[s]tates cannot require a procedure that is inconsistent with the FAA, even if it is desirable for unrelated reasons."

After the *Concepcion* decision, in an employment case, the Supreme Court affirmed that class action waivers in arbitration clauses are valid and enforceable. *Epic Systems Corp. v. Lewis* 138 S. Ct. 1612 (2018) (finding that arbitration agreements in employment contracts requiring individualized proceedings are enforceable). The key to enforcement of such waivers, however, is their inclusion in an arbitration clause. This is because the FAA governs arbitration clauses and preempts any state law that is inconsistent with those clauses. As a result, a class action waiver that is not contained within an arbitration clause may not be enforced unless it is permitted under state law.

For example, a federal court in Rhode Island struck down an auto dealer's stand-alone class action waiver in an auto leasing agreement in October 2023. The case arose after a customer claimed that the residual value of her car at the end of her lease term was $2,000 more than she had agreed to pay. The lease included a clause waiving any class action relating to her lease. The customer still brought a class action against the dealer, and the court found that the waiver was not contained within an arbitration clause, so the FAA could not apply to protect the clause against Rhode Island public policy opposing the clause. The court then struck down the stand-alone waiver under Rhode Island law and allowed the class action to proceed.

This case from Rhode Island highlights the importance of having counsel review your arbitration agreements and class action waivers.

Other Challenges to Arbitration Clauses Post-*Concepcion*

Unconscionability. In the aftermath of the *Concepcion* decision, plaintiff's lawyers continued to attempt to invalidate arbitration clauses for unconscionability under state law with limited success. For example, in 2012, both the Third and Eleventh Circuit Courts of Appeals affirmed district court orders under *Concepcion* granting defendant creditors' motions to compel arbitration on an individual (rather than on a class-wide) basis over plaintiffs' objections that Arbitration Clauses containing class waivers in credit card and wireless telephone service agreements were unconscionable and unenforceable. On the other hand, some courts from Massachusetts to California have struggled to invalidate Arbitration Clauses on unconscionability grounds. One state court addressed the issue of whether the arbitration agreement as a whole was unenforceable as unconscionable under applicable state contract law. The majority concluded that it was indeed unenforceable because it was:

- Non-negotiable and difficult for consumers to understand;
- The record showed it would be unlikely for the plaintiff to be able to retain counsel to proceed individually in arbitration;
- There was considerable disparity in bargaining power; and
- **The substantive terms were much less fair to consumers than those of the agreement upheld in *Concepcion*.**

Compliance Tip

A class action waiver in an arbitration clause has a better chance of being enforceable if its terms are fair to the consumer and are easy for the consumer to understand.

Scope. Following *Concepcion*, plaintiff's lawyers continue to challenge the scope of arbitration clauses. If the arbitration clause does not encompass certain issues or individuals, then arbitration may not be compelled. *White v. Sunoco*, 870 F.3d 257 (3d Cir. 2017) (declining to compel arbitration when the defendant was not a signatory to an arbitration agreement).

Lack of Mutual Assent. A challenge to an arbitration provision may also arise based on a lack of assent to the provision. In order for an individual to be bound by an arbitration provision, that individual must know, understand, and assent to the terms of the arbitration agreement. If an individual does not assent to the arbitration agreement, then the arbitration agreement will not be enforceable. Courts have applied this principle in a manner that is very consumer friendly. For example, one court invalidated an arbitration provision contained in terms and conditions that could be accessed through a hyperlink. **The court ruled that the hyperlink was not conspicuous because it was presented in a grey rectangular box with white text, not the commonly used blue color with underlining. *Cullinane v. Uber Techs., Inc., 893 F.3d 53 (1st Cir. 2018).***

Compliance Tip

If your arbitration provision is provided to a customer through a hyperlink, make sure the hyperlink is easy for the customer to see and access.

In another case, a court found a lack of mutual assent when an individual was blind and could not physically read the arbitration clause. There was no evidence that the terms of the arbitration clause were read to the individual. *Nat'l Fed'n of the Blind v. The Container Store, Inc*., 904 F.3d 70 (1st Cir. 2018). In sum, it is important that an individual be aware of, and have easy access to, the arbitration agreement.

Waiver. Even if a court finds that an arbitration agreement is valid and binding, a party to that agreement may waive its right to compel arbitration by proceeding with litigation in court. Filing a responsive pleading, engaging in discovery, and allowing a court to rule on significant issues in the case will lead some courts to find the right to arbitration has been waived. *Martin v. Yasuda*, 829 F.3d 1118 (9th Cir. 2016) (ruling that a defendant waived arbitration by proceeding with litigation for 17 months); *Forby v. One Techs., L.P.*, 909 F.3d 780 (5th Cir. 2018) (finding the defendant waived arbitration by invoking arbitration after the court ruled on several key issues). **In 2022, the U.S. Supreme Court held that a party does not need to show that it would be prejudiced by shifting from litigation to arbitration when claiming that the other party waived its right to arbitrate by acting in a manner inconsistent with the arbitration agreement. *Morgan v. Sundance, Inc., 142 S. Ct. 1708 (2022).***

Compliance Tip

Enforce your arbitration agreement early on in litigation to avoid waiving your right to arbitration.

Appellate Review. A consumer may ask an appellate court to review an arbitration award. Such request may be denied if the arbitration agreement includes an "appellate waiver." For example, courts in the Fourth and Tenth Circuits must enforce appellate waivers in arbitration agreements. *Beckley Oncology Assocs., Inc. v. Abumasmah*, 993 F.3d 261, 264 (4th Cir. 2021) (enforcing provision whereby parties agreed that arbitrator's decision "shall be final and conclusive and enforceable in any court of competent jurisdiction without any right of judicial review or appeal"); *MACTEC, Inc. v. Gorelick*, 427 F.3d 821, 830 (10th Cir. 2005) (arbitration provision providing that "[j]udgment upon the award rendered by the arbitrator shall be final and nonappealable" clearly established parties' intent to preclude appellate court from reviewing lower court's judgment upon award).

Questions of Arbitrability

When a challenge to an arbitration agreement arises, the question of who gets to resolve the challenge often arises as well. The Supreme Court determined in *Henry Schein, Inc. v. Archer & White Sales, Inc*., 139 S. Ct. 524 (2019), that questions of arbitrability may be resolved by an arbitrator instead of a judge. However, in cases where parties have multiple agreements that conflict on the issue of who decides arbitrability, the issue of which agreement governs must be resolved by a judge. *Coinbase, Inc. v. Suski*, 144

S. Ct. 1186 (2024). Therefore, it is **best practice to state in your arbitration provision whether a judge or arbitrator decides questions of arbitrability and to ensure your selection is consistent across your agreements.**

Recommended Practice

State within the arbitration provision of a contract whether a judge or arbitrator decides questions of arbitrability and make sure your selection is consistent across other agreements.

In 2022, the Supreme Court determined that federal courts lack subject-matter jurisdiction to confirm or vacate an arbitration award when the only basis for jurisdiction is that the underlying dispute involved a federal question. *Badgerow v. Walters*, 142 S. Ct. 1310 (2022). The petition to confirm or vacate an award must itself support federal jurisdiction for a federal court to consider it. This ruling might make arbitration less effective because it means that, in some circumstances, state courts have the option of disregarding arbitration awards.

Mass Arbitration Trend

Plaintiff's lawyers are now using "mass arbitration" to turn arbitration agreements against companies. Mass arbitration occurs when a law firm files hundreds or thousands of individual arbitrations against the same defendant company at once, thereby requiring the defendant company to pay significant fees (*e.g.*, initial filing fee, case management fee, hearing costs, etc.), with many due even before the arbitration proceeds. The fees associated with mass arbitration can pressure companies into settling claims instead of proceeding with arbitration or testing the claims' merits in court.

The American Arbitration Association (AAA) and Judicial Arbitration and Mediation Services (JAMS) were initially reluctant to institute "mass arbitration" protocols. In an attempt to deter mass arbitrations, AAA amended its fee structure for "Multiple Consumer Case Filings" in late 2020 and created a rule in 2022 expressly allowing consolidation of existing arbitrations. That rule, Rule R-8, requires the party seeking consolidation to make a written request and allows other parties to respond in writing before an arbitrator decides whether to consolidate and thereby reduce the number of fees companies must pay. The rule only applied to business-to-business disputes, however, leaving it up to arbitrators' discretion whether to allow consolidation in consumer arbitrations. Despite the AAA's efforts through its fee structure amendment and consolidation rule, mass arbitrations continue to rise. **In response, AAA and JAMS enacted comprehensive mass arbitration rules in 2024.**

Watch List for 2025

AAA and JAMS have enacted new mass arbitration rules that may make it more difficult for mass arbitrations to be brought against companies in 2025 and beyond.

AAA issued its Mass Arbitration Supplementary Rules in January 2024, and JAMS issued its Mass Arbitration Procedures and Guidelines in May 2024. **AAA's rules apply to mass arbitrations brought by 25 or more consumer claimants against the same defendant or 100 or more non-consumer claimants against the same defendant.**

Did You Know?

Arbitrations brought by 25 or more consumers against the same company may be considered a "mass arbitration" under the AAA's new mass arbitration rules.

AAA also requires pre-arbitration mediation and provides for a merits arbitrator to review the findings of a process arbitrator under an "abuse of discretion" standard. JAMS's rules do not include these provisions. JAMS's rules apply to mass arbitrations brought by 75 or more claimants, whether consumer or non-consumer, against the same defendant. Both the AAA and JAMS rules require the parties to agree to use the rules in the event of arbitration, but the AAA rules still give the arbitrator discretion not to apply the rules under the circumstances of the case.

Auto dealers should consult with their counsel to ensure their arbitration agreements curb the likelihood of mass arbitration through provisions consenting to application of AAA and/or JAMS mass arbitration rules and reserving the right to seek consolidation of mass arbitration actions, among other contractual safeguards.

Recommended Practice

Ensure your arbitration agreements adopt new mass arbitration rules and reserve your right to consolidate mass arbitration actions.

Anti-Arbitration Agreement Legislation

In 2021, the bipartisan Forced Arbitration Injustice Repeal (FAIR) Act, H.R. 963, was introduced to prohibit pre-dispute arbitration agreements for consumer, employment, antitrust, and civil rights disputes. The House of Representatives passed the FAIR Act on March 17, 2022, but the Act was not taken up for a vote in the Senate. The Act was then reintroduced in the Senate in 2023 and referred to the Senate Judiciary Committee, but the Committee never took up the Act for consideration. The Act may be introduced again in a future session of Congress and could significantly alter the landscape of mandatory arbitration. Auto dealers should continue to monitor for the introduction of similar federal legislation in the coming years.

Class Action Fairness Act

The federal Class Action Fairness Act of 2005 makes it easier to file a class action if there are at least 100 class members and the total amount sued for exceeds $5 million. Jury members may have unfavorable opinions of auto dealers and may be sympathetic to the plaintiff class of consumers if the case makes it to trial before a jury. After the *Concepcion* case upholding class action waivers in arbitration clauses, however, such jury trial cases are more difficult to bring against auto dealers who incorporate arbitration clauses into their contracts.

If arbitration clauses are properly drafted by allowing the consumer reasonable access to a fair and inexpensive dispute resolution process and forum, like the consumer-friendly clause in *Concepcion* did, at least for now, most courts will enforce arbitration clauses despite the liberality of the Class Action Fairness Act.

Important Laws and Regulations

The Federal Arbitration Act

The Federal Arbitration Act (FAA), originally passed in 1925, states a broad national policy in favor of enforcing agreements to arbitrate and applies whenever a transaction involves "interstate commerce." Every transaction that somehow involves more than one state is likely to meet this low "interstate commerce" standard. It may cover most automobile sales and financing transactions if any item purchased or the customer comes from out of state (such as the financing source or provider of an aftermarket product). Generally, the FAA preempts inconsistent state laws, such as a state law that prohibits arbitration of consumer claims. The U.S. Supreme Court has also held as a general proposition that the FAA does not allow class arbitrations absent an agreement between the parties in their arbitration clauses. The validity and preemptive effect of the FAA was affirmed in the Supreme Court's *Concepcion* decision.

While more difficult after *Concepcion*, courts still have the power to refuse to enforce arbitration provisions that are ruled "unconscionable" or void under state law. The so-called "Savings Clause" of the FAA (which provides that arbitration provisions are "valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract") still permits a challenge to arbitration provisions on grounds of fraud, duress, or unconscionability. Some courts describe unconscionability as "the absence of meaningful choice on the part of one of the parties, together with contract terms that are unreasonably favorable to the other party." A California court held that while *Concepcion* and the FAA require that class action waivers be enforced, they do not preempt generally applicable state contract law defenses, such as fraud, duress, or unconscionability, from applying to other arbitration provisions.

To defeat a claim of unconscionability, **arbitration provisions must be carefully drafted. Consult your attorney for assistance. Some points to consider when drafting:**

Recommended Practice

> To help your arbitration clause be upheld in court, consider giving both parties the right to invoke arbitration, making the arbitration clause text larger and easier to read, and placing the arbitration clause near the parties' signatures, among other practices.

- Treat both parties equally, giving either party the right to invoke arbitration;
- Don't use small boilerplate type in non-negotiable contracts;
- Don't draft a provision that contains hardships from a consumer's perspective;
- Arbitration provisions should be conspicuous in a contract (such as through larger type and bolder printing than the rest of the document);
- Consider whether you want to prohibit class action arbitrations;
- Arbitration provisions may be best placed near the consumer's signature or at least require separate initialing by the consumer;
- Consult state law, which may require that arbitration provisions contain specific language; and
- If exceptions for small claims actions or repossessions are stated, make them clear and conspicuous.

Notwithstanding the *Concepcion* decision, courts' interpretations of arbitration provisions are constantly evolving, and dealers should regularly consult an attorney for updates, especially about court decisions in the states in which the dealer operates.

American Arbitration Association's Mandatory Filing Policy

The American Arbitration Association (AAA) requires you to annually register your arbitration provisions for approval by the AAA for compliance with its "Consumer Due Process Protocol" and pay a fee. A forms provider may not file an approval for all users of the form. Each dealer must make its own filing and pay its own fees. If you don't register in advance, you may register at the time you are seeking to arbitrate a matter, but you will be required to pay an additional fee.

The AAA will evaluate your arbitration provision to see if it complies with the Consumer Due Process Protocol. If it complies, the clause will be posted on the AAA's Consumer Clause Registry for public access, along with your dealership's name, address, and other related documents and information. You can register your arbitration provisions at consumerreview@adr.org or online at https://apps.adr.org/ClauseRegistryUI/faces/org/adr/extapps/clauseregistry/view/pages/clauseRegistry.jsf.

If the AAA determines that your arbitration provisions do not comply, an amended version can be resubmitted. Dealers should note, however, that the AAA's approval of arbitration language does not guarantee that a court will agree to enforce it.

Recommended Practices

1. **Use an attorney to help navigate state arbitration laws and provide language to make certain that your state's contract laws will not negate the arbitration provisions you are using.**

Recommended Practice

> Consult your attorney on state arbitration laws and ensure your contracts use the correct language in arbitration provisions.

Have a periodic "check-up" with your attorney to make sure that new cases have not changed the likelihood that your arbitration language is enforceable.

2. **Give the customer time to read and understand the entire RISC or Leasing Agreement, but especially the arbitration and class action waiver provisions, the customer may claim they did not understand or agree to the provisions.**

Recommended Practice

> Allow the customer time to read and understand the entire RISC or Leasing Agreement.

Such provisions in a Buyer's Order, RISC, lease agreement, or a stand-alone arbitration agreement should be easy to understand, as well as clear and conspicuous, preferably in bold type and in a larger type size than other provisions. If the deal was negotiated in Spanish or another foreign language, make sure to explain the arbitration provisions to the consumer in that language when explaining the contract terms of the deal. It is a best practice to give the consumer a translation of the arbitration provisions as well (if you are not already required to provide a translation of documentation under applicable law).

3. **Get the consumer's signature or initials on any arbitration provisions. Placing the arbitration provisions just above the signature line in a contract could meet this consideration.**

Recommended Practice

> Make sure to have the customer sign or initial any arbitration provisions.

If a space for initials is provided, double-check the contract to make sure that the customer has also initialed that space to prevent any issues with its enforcement, even if the customer otherwise provided a signature at the end of the contract.

4. **Avoid one-sided terms that favor the dealership.**

Recommended Practice

> Avoid one-sided arbitration terms that favor the dealership and use provisions that maintain a sense of fairness and balance.

Cases invalidating arbitration provisions as unconscionable almost invariably gave the dealer greater rights than the consumer. Use provisions that maintain a sense of fairness in the arbitration process.

5. **Regularly revise your employment arbitration agreements for compliance with law.**

Recommended Practice

> Regularly revise your employment arbitration agreements to keep them in compliance and up to date with current law.

An arbitration agreement signed as a condition of employment could be deemed unenforceable depending on the state and surrounding circumstances. Therefore, to avoid doubt, seek counsel and consider implementing one arbitration agreement and removing any arbitration language from other documents.

6. **Amend arbitration agreements to counter mass arbitration.**

Recommended Practice

> Amend arbitration agreements to counter mass arbitration.

Work with an attorney to make your arbitration agreements less susceptible to exploitation by plaintiff's attorneys. Provisions adopting AAA and/or JAMS mass arbitration rules, requiring detailed individual requests for arbitration, mandating individual pre-arbitration conferences, or consolidating mass arbitration claims into smaller "batches" for more efficient resolution are just some methods of minimizing the likelihood and potential impact of mass litigation. Experienced counsel can help you decide what amendments would best suit your needs.

Additional Resources

AT&T Mobility LLC v. Concepcion, 563 U.S. 333 (2011)
https://supreme.justia.com/cases/federal/us/563/333/

American Arbitration Association
http://www.adr.org/

American Arbitration Association, Consumer Clause Registry
https://apps.adr.org/ClauseRegistryUI/faces/org/adr/extapps/clauseregistry/view/pages/clauseRegistry.jsf

American Arbitration Association, AAA Mass Arbitration
https://www.adr.org/mass-arbitration

American Arbitration Association, AAA Mass Arbitration Supplementary Rules (April 2024)
https://www.adr.org/sites/default/files/Mass-Arbitration-Supplementary-Rules.pdf

American Arbitration Association, AAA Commercial Arbitration Rules and Mediation Procedures Significant Amendments (September 2022)
https://www.adr.org/sites/default/files/document_repository/AAA409_CommRules_Significant_Amendments_Sept2022.pdf

CFPB, Learn How the Complaint Process Works
https://www.consumerfinance.gov/complaint/process/

Judicial Arbitration and Mediation Services
https://www.jamsadr.com/

Judicial Arbitration and Mediation Services, JAMS Mass Arbitration Procedures and Guidelines (May 2024)
https://www.jamsadr.com/mass-arbitration-procedures

Telemarketing Requirements

Telemarketing can help your dealership to thrive but can also expose your dealership to significant penalties if not done according to certain consent, timing, and other requirements. Both federal and state law impose requirements on dealer telemarketing activities.

Learn how to legally text, call, email, or fax marketing messages →

Did You Know?

The FTC recently extended the Telemarketing Sales Rule (TSR) to also apply to business-to-business telemarketing, rather than only to business-to-consumer telemarketing. Make sure your marketing messages to other businesses comply with TSR requirements. See more

Compliance Tip

Review your marketing lead buying practices to comply with the FCC's new One-to-One Rule set to take effect in January 2025. The new Rule prohibits multiple marketers from relying on a single consumer consent, and it requires marketing messages to be associated with the reason that the consumer gave its consent. See more Compliance Tips

Watch List for 2025

Starting on April 11, 2025, the FCC will require businesses to act within 10 business days to honor a customer's request to withdraw consent to marketing messages or to be added to a business's internal do-not-call list. See more

Recommended Practice

Scrub your internal marketing target lists against applicable federal and state do-not-call lists at least every 14 days to remove consumers who have opted out of communications from you or your affiliates. See more Recommended Practices

Breakout Sections

Telemarketing Sales Rule and Telephone Consumer Protection Act

At the federal level, telemarketing is regulated by two sources: (i) the Telephone Consumer Protection Act (TCPA), which is enforced by the Federal Communications Commission (FCC); and (ii) the Telemarketing Sales Rule (TSR), which is enforced by the Federal Trade Commission (FTC) and in some instances the Consumer Financial Protection Bureau (CFPB), which treats violations of the TSR as an unfair, deceptive, or abusive act or practice.

While both the TCPA and the TSR continue to generate increasing numbers of lawsuits and litigation each year, the TCPA has been used in many notable class actions garnering multimillion-dollar settlements (for example, AT&T Mobility, Caribbean Cruise Line, Capital One, US Coachways, and Dish Network all paid over $300 million in settlements between 2014 and 2017). However, as a result of the U.S. Supreme Court ruling in *Facebook v. Duguid* in April 2021, the scope of the TCPA has been significantly limited, and the likelihood of seeing significant class action settlements in 2025 is low. Nonetheless, these regulatory regimes can be complicated because the two standards are similar in some cases, while in other cases the two standards cover the same subject with different requirements and prohibitions, and in still other cases, one standard may address an issue on which the other is silent. **This structure requires careful planning and consultation with legal and marketing teams to implement a telemarketing campaign that complies with all applicable standards, particularly TCPA and TSR.**

Compliance Tip

Plan and consult with legal and marketing teams prior to implementing any telemarketing campaign so it complies with all applicable standards.

Telemarketing Sales Rule

The Telemarketing and Consumer Fraud and Abuse Prevention Act (Telemarketing Act) directed the FTC to issue a rule prohibiting deceptive and abusive telemarketing conduct. In response, the FTC established the Telemarketing Sales Rule (TSR). The TSR regulates "telemarketing," which is defined as "a plan, program, or campaign . . . conducted to induce purchases of goods or services. . . by use of one or more telephones and involves more than one interstate telephone call." It applies to all businesses or individuals that engage in "telemarketing," including "telemarketers" when they initiate calls to, or receive calls from, consumers or businesses, and "sellers" when they provide, offer to provide, or arrange to provide goods or services to consumers or businesses in exchange for payment. Even if an entity or individual does not meet the definition of a "seller" or "telemarketer" in this context, the TSR may still apply if they provide substantial support to sellers or telemarketers. Calls made from outside of the United States must also comply with the TSR. Note that the TSR previously exempted calls to businesses from its requirements but has since been amended to reverse that exemption.

The FTC maintains the national "Do Not Call" registry prohibiting telemarketing calls to the listed numbers, which include both land lines and cell numbers, subject to exceptions for calls based on a business relationship or express permission. (The FCC also enforces compliance with the national list.) **Because several states maintain their own "do-not-call" lists independent of the national list, dealers must scrub telemarketing lists against both the FTC's National Do Not Call Registry and applicable state do-not-call lists.**

Recommended Practice:

Scrub telemarketing lists against both the FTC's National Do Not Call Registry and applicable state do-not-call lists.

Additionally, dealers are required to keep their own internal company-specific list of customers who opt out of telephone communications, and they are required to delete these customers' contact information from marketing lists. If you share customer information with affiliates or third parties, make sure to scrub from the shared lists any customers who have opted out of being contacted in any medium of expression. The TSR expressly prohibits callers from interfering with consumers' efforts to exercise their company-specific do-not-call rights and lists specific proscribed activities, including hanging up on the consumer and requiring the consumer to listen

to a sales pitch before processing the do-not-call request. The penalty for calling a consumer who asked not to be called potentially exposes a seller and telemarketer to a civil penalty of **$50,120 for each violation**.

Did You Know?

You could risk a penalty of $50,120 for calling a customer who asked not to be called, so be sure to maintain your dealership's do-not-call list.

Beyond do-not-call provisions, the TSR, among other things, requires a certain "prompt" disclosure of material information at the outset of each sales call or sales pitch and certain other disclosures of important information before the consumer agrees to purchase any goods or services in a telemarketing transaction. The prompt disclosures include the seller's identity and the call's sales purpose. These disclosures must be "clear and conspicuous" in a way that a consumer will notice and understand.

The TSR specifies several categories of material information that must be provided to consumers:

1. Cost and Quantity. The total cost to buy, receive, or use the offered goods or services. If disclosing the installment payments and the amount of each payment satisfies the requirement, then the amount and number of the payments must correlate to a billing schedule. Note also that if the offer is for a consumer credit product, the TSR provides that TILA and Regulation Z disclosure requirements may apply;
2. Material Restrictions, Limitations or Conditions. Material information is information that would likely affect the consumer's choice of goods, services, or charitable contribution;
3. No Refund Policy. If applicable, a no-refund policy and/or "all sales are final" policy must be disclosed clearly and conspicuously, as well as all terms and conditions likely to affect a consumer's decision whether to buy the goods or services offered;
4. Prize Promotions. Includes any sweepstakes or games of chance and a representation that the consumer has won, has been selected to receive, or may be eligible to receive a prize or purported prize; and
5. Full details of any "negative option plan," which is an offer or agreement to sell or provide any goods or services on an ongoing basis where, following a consumer's initial enrollment in a program, the seller interprets the consumer's silence or failure to affirmatively reject or cancel the agreement as acceptance of receiving future goods or services.

Other disclosures concerning sales of credit card loss protection and debt relief services are also required to be disclosed although they likely do not apply to a dealer's model. Any misrepresentations regarding this information are prohibited.

The TSR requires sellers to obtain a consumer's "express verifiable authorization" confirming a telemarketing transaction, which means giving the consumer several prescribed items of information to complete and confirm the transaction. It is required where a payment is made by a method other than a credit card.

The TSR separately requires sellers to obtain the consumer's "express informed consent" to a telemarketing transaction. The specific requirements of this "informed consent" standard differ depending on the details of the relationship between the seller and the consumer and the nature of the offer. However, consent would not meet the requirement if the consumer does not receive the required material disclosures. **The TSR's list of prohibited abusive practices includes repeated calling with an intent to harass or annoy, calling before 8:00 a.m. or after 9:00 p.m., and restrictions on abandoned calls and prerecorded message telemarketing.**

Did You Know?

The TSR's list of prohibited abusive practices includes calling before 8:00 a.m. or after 9:00 p.m.

The TSR generally prohibits a high percentage of abandoned calls but establishes a limited safe harbor if the telemarketer:

- Uses technology that ensures abandonment of no more than three percent of all calls answered by a live person, measured over the duration of a single calling campaign, if less than 30 days, or separately over each successive 30-day period or portion thereof that the campaign continues;
- Allows the telephone to ring for 15 seconds or four rings before disconnecting an unanswered call;
- Plays a recorded message stating the name and telephone number of the seller on whose behalf the call was placed whenever a live sales representative is unavailable within two seconds of a live person answering the call; and
- Maintains records documenting adherence to the three requirements above.

A telemarketing call is abandoned if a live consumer answers the call and no live sales agent is available to speak to the consumer within two seconds. Predictive dialers can produce abandoned calls when the dialer calls more consumers than there are available sales agents. To take advantage of the safe harbor, callers may use a predictive dialer provided that it does not abandon more than three percent of all calls answered by a live consumer. For the permitted three percent of calls that can be abandoned, the caller must provide a recorded message identifying the caller by name and telephone number. As explained below, the FCC's TCPA rule also regulates abandoned calls but establishes a stricter set of requirements for its safe harbor.

The TSR requires the called consumer's express written agreement to deliver prerecorded telemarketing messages.

Compliance Tip

The TSR requires the called consumer's express written agreement to deliver prerecorded telemarketing messages.

This agreement must be in writing, must be signed by the consumer, must include the consumer's telephone number, must identify the seller receiving the consent, and must explain what the consumer is agreeing to. The seller must also meet the following three requirements:

- Before the consumer agrees, the seller must clearly and conspicuously disclose the consequences of agreeing — namely, that the agreement will result in the seller delivering prerecorded messages to the consumer via telemarketing calls;
- Sellers are prohibited from requiring a consumer to provide this agreement as a condition of any purchase. In other words, consumers must be able to do business with the seller without providing this agreement to receive prerecorded telemarketing messages; and
- Sellers must give the consumer an opportunity to designate the telephone number to which the calls may be placed.

As to the call abandonment provision, the FCC's TCPA rule also regulates in this area with standards that are stricter than the TSR's. The FCC's approach is set out below.

Even when the seller has the consumer's consent, all prerecorded telemarketing calls must include an automated interactive opt-out mechanism that allows the consumer to make a company-specific do-not-call request. This mechanism must be presented to the consumer within two seconds at the start of the call and must begin with the "prompt" disclosures required by the TSR. This opt-out mechanism must be available throughout the call and must disconnect from the consumer's line immediately after the consumer uses the mechanism to opt out. For prerecorded telemarketing calls delivered to a consumer's voicemail, where the opt-out mechanism would not be operational, the message must provide a toll-free number that connects to an automated opt-out mechanism.

Note that the TSR offers a partial exemption for telemarketing calls that require a face-to-face sales presentation before the transaction is completed. Some but not all TSR provisions apply to these calls.

In March 2024, the FTC amended the TSR to extend the rule's protections to businesses and to update the rule's recordkeeping requirements. Specifically, the TSR imposes new requirements for call detail records and related safe harbors, consent records, and DNC compliance records. The TSR further prohibits misrepresentations and misleading or false statements in telemarketing calls to businesses, rather than only for calls to consumers, but the rule does not yet require telemarketers to comply with other TSR recordkeeping, disclosure, or other requirements for their calls to businesses. Also in March 2024, the FTC proposed an additional amendment to the TSR to extend to calls made by consumers to telemarketers to obtain technical support services, which is a growing scam that primarily harms older adults. **The proposed rule may be finalized in 2025.**

Did You Know?

The TSR has been extended to apply to business-to-business, rather than only to business-to-consumer, telemarketing.

Telephone Consumer Protection Act

As noted above, the FCC also regulates telemarketing and servicing calls and text messages using auto-dialers and pre-recorded messages to cell phones under the TCPA.

Historically, a key issue under the TCPA was what constituted an "auto dialer." Generally, "auto dialers" are any devices that "have the capacity" to store numbers to be called and to dial such numbers. Even if the machine is being used to make calls manually, if the device "had the capability" of auto dialing, it was considered an auto dialer, and the call was treated as if it was made by an auto dialer. When asked for an example of a device that is not an auto dialer, the FCC responded that a rotary dial phone is not an auto dialer. Over time, the FCC has consistently expanded its interpretation of what constitutes a regulated auto dialer. Indeed, in 2015, the FCC adopted the position that the TCPA's auto dialer standard can even apply to equipment based on its "potential functionalities" for dialing numbers. This interpretation exposed companies to a constant increase of class action lawsuits, many resulting in multi-million-dollar settlements.

However, in 2021, the U.S. Supreme Court issued a highly anticipated decision in *Facebook v. Duguid*, 141 S. Ct. 1163, resolving the long-standing dispute as to the scope of an "auto dialer." The Supreme Court concluded that a device that merely has the capacity to store numbers and dial them is not enough for the device to qualify as an "auto dialer" under the TCPA. The impact of this narrow interpretation is that lawsuits under the TCPA must now prove that the call or text at issue resulted from the use of a "random or sequential number generator" (i.e., auto dialer) rather than a preexisting list of numbers. This is a favorable decision for businesses that call or text individuals, so long as the business does not use an auto dialer to do so.

The FCC also monitors telemarketing calls made to a cell phone or a landline. Some of these standards mirror the TSR's, but others do not. The FCC's standards for complying with the national do-not-call list for telemarketing calls are similar to the TSR's. The FCC, like the TSR, establishes company-specific do-not-call rights for consumers, but the standards are different. Most significantly, the FCC's approach requires callers to have a written do-not-call compliance policy that is available upon request to anyone who asks to see it.

The second key element of the FCC's telemarketing standards regulates the use of auto dialers and prerecorded messages. This is primarily a consent standard. Callers must have "prior express written consent" to use an auto dialer or a prerecorded message to place a telemarketing call to a cell phone, and they must obtain "prior express consent" to use auto dialers or prerecorded messages to place a telemarketing call to a residential landline. The "prior express written consent" required by the FCC's TCPA rule must be a written agreement signed by the consumer. It should include the consumer's telephone number, identify the seller receiving the consent, and be sufficient to show that the consumer received

"clear and conspicuous" notice of what the consumer is agreeing to. What makes the FCC's approach for TCPA stricter than the FTC's for TSR is that the consent must also be sufficient to show that the consumer received clear and conspicuous notice of the fact that the seller cannot condition a purchase on the consumer providing this consent. The TSR also prohibits conditioning a purchase on this consent, but the TSR does not require the agreement to say so. Customers can withdraw their consent "through any reasonable means," including orally, at any time. **The FCC has interpreted this to mean customers can use words such as "stop, quit, end, revoke, opt out, cancel, or unsubscribe" to withdraw their consent**.

Compliance Tip

The FCC requires businesses to honor consent withdrawal requests made through "any reasonable means," including through the use of the words "stop, quit, end, revoke, opt out, cancel, or unsubscribe."

Effective on April 11, 2025, the FCC will require telemarketers to honor consent withdrawal requests and do-not-call requests within 10 business days.

Watch List for 2025

Starting on April 11, 2025, businesses will have 10 business days to honor consent withdrawal requests and do-not-call requests relating to the businesses' telemarketing.

The FCC has taken the position that a text message is equivalent to a telephone call to a cell phone and is subject to the same consent requirements as auto dialed calls and prerecorded messages. As a result, any marketing text message sent using technology that satisfies the TCPA's auto dialer definition requires "prior express written consent." If a customer withdraws consent to receive marketing text messages, **the FCC has amended its TCPA rule to allow the telemarketer to send one text message in response confirming or clarifying the scope of the request within 5 minutes.**

Did You Know?

Businesses have 5 minutes after a consent withdrawal request to send a text confirming or clarifying the withdrawal.

Addressing requirements for consent, the FCC finalized its One-to-One Consent Rule in 2024, which becomes effective on January 27, 2025, modifying the TCPA's definition of "prior express consent" to mean "an agreement, in writing, that bears the signature of the person called or texted that clearly and conspicuously authorizes no more than one identified seller to deliver or cause to be delivered to the person called or texted advertisements or telemarketing messages using an automatic telephone dialing system or an artificial or prerecorded voice." In addition, "[c]alls and texts must be logically and topically associated with the interaction that prompted the consent and the agreement must identify the telephone number to which the signatory authorizes such advertisements or telemarketing messages to be delivered."

The FCC's new One-to-One Consent Rule definition makes a couple significant changes to marketing lead generation activities. First, a telemarketer must now directly obtain consent from a consumer before sending the consumer marketing messages, and it can no longer rely on the consumer's consent provided to the marketer's affiliates. Put simply, multiple marketers can no longer rely on a single consent from a consumer under the Rule. Second, a telemarketer can only send marketing messages to the consumer that are "associated with the interaction" that prompted the consent. The FCC does not further define this requirement but offers an example that "a consumer giving consent on a car loan comparison shopping website does not consent to get robotexts or robocalls about loan consolidation." Given the ambiguities in the Rule, litigation against the Rule is expected.

In the meantime, however, auto dealers should audit their lead generation practices to ensure they comply with the rule when telemarketing to consumers.

Compliance Tip:

Review your marketing lead buying practices to comply with the FCC's new One-to-One Rule set to take effect on January 27, 2025.

The FCC also imposes disclosure requirements that are specific to prerecorded messages. Prerecorded telemarketing messages must identify the seller at the outset of the message and provide the seller's telephone number during the message. Consumers must be able to use the telephone number provided to make a company-specific do-not-call request. These messages, even with valid consent, must include an automated mechanism for making a company-specific do-not-call request. Messages left on voicemail must provide a toll-free number that connects to this type of automated opt-out mechanism. The mechanism must immediately disconnect from the consumer's line after the consumer uses it.

Like the TSR, the FCC's TCPA rule prohibits abandoned telemarketing calls but establishes a safe harbor allowing for restricted use of a predictive dialer. Notably, unlike the TSR, the FCC's safe harbor requires the brief message identifying the caller by name and telephone number to also include an automated mechanism for making a company-specific do-not-call request. The TCPA, like the TSR, prohibits telemarketing calls before 8:00 a.m. or after 9:00 p.m. and requires transmission of caller ID information in every telemarketing call. **The TSR can be enforced by the FTC and State Attorneys General.**

Compliance Tip

Do not make telemarketing calls before 8:00 a.m. or after 9:00 p.m.

The TCPA provides for unlimited strict liability of $500 to $1,500 per call or text message made using an auto dialer and without obtaining proper advance written consent.

Did You Know?

You could be fined $500 - $1,500 per call or text message under the Telephone Consumer Protection Act (TCPA) if you haven't obtained written consent.

There is a similar penalty structure for the TCPA's do-not-call provisions, but the penalty figure is an "up to" amount that courts can adjust, rather than a fixed amount. In the past, numerous class actions have been filed under the TCPA in large part because of the absence of any cap on class action damages. As a practical matter, the ability to enforce extends to the called party. The "called party" means the current phone subscriber or the customary user of the cell phone. As a result, you can be held strictly liable for a call to a wrong number, regardless of whether the original subscriber had previously provided his or her consent.

The FCC had established a one-call safe harbor for unintended calls to reassigned numbers, but a 2018 federal appellate court decision, *ACA International v. FCC*, vacated the FCC's "auto dialer" guidance and set aside the FCC's handling of TCPA liability for improper calls to reassigned numbers. **In response, the FCC created a Reassigned Numbers Database and established a new safe harbor rule effective in 2021 to replace the one-call safe harbor with a rule that callers are not liable for unintended calls to reassigned numbers if they can establish that they scrubbed their numbers lists against the FCC database within 30 days prior to the call.**

Compliance Tip

Scrub your telemarketing contacts list against the FCC Reassigned Numbers Database once every 30 days to protect against TCPA liability.

The database can be found on the FCC's website here: https://www.fcc.gov/reassigned-numbers-database.

The TCPA can also be enforced administratively by federal agencies. Federal agencies have brought cases alleging unfair, deceptive, or abusive acts or practices in the context of telemarketing campaigns. In light of those cases, when telemarketing products, a dealer must state promptly the purpose of

the call; clearly disclose, prior to purchase, the cost of the product and all material conditions, benefits, and restrictions relating to the product; disclose clearly that the purchase of the product is voluntary and not required; make all legally required disclosures in a clear manner and at a reasonable speed and cadence so the consumer can understand them; and after disclosures are read, require the customer to acknowledge the purchase is voluntary and that the customer affirmatively requests or consents to purchase the product. If the product has a cancellation or refund policy, the dealer must disclose the policy and give the phone number to cancel and the time in which to get a refund. The customer's purchase and means of payment must also be disclosed and confirmed. If paying by credit card, the customer must give the full credit card number for payment to the sales representative.

Mini-TCPA Laws

After the Facebook ruling, some members of Congress and consumer advocacy groups saw a liability gap that needed to be filled. A few states responded by enacting new telemarketing laws (so-called "mini-TCPAs") to more tightly regulate telemarketers who have not been given express consent from individuals to receive certain telemarketing calls or texts. For example, Florida quickly passed its own legislation, the Florida Telephone Solicitation Act, in 2021 to more broadly regulate all "telephonic sales calls," not just auto dialers. **The Act was amended in 2023 to, among other things, limit the categories of equipment to which the Act applies and provide a 15-day notice and cure period before a lawsuit can be brought under the TCPA.**

Did You Know?

Multiple states have enacted their own telemarketing laws (called "mini-TCPAs") to impose additional requirements on companies engaged in telemarketing.

Following Florida's lead, Oklahoma passed its Telephone Solicitation Act in 2022 to regulate any "commercial telephonic sales call" in that state. Washington then passed its Commercial Telephone Solicitation Act in 2022 to regulate "unsolicited telephone solicitations." Washington has since also passed a Robocall Scam Protection Act in 2023 to prohibit telemarketing, and even assisting with telemarketing, through an "automatic dialing and announcing device." Until it becomes clear how courts will interpret these three state laws, dubbed mini-TCPA's because of their broad prohibitions, companies operating in these states face considerable uncertainty about what practices may result in liability.

Several other states have enacted their own mini-TCPAs in recent years. For example, Maryland's Stop the Spam Calls Act took effect in 2024 to prohibit telemarketing through "an automated system for the selection or dialing telephone numbers" or "the playing of a recorded message when connection is completed to the number called." Other states, including Arizona, Connecticut, New York, and Tennessee, have amended their "do not call" laws to specifically ban text message solicitations or require certain do-not-call option disclosures. Many states provide "quiet hours" during which telemarketing cannot occur and maintain state-specific do-not-call lists to which telemarketers must adhere when placing calls or sending texts.

Given that these rules are very complicated and vary state by state, you should consult with an attorney on your specific marketing practices, particularly to confirm whether you are using an auto dialer, are subject to other aspects of the TCPA, or are calling or texting individuals in particular states that may have heightened requirements for telemarketing. Due to increasing potential liability under these laws, **we recommend as a best practice that dealers obtain prior express written consent from customers before marketing through calls or texts to customers.**

Recommended Practice

Obtain prior express written consent from customers before marketing through calls or texts to customers.

Email

The federal CAN-SPAM Act of 2003 requires that each commercial email conspicuously give the consumer a way to opt out of receiving further commercial messages.

Did You Know?

When a customer unsubscribes from an email list, you have 10 days to honor their opt-out request.

Senders must honor opt-out requests within 10 business days. Commercial emails also must contain the sender's address, a notification that the message is an advertisement, and other specific language. CAN-SPAM prohibits misleading subject lines and "from" line information. The prohibition on misleading "from" lines also applies to "transactional or relationship" messages, which are emails that relate to an existing business relationship between the sender and recipient and that do not market products or services, such as messages informing a customer of a warranty or recall notice. Your counsel can advise you about state email laws and the interplay between federal and state email standards.

Fax

The TCPA, as amended by the Junk Fax Prevention Act of 2005, restricts the ability to send fax advertisements. Unsolicited fax advertisements are prohibited unless they are based on an established business relationship between the parties or prior express invitation or permission. The general rules are that the first page of the fax advertisement must include a clear and conspicuous notice providing instructions for opting out of future advertising faxes from the sender. This notice must explain the recipient's opt-out rights and note that a sender's failure to honor an opt-out request within 30 days is unlawful. This notice must also include a telephone number and fax number for submitting an opt-out request. If neither of these options is toll-free, the notice must also provide a cost-free opt-out mechanism available via a website or email address. The sender's opt-out mechanism must be available to receive opt-out requests 24 hours a day, 7 days a week. The required opt-out notice must include instructions for submitting a valid request. Specifically, the notice must explain that the request must include the recipient's fax number, and the request must be submitted using the means made available by the sender. The FCC has said that even fax advertisements that are based on the recipient's express permission must include this opt-out notice, but a federal appellate court challenged this position as regulatory overreach that is not supported by the statute. Senders must honor opt-out requests in the shortest reasonable time, not to exceed 30 days.

Under a separate standard administered by the FCC, all fax communications must contain, at the top or bottom margin on the first page, the date and time of transmission and, on every page, the sender's identity.

Recommended Practices

1. **If you conduct direct marketing, periodically scrub your target lists for persons who have excluded themselves from the means of communication you intend to use (telemarketing, faxes, and email).**

Recommended Practice

If you conduct direct marketing, don't forget to periodically remove people who have opted out or unsubscribed.

You should keep a separate list of consumers who opt out of telemarketing, faxes, and email and be careful before using an auto dialer or prerecorded message to obtain the appropriate consents from the party you are calling or texting. This consent must include specific disclosures and comply with specific content requirements. Adequately scrub telemarketing lists of phone numbers against the FTC's National Do Not Call Registry (www.donotcall.gov), your state's Do-Not-Call list and your dealership's list of persons who have asked not to be called. The Association of National Advertisers (www.ana.net) also maintains "do not contact" lists that you should scrub your lists against. If you are telemarketing, get assurances from vendors on having obtained customer consents and exclusions of persons listed on federal and state Do-Not-Call lists, then double-check against Do-Not-Call lists, as well as your own dealership's list of customers who

have asked not to be called. The class action liability potential under the TCPA makes this a critical area for businesses to be compliant. Also, note that many State Attorneys General and Motor Vehicle Departments have their own rules or guidelines for advertising motor vehicles.

2. Maintain an internal do-not-call list independent of any other applicable do-not-call lists.

Recommended Practice

> Maintain an internal do-not-call list independent of any other applicable national or state do-not-call lists.

You must regularly scrub your internal target lists against the applicable federal and state do-not-call lists to remove consumers who have opted out of communications (i.e., telemarketing, texts, faxes, e-mails) from you or your affiliates and update these opt-out lists at least every 30 days for landlines and every 15 days for wireless cell numbers. Out of an abundance of caution, we recommend that you scrub your internal target lists every 14 days. Note that state laws may have more restrictive requirements, and we recommend that you consult with your local attorney.

3. Obtain a customer's prior express written consent before delivering telemarketing calls or text messages with an automatic dialer, including prerecorded messages.

Recommended Practice

> Get a customer's written consent before using an auto dialer to call or send texts with marketing messages.

If you want to take a more prudent approach, you could adopt a policy and implement a practice whereby you obtain a consumer's express written consent before making any telemarketing calls regardless of whether the calls are made with an automatic dialer and/or include a prerecorded message. Indeed, this prior consent approach is required in a number of countries outside the United States. For example, see Canada's Anti-Spam Law (CASL).

4. Honor do-not-call list requests and consent withdrawal requests promptly and within at least 10 business days.

Recommended Practice

> Honor do-not-call list requests and consent withdrawal requests promptly and within at least 10 business days

Under the FCC's rules for implementing the TCPA, businesses are required to honor customer requests to be added to a business's internal do-not-call list or to stop receiving telemarketing messages, whether by phone or email, within 10 business days. To avoid penalties for noncompliance with the TCPA, businesses should aim to respond to such requests earlier, within 5-8 business days if possible.

5. Vet all third-party telemarketing vendors.

Recommended Practice

> Vet all third-party telemarketing vendors because you could be held responsible for some of their actions.

If you decide to hire a third party to make telemarketing calls, it is recommended that you conduct due diligence on the third party's policies and procedures, litigation history (e.g., whether the third party was named in any relevant litigation), and any public complaints lodged against the third party, among other things. Also, as with the use of any third party, ensure that any personal information shared with them will not be used for purposes outside the scope of the agreement to avoid the transfer of data constituting a "sale."

Additional Resources:

FCC, Reassigned Numbers Database
https://www.fcc.gov/reassigned-numbers-database

FCC, FCC Adopts New Rules to Empower Consumers to Stop Unwanted Robocalls and Robotexts (February 2024)
https://docs.fcc.gov/public/attachments/DOC-400522A1.pdf

FCC, TCPA Final and Proposed Amendments (February 2024)
https://docs.fcc.gov/public/attachments/FCC-24-24A1.pdf

FCC, One-to-One Consent Rule ("Prior Express Written Consent" Definition) (December 2023)
https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-L/section-64.1200#p-64.1200(f)(9)

FCC, FCC Closes 'Lead Generator' Robocall Loophole & Adopts Robotext Rules (December 2023)
https://www.fcc.gov/document/fcc-closes-lead-generator-robocall-loophole-adopts-robotext-rules

FCC, Targeting and Eliminating Unlawful Text Messages (December 2023)
https://docs.fcc.gov/public/attachments/FCC-23-107A1.pdf

FTC, FTC Implements New Protections for Businesses Against Telemarketing Fraud and Affirms Protections Against AI-enabled Scam Calls (March 2024)
https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-implements-new-protections-businesses-against-telemarketing-fraud-affirms-protections-against-ai

FTC, CAN-SPAM Act: A Compliance Guide for Business (January 2024)
https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business

FTC, Complying With the Telemarketing Sales Rule (May 2023)
https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule

Contact Center Compliance, TCPA & DNC FAQ
https://www.dnc.com/faq/whats-difference-between-tcpa-and-dnc

Recordkeeping Practices

The records of your dealership are critical assets but often contain sensitive information that should not be kept forever. Record retention and destruction policies are vital for safeguarding, storing, and disposing of records according to the law and your business needs.

Develop appropriate policies for record retention and destruction →

Did You Know?

The FTC's Telemarketing Sales Rule was amended in 2024 to require telemarketing scripts, marketing materials, customer information, and other information relating to telemarketing campaigns to be retained for a minimum of five years instead of 24 months.

Watch List for 2025

The required retention period for Office of Foreign Asset Controls (OFAC) records, including records of checking customers against OFAC's list of Specially Designated Nationals and Blocked Persons, will increase to ten years starting on March 12, 2025.

Compliance Tip

Avoid maintaining records in hard drives of physical devices, such as laptops, tablets, phones, and more, that could expose the records to potential security breaches if the device ends up misplaced or stolen. See more Recommended Practices

Recommended Practice

Only retain records containing customer information for as long as necessary for legal compliance and for your business purposes, then securely destroy them to protect the information from exposure to potential data breaches or other security incidents. See more in Electronic Storage of Business Records

Breakout Sections

Recordkeeping Practices

The records of an auto dealer are critical assets of its business, including all records produced and received in connection with the operation of the dealership's business, whether such records are in a physical or electronic format. **A company record may be as obvious as a memorandum, an email, or a contract, or something less obvious, such as a computerized desk calendar, an appointment book, an instant message, a text message, an expense record, a social media website entry, or a blog posting.**

Did You Know?

An appointment, IM, text message, expense record, and even a social media post are all considered company records.

Information contained in flash drives, memory sticks, PSTs, USB drives, backup tapes, and on wireless devices such as iPhones, Android phones, PDAs, tablets, and other portable media can also be company records. This Topic focuses principally on federal laws and regulations regarding records of vehicle sales, leases, and finance & insurance(F&I).

Records Maintenance and Retention Policy

It is important that your dealership **have a policy on records maintenance and retention**,

Compliance Tip

Create a policy on records maintenance and retention that includes keeping records centrally, rather than on local drives on PCs or portable devices.

and it is recommended that your records be kept centrally rather than contained on local PCs or portable devices to make your policy easier to administer. You have to know where your records are located before you can effectively manage them. This is especially true for electronic records.

In addition to knowing where your records are, you also want to know how long to keep (or not keep) records. In particular, you want to ensure that you are not maintaining sensitive consumer information longer than necessary. The FTC has repeatedly warned that companies should retain nonpublic personal information (NPI) only as long as necessary to fulfill the business and regulatory purposes for which it was collected, because keeping such information creates a risk to consumers. Moreover, retaining all sensitive consumer information forever is expensive from a storage perspective and, in the event of a data security breach, could subject the business to increased liability. There are many reasons to retain records, however. State record retention laws range from employment records to service and waste disposal records, and record retention requirements are not uniform among the states. Every state has its own retention requirements for dealer sales records, auto repair and servicing records, tax records, payroll and employment records, and environmental and facility-related records, among others. Consult your local counsel or compliance professional when establishing retention periods for specific categories of your dealership's records.

Important Laws and Regulations

Federal and state record retention requirements generally apply no matter what the record's format or characteristic (i.e., both physical and electronic).

Did You Know?

Different regulations require records to be maintained for different periods of time.

Failure to retain records for the required time periods can subject a dealership to penalties or fines. Adequate resources should be allotted to develop and implement a record retention policy that reflects applicable federal and state requirements.

For example, the Equal Credit Opportunity Act (ECOA) requires generally that all written or recorded information concerning a credit application (including any credit report on the consumer, any notation of action taken, such as adverse action notices, risk-based pricing notices, and decisions sent back by finance sources, as well as any documents submitted by the consumer, such as paystubs) must be retained for a minimum period of 25 months after the consumer is notified of the action taken on their credit

application (e.g., approval, counteroffer, adverse action notice, or notice of incomplete application). **This includes information on completed deals, "dead deals," or withdrawn credit applications where the dealer never completes a credit transaction with the consumer.**

Recommended Practice

Due to federal & state record retention requirements, you should retain applicant records for both completed deals and "dead deals" or withdrawn credit applications where the dealer never completes a credit transaction with the consumer.

However, many attorneys advise dealers to retain these records for at least five years from notification of the credit decision, which is the outside limit of the statute of limitations period during which a consumer can bring a claim under ECOA.

An entity is required to maintain evidence of compliance with the Electronic Fund Transfer Act (EFTA) and Regulation B (ECOA's implementing regulations) for two years. Under the Fair Credit Reporting Act (FCRA), the statute of limitation is the earlier of two years after the date when the plaintiff discovers the violation that is the basis for such liability, or five years after the date on which the violation that is the basis for such liability occurs.

Under the FCRA, prescreen selection criteria must be maintained in writing for three years after the offer was made to the consumer. Office of Foreign Assets (OFAC) **records must be retained for five years, but that will increase to ten years starting on March 12, 2025**.

Watch List for 2025

OFAC records must be retained for 10 years instead of 5 years starting on March 12, 2025.

States may impose additional retention period requirements. Consult your local counsel on the appropriate retention period for your dealership in your state.

Under Regulation Z, which implements the Truth in Lending Act (TILA), creditors are required to retain evidence of compliance with lending disclosure requirements up to two years after the date the disclosures are required to be made or action is taken. Lessors are required to retain evidence of compliance with Regulation M, which implements the Consumer Leasing Act (CLA), other than advertising, for a period of not less than two years after the date of the disclosures are required to be made or an action is required to be taken.

Your contracts with consumer reporting agencies and lenders may also have record retention rules that you must comply with.

FTC Consumer Report Information and Records Disposal Rule

The Disposal Rule requires persons who maintain or otherwise possess consumer report information for a business purpose to properly dispose of such information by taking reasonable measures to protect information against unauthorized access or use in connection with its disposal. For example, **paper records should be cross-shredded, burned, or pulverized so the consumer information cannot be read. Consumer information must also be destroyed or erased from all electronic media so that the information cannot be read or reconstructed.**

Compliance Tip

Once the record is no longer needed or legally required, completely destroy the record in a way that the information cannot be read or reconstructed.

For PCs, copiers, smartphones, tablets, and fax machines, this means not only deleting the information but wiping the hard drive clean, as deleted information can remain on the hard drives of these digital devices even if the data is "deleted" by the user. The Disposal Rule also requires that dealers properly vet and supervise any records disposal company used by the dealers.

Disposal destruction procedures should be included as a part of a dealership's Information Security Program (see Topic 4) and followed systematically.

Telemarketing Sales Rule

The FTC's Telemarketing Sales Rule was amended in 2024 to require that telemarketing scripts and marketing materials, customer information, and other information relating to telemarketing campaigns be kept for a minimum of five years from the date the record is produced, instead of the previous minimum of 24 months.

Did You Know?

Telemarketing scripts and related marketing campaign materials must be kept for a minimum of five years.

If a dealer uses a telemarketing firm, the dealer should consider requiring the telemarketing firm by contract to retain the necessary records on its behalf. However, record retention remains the dealer's responsibility. An agency's failure to retain records for the dealer will not provide a viable defense in court.

The Telephone Consumer Protection Act's (TCPA) recordkeeping provision is much narrower. However, callers bear the burden of proving that their telemarketing conduct complies with the law, creating a virtual recordkeeping obligation. Based on the statute of limitations for bringing a TCPA claim, dealers should consider keeping these records for at least four years.

Electronic technology has made the issue of recordkeeping and destruction far more complex and critical. Electronic records include more than Word documents, emails, and text messages. They include any electronically stored information generated or contained in the hard drive of any media or in any storage item, including PCs, servers, copiers, fax machines, smartphones, tablets, PDAs, USB flash drives, laptops, and other portable devices. Electronic records include drafts, instant messages, charts, PowerPoints, spreadsheets, and other documents composed, sent, or received by the device. They constitute the largest percentage of records your dealership creates and uses today. If you are sued, discovery of electronic documents becomes a costly process, as you will need to search all devices and cannot simply rely on what is on your central servers.

Email and text messages present a particular challenge for records retention programs. **It is important to develop and consistently maintain a specific policy on email and text message retention and deletion.**

Compliance Tip

Develop and maintain a policy on email and text message retention and deletion.

There is no perfect time period during which you must generally retain emails or text messages (subject to the requirements of any laws that apply to the subject matter of such message), but long email or text message retention periods will cause a greater expense in searching and identifying relevant emails and texts in the event of a lawsuit. The same is true for other forms of instant messages and chats, which are also electronic records. For example, consider encouraging your employees to engage in best practices with emails and texts, such as not selecting "reply to all" on sensitive emails when not necessary, as it causes emails to proliferate and potentially end up being received by the wrong people.

Telephone Consumer Protection Act

To comply with the TCPA, an entity must develop policies and implement procedures to meet retention obligations, as well as train employees on compliance. The policy should outline the retention of various pieces of information. Specifically, the policy should: (i) clearly address opt-out mechanisms; (ii) require periodically scrubbing call lists against the national Do Not Call Registry and internal do-not-call lists (which requires maintaining opt-out lists and internal do-not-call requests); (iii) ensure that any third-party vendor used to make calls complies with the TCPA, and (iv) obtain written consent from customers to receive telemarketing messages, among other things. Further, to maintain compliance with the TCPA, keep all records of consents given by customers for at least four years. You can find more information to help you comply with the TCPA in Topic 10.

Electronic Storage of Business Records

Most states have adopted a form of the Uniform Photographic Copies of Business and Public Records as Evidence Act. Except for certain limited categories of documents, states generally permit the conversion of paper documents to electronic form for recordkeeping purposes. Federal and state evidence laws also permit the use of electronically converted documents in lawsuits or regulatory proceedings. The electronic records must be authentic reproductions of the original and be deemed to be reliable, trustworthy, and accurate for their use as evidence. A paper record should be electronically captured at or near the time of the event or transaction and must be complete and available for retrieval as requested for regulatory or business purposes. The context and the structure of the electronic record must also be preserved for the full retention life of the record, including any migration of the record from one system or medium to another. If a record is electronically converted in a trustworthy manner, the original paper record generally can be securely destroyed.

Federal privacy laws and regulations require that documents containing personal customer information must be handled, maintained, and disposed of in a secure manner. If these records are not securely maintained and then destroyed when no longer required, they may be vulnerable to unauthorized acquisition or use (e.g., identify theft). Further, a dealership may be subject to an enforcement action by the FTC for violating the Safeguards Rule and Disposal Rule, private litigation, or administrative proceedings under state law.

The FTC treats retaining consumer information longer than necessary as a shortcoming in data security that, along with other security deficiencies, can constitute "unfair acts or practices" in violation of Section 5 of the FTC Act. **Again, the FTC has repeatedly stated its position that businesses should keep records containing customer information only for as long as necessary**, and then destroy them in a secure manner, uniformly for both paper and electronic records.

Compliance Tip

Only retain records containing customer information for as long as necessary for legal compliance and for your business, then securely destroy them.

This also helps to eliminate unnecessary customer information from your records that could be obtained during a data breach or other security incident.

In the event of actual or threatened litigation or regulatory enforcement proceedings, a dealer should immediately implement a "litigation hold" process suspending all electronic and physical document destruction and requiring employees to identify and preserve relevant documents, including emails and text messages. Even inadvertent or negligent destruction or loss of email, texts, or other documents relevant to a threatened or pending lawsuit or investigation can be grounds for a court to impose sanctions for "spoliation" (destruction) of evidence. Recently, a number of states have recognized private tort claims for the negligent spoliation of evidence.

Recommended Practices

1. **Have a comprehensive record retention policy for both paper and electronic records and consistently apply it.**

Recommended Practice

Train your employees on your record retention policy for both paper and electronic records and apply it consistently towards your business practices.

Know what records you keep, and only keep records you need for business. Know where they are located and why you keep them there. Categorize your records and know the federal and state laws on mandatory time periods for retaining different categories of records. Your records policy should define how, for how long, and where your records are maintained, as well as when and how records are to be destroyed. Your practices should be consistent with your policy. The policy should also describe responsibilities relating to company

records. Train your employees on your policy and obtain their written acknowledgement to comply with it. Limit and log all access to all records (paper and electronic) containing personal customer information.

2. **Avoid maintaining records in the hard drives of personal computers, laptops, tablets, memory sticks, PSTs, flash drives, or remote storage devices such as smartphones.**

Recommended Practice

> Avoid maintaining records in the hard drives of personal computers, phones, portable computing or storage devices (e.g. thumb drives, memory sticks) to reduce likelihood of security breaches.

This can expose those records to potential data breaches or other security incidents, especially if the device containing the records gets misplaced or otherwise falls into the wrong hands. It is a best practice to maintain records only on central servers and limit users to "read only" access on their remote devices.

3. **Consider using electronic documents and obtaining electronic signatures instead of ink ones.**

Compliance Tip

> For easier record tracking and retention, consider using electronic documents and obtaining electronic signatures instead of ink ones.

Electronic documents—credit applications, contracts, notices, consents—are more secure and easily retrieved when stored centrally in limited-access electronic databases or in a secure cloud server where they won't get lost in file warehouses. Scan paper documents to upload into your electronic document storage system. Most states generally permit electronic storage of records, including conversion of paper original documents to electronic format for storage. Certain electronic records systems permit key word or phrase searching to locate documents as well. This makes locating documents much less tedious, particularly if the records are maintained in a central server or repository and not on PCs and remote devices. Your records storage policy should also address employees using their own devices for dealership business. No non-public information (NPI) should be permitted to be downloaded to any personal device or storage means such as a USB port or external hard drive.

4. **Retain company records only until they are of no further use or value to you and after any legally imposed retention time periods have expired**

Recommended Practice

> Retain company records only until they are of no further use or value to you and after any legally imposed retention time periods have expired.

After a record's current use and legally mandated retention period has passed, either securely destroy the record or store it in a safe, secure, and less accessible location. Securely destroy all records containing any personal information of customers, especially records that contain Social Security numbers, drivers' licenses, and credit or debit card account numbers. Be careful when discarding old computers, cell phones, flash drives, and smartphones. Even "deleted" information may remain on a hard drive or flash memory. Copiers and fax machines also contain hard drives that retain copies of records, especially if they contain scanning functions or online connections. Destroy the hard drive or use a software program that will irrevocably erase and expunge all of the information before trading the items in or discarding them.

5. **Implement and enforce a retention policy for email and text messages.** Most casual email and text messages should be purged from your system within a short time, unless their subject matter triggers any retention laws. **Junk email should be purged immediately.**

Recommended Practice

> Junk email should be purged immediately because it can contain malicious links, phishing attempts, or malware that could compromise your security, and by deleting it quickly you minimize the risk of accidentally clicking on something harmful.

Identify a general time frame from creation in which all email

(both sent and received items) will be purged unless a user takes affirmative action to archive or otherwise preserve the email as a business record. Make preservation an email-by-email task rather than allowing preservation of all emails. **Attempt to centralize all emails and avoid letting them be moved to PC hard drives, memory sticks, PSTs, USB drives, remote devices, or forwarded to a web-based email address or other non-central storage.**

Compliance Tip

Avoid moving emails or collecting Personally Identifiable Information from personal email addresses or other non-central storage.

Do the same with text messages. Educate employees on good email practices such as limiting the number of recipients and sending shorter emails only for the purpose of creating action by the recipient. Have a procedure to suspend email and text message purging in the event of a "litigation hold" until all email and text messages relevant to the litigation hold have been identified, segregated, and preserved. Failure to do so may give rise to a "spoliation" claim.

6. **Identify and retain any records that may be relevant to a lawsuit or possible regulatory inquiry.**

Recommended Practice

Retain any records that may be relevant to a lawsuit or regulatory inquiry.

Establish a process for a "litigation hold" that halts the document destruction process for paper and electronic documents (including emails and text messages) so as not to destroy documents that may be relevant to ongoing or potential litigation or to a government audit. Having a consistent document destruction policy and centralization of electronic records onto company or cloud-based servers, and not individual devices like flash drives, laptops, tablets, smartphones, or external hard drives, can facilitate electronic discovery in litigation.

7. **Secure records that contain consumer information in accordance with your FTC Safeguards Rule Information Security Program,**

Recommended Practice

Secure records that contain consumer information in accordance with your FTC Safeguards Rule Information Security Program.

and destroy these documents securely when they are no longer required under your FTC Information Disposal Program. Be consistent in recordkeeping and destruction times. The current Safeguards Rule requires automobile dealers to develop, implement, and maintain an information security program with technical, administrative, and physical safeguards for handling consumer data. See Topic 4 for more on the Safeguards Rule and other data security requirements.

8. **Exercise due diligence in hiring a vendor to store, dispose of, and destroy your records.** Have a trusted dealership employee supervise any vendor destroying records that contain customer information. Ask the vendor about its background checking processes and bonding of employees who will collect and destroy customer information documents. **Do your due diligence on a vendor who will store your records in a cloud server, particularly as to their security certifications and experience in handling attempted or actual breaches of their server.**

Recommended Practice

Secure records that contain consumer information in accordance with your FTC Safeguards Rule Information Security Program.

Your vendor contract should give you the right to audit and obtain a copy of the vendor's security audits and impose indemnification and liability on the vendor for any costs or losses incurred in any data security breach that results in your customer information being wrongfully accessed or compromised, including the costs of sending notices and giving affected customers at least a year of credit monitoring services.

9. Assess the risk of collecting and keeping too much data or records that are not required.

Recommended Practice

> Even if certain data may not need to be destroyed, consider whether the benefit of keeping that data outweighs the potential cost of doing so.

Many businesses believe that the more data they have, the better they can perform. While it is true that a lot of data often leads to better analytics, it is equally important to assess the cost to benefit ratio of keeping too much data and risking breaches of that data. Remember: If you do not need it and it is not legally required, consider deleting it.

Additional Resources

U.S. Chamber of Commerce, How Long Should Your Small Business Keep Documents? (November 2024)
https://www.uschamber.com/co/start/strategy/how-long-to-keep-business-documents

Iron Mountain, Fundamentals of Records Retention Schedule (April 2024)
https://www.ironmountain.com/resources/whitepapers/f/fundamentals-of-records-retention-schedule

Forbes, The Data Purge: An Era of Defensible Retention and Data Minimization (June 2023)
https://www.forbes.com/sites/douglaslaney/2023/06/13/the-data-purge-an-era-of-defensible-retention-and-data-minimization/?sh=9b86572b2416

Xfinity, How to Remove Personal Information on a Phone (October 2022)
https://www.xfinity.com/mobile/support/article/remove-personal-information-from-phone-returns-exchanges

BizTech Magazine, How to Prepare Your Company for E-Discovery (December 2012)
https://biztechmagazine.com/article/2012/12/how-prepare-your-company-e-discovery

Association of Records Managers and Administrators (ARMA), Standards and Best Practices for Records Maintenance
https://www.arma.org/page/standards

CMS

Compliance Management Systems

Dealers must maintain a Compliance Management System (CMS) of policies and procedures that protect their dealerships and customers through compliance with state and federal law. The CMS should address business information safeguards, customer communication practices, vendor oversight, and more.

Keep your CMS updated with best practices for legal compliance →

Did You Know?

While dealers may outsource services to vendors, they cannot outsource their responsibility for compliance with federal and state laws. Ensure your CMS addresses the fact that regulators may hold dealers responsible for compliance violations that result from vendors' actions on their behalf. Read more in Vendor Management

Compliance Tip

Identify for each credit sale whether you charged a customer the dealership's standard participation rate or whether you decreased that rate for a reason pre-identified in a ECOA/Fair Lending form included in your CMS, such as the NADA form linked in the Additional Resources below. See more Compliance Tips

Watch List for 2025

Recent studies have found that between 88 to 95 percent of data breaches result from employee negligence. Ensure your employees are properly trained in your CMS's record safeguarding, retention, and destruction policies to help protect your dealership from data breaches in 2025.

Recommended Practice

Involve your owner/management in your CMS implementation and monitoring, such as by naming a senior officer of your dealership to be in charge of your ECOA/Fair Lending policy, to improve your culture of compliance and increase employee adherence. See more Recommended Practices

Breakout Sections

Compliance Management Systems

Compliance is a critical priority for any auto dealer. Done properly, it will save dealerships costs and expenses and help them avoid practices that could result in fines, damages, and penalties from federal and state government investigations or consumer lawsuits. In today's business environment, it's more than a best practice to adopt a Compliance Management System (CMS). It's a business necessity, just as it is critical to bring a culture of compliance into your dealership that starts with senior management support.

CMS Implementation

A CMS consists of your policies, procedures, and operational practices, and it is designed to promote compliance with applicable laws and regulations. It does not have to be a hugely complex undertaking; you may have many of the necessary policies and procedures described in this Compliance Guide – as well as corresponding practices – already in place. Effectively documenting and maintaining your policies, procedures, and practices can be key to your defense if you are ever investigated.

An effective CMS starts from the top. It should be approved and championed by your Board of Directors or, if you don't have a Board, your executive officers and dealer principals. The senior officer in charge of the CMS should report to your Board or senior management group on dealership compliance at least semi-annually and preferably quarterly, so that omissions or potential violations are quickly identified and corrected.

CMS Policies and Procedures

Your CMS program and documentation should be aligned with your dealership's policies and practices and be in full compliance with the requirements of consumer protection laws. **It should develop and maintain a sound policy and compliance program for the entire set of products and services offered to consumers.**

Compliance Tip

Develop and maintain a policy and compliance program for all the products and services your dealership offers to consumers.

The CFPB regularly issues guidance about the components of a CMS for financial institutions through its Consumer Financial Protection Circulars launched in 2022. These Circulars and other guidance represent best practices for dealers not subject to CFPB jurisdiction, as well. A CMS must have control procedures to ensure your dealership stays compliant. Compliance audits, policy reviews, corrective action, and policy and procedure modifications on an ongoing basis are essential. The CMS and component policies should also provide that dealership employees will be held accountable for conduct that does not meet the requirements under the CMS, whether in the form of adverse compensation consequences and/or termination of employment for repeat offenders.

Much of your CMS will include a compilation of policies that we have discussed in this Compliance Guide. These include your Privacy, Safeguards, Data Destruction, Red Flags, Fair Credit, Fair Lending, UDAP, Advertising and Marketing, Customer Complaints, Record Retention, and other subject matters referenced within the preceding Topics.

Training and Monitoring Employees

A CMS is only effective if properly implemented. A critical component of an effective CMS is ongoing employee training and monitoring. Employee training helps employees understand their legal obligations and the consequences of non-compliance. For example, **a recent joint study by Stanford and Tessian revealed that employee negligence is the leading cause of 88% of data breach incidents, while a separate study by IBM suggests the figure may be closer to 95%.**

Did You Know?

A principal cause of data security breaches is simply employee negligence. Providing continuous employee training can reduce the chance of inadvertent compliance violations and mitigate operational and regulatory risk.

Table of Contents

Employee training helps employees to stay well-informed and equipped to mitigate operational and regulatory risk. Therefore training should be continuous, monitored for completion, and regularly updated to incorporate any new regulatory changes. Monitoring employee conduct in individual transactions, as well as monitoring data flow in your system and user activity can also help to identify possible patterns of irregularities. Employee training and monitoring reinforces the importance of compliance and helps employees apply best practices in their daily tasks, ensuring long-term legal and ethical adherence.

Tracking and Responding to Consumer Complaints

As part of your CMS, **regulators expect that you will have in place a formal program for tracking and responding to consumer complaints.**

Compliance Tip

Develop a formal program for tracking and responding to consumer complaints to maintain a positive relationship with customers, minimize legal risks, and foster continuous improvement within the dealership.

The CFPB has established an online consumer complaint database, and the FTC encourages consumers and businesses to file complaints about auto dealerships, as well. Consumer complaints go a long way toward establishing which dealerships the FTC and State Attorneys General will investigate for violations. To mitigate regulatory issues, seek to resolve consumer complaints informally through the dealership. This is not just about increasing consumer satisfaction scores. It's about avoiding the costs, expenses, and divergence of management time related to a regulatory investigation. Your CMS should describe the process for handling customer complaints, timelines for responding, methods for escalation and mediation, and resolution by a senior dealership officer or neutral third party, if necessary, as well as establish a mechanism for tracking complaints. Consider going the extra mile to resolve consumer complaints, even if it means the consumer may receive more than you believe they are entitled to. Treat every customer individually but use a consistent process of initiating complaint responses within a short period of time and having appropriate escalation procedures. Do your best to resolve the complaint within your dealership.

Vendor Management

The FTC and CFPB are watchful of vendor management oversight policies and functions, as some of your compliance work and many of your business processes may be outsourced to third parties. While your dealership can outsource services, it cannot outsource responsibility for compliance. You are ultimately responsible for the performance and any failures to perform or comply by your vendors. **Your CMS should contain a policy for selecting, managing, auditing, and resolving service,**

Did You Know?

While dealers may outsource services to vendors, they remain responsible for their vendors' compliance with federal and state laws while providing those services.

security, and performance issues with third-party service providers, and include the right to audit them. It is not enough to delegate any of your compliance obligations to third parties. You need to stay on top of them and make sure they are following your policies, particularly if they have the ability to access your customers' nonpublic personal information. In the CFPB's 2012 Bulletin on service providers, which was amended and re-issued in 2016, the agency indicated that it is critical for companies to:

- Conduct thorough due diligence of service providers;
- Review service providers' compliance policies, procedures, internal controls, and training materials;
- Include clear compliance expectations in service provider contracts, as well as appropriate and enforceable consequences for non-compliance;
- Regularly monitor service providers for compliance; and
- Take prompt and appropriate action for non-compliance, including termination of contracts.

While the CFPB's guidance applies to those entities subject to its jurisdiction, it can be used by any organization as a foundation for a service provider supervision program.

Dealer Finance Participation

Dealers should consider adopting and implementing an ECOA/Fair Lending policy that states the dealership's policy to not discriminate in any aspect of a credit transaction. Dealers should then monitor compliance with the same and address all issues as they arise. Staff training and monitoring buy rate participation can be a part of the policy. One good practice, originally developed by the Department of Justice (DOJ) as part of a prior enforcement action, is to implement a consistent buy rate participation amount for all customers and permit markdowns only for significant, nondiscriminatory, pre-identified legitimate business reasons. The reasons should be documented in the deal jacket to demonstrate the legitimacy of the action, should a finance source or regulator audit the dealer's practices. This documentation should be a purely internal document and not something given to the customer. This approach is the foundation of the NADA-NAMAD-AIADA Fair Credit Compliance Policy and Program Certification Form (NADA Form), which closely tracks not only the approach of the DOJ but also provides a list of the specific legitimate business reasons it approved in the case settlements it entered into in 2007 with two dealers. The NADA Form is linked in the Additional Resources below.

There are many examples of legitimate business reasons that justify differences in participation, and you should consult with your attorney to determine which of those is applicable to your dealership. But using the seven reasons suggested by the DOJ may be the safest course of action. These are:

1. The finance source's restriction on rate participation is lower than the dealers' standardized rate participation;
2. The customer's ability to satisfy monthly payment requirements is constrained;
3. The customer has a competing offer from another dealer or finance source;
4. The dealer extended a special promotional offer to all customers on the same terms;
5. The transaction is eligible for a captive's or other finance source's subvented interest rates (a rate typically subsidized by a vehicle manufacturer such that the APR the customer pays is below the finance source's typical buy rates, such as a 0% APR program);
6. The transaction is eligible for the dealership's employee incentive program; or
7. The dealer has documented inventory reduction considerations related to specific vehicles.

For example, if the customer has another offer of credit from a bank, credit union, or another dealer meeting or beating your APR, this could be a legitimate, non-discriminatory business reason for a different participation rate. Your ECOA/Fair Lending policy should have the specific requirements of your program including, for example, by how much a competing APR should beat your APR before you offer a lower rate. A good practice is to document in the deal jacket the name of the other creditor and the terms of the competitive offer. While such a practice will certainly not guarantee immunity from a credit discrimination claim, you will at least have a consistent policy and process to justify potential disparities in your portfolio.

In each credit sale deal jacket, you should insert the NADA Form (or a similar form) indicating either that you charged the customer the dealership's standard participation rate or that you decreased that rate for any of the pre-identified reasons in the form.

Compliance Tip

Identify for each credit sale whether you charged a customer the dealership's standard participation rate or you decreased that rate for a reason pre-identified in the NADA form.

Doing this consistently on every credit sale deal is one way to help protect your dealership from a credit discrimination claim. In creating the standardized non-discriminatory business reasons for a reduced participation, you should discuss your choices with your attorney prior to implementation. Consider using the DOJ reasons identified above as a guide to developing your reasons. Note that the CFPB has informally indicated that an open-ended "other" reason is not acceptable because the agency believes such a practice creates an opportunity for a dealer to apply its rate participation exception policy in an inconsistent manner.

In 2023, the CFPB launched a new auto finance data pilot, as part of its ongoing commitment to ensuring that the auto market provides fair, transparent, and competitive products and services. Specifically, the CFPB is concerned about larger loan amounts, higher monthly payments, and an increase in auto loan delinquencies, particularly for low-income consumers and those with subprime credit scores. The CFPB's initial discussions with industry stakeholders, other federal regulators, market analysts, and consumer advocates identified three areas where additional data visibility will be important: (1) lending channel differences (i.e., direct vs. indirect loans); (2) data granularity, consistency, and quality; and (3) loan performance trends.

The CFPB released its first findings from the pilot in 2024, which found that including negative equity in financing, particularly in relation to vehicle trade-ins, can increase the risk of a consumer's default on the financing.

Did You Know?

The CFPB found in 2024 that including negative equity in financing may increase the risk of consumer loan default.

In response to these findings, three consumer advocacy groups—the Consumer Federation of America, the National Consumer Law Center, and Americans for Financial Reform Education Fund—sent a letter to the CFPB showing their support of the pilot, encouraging the CFPB to release more information, and requesting that the CFPB expand the amount of data collected from the pilot. To learn more about the pilot and the CFPB's next steps, please see the link in the Additional Resources section of this Topic.

Note that despite the CFPB's activity in the indirect auto finance market, the consent decrees and other regulatory resolutions have not produced the CFPB's desired result of eliminating rate participation in the market generally. As a result, the CFPB continues to monitor rate participation and bring enforcement actions against perceived discriminatory lending. When coupled with training, monitoring for rate deviations, and taking remedial action as needed, this dealer participation practice better positions a dealer for responding to a fair lending inquiry.

Recommended Practices

1. Adopt a dealership-wide ECOA/Fair Lending policy and consider naming a senior officer to be in charge of the policy.

Recommended Practice

Adopt a dealership-wide ECOA/Fair Lending policy and consider naming a senior officer to be in charge of the policy.

The policy should clearly state the dealership's commitment to equal treatment and non-discrimination in all aspects of a credit transaction. Sales and F&I personnel who set prices or rates to consumers should be trained and tested regularly with respect to the policy. Monitor rate markups to ensure consistent application of the policy. Make the policy available to finance sources who send you communications about fair lending issues and be prepared to show the affirmative steps your dealership takes to make fair lending a priority.

2. Begin all negotiations with a set rate markup amount for credit transactions.

Recommended Practice

Begin all negotiations with a set rate markup amount for credit transactions to provide evidence of lack of discrimination.

Starting each customer with the same rate markup (and hopefully completing a large number of your deals at that figure or close to it)

will provide good evidence of the absence of discriminatory pricing. It is critical that you monitor rate markups for similarly qualified customers, and if you observe material differences that you speak with the dealership personnel involved and learn the reasons. Make redress to customers if appropriate. Document your final rate markup on each credit sale – be it the standard rate markup or a lower rate based on the pre-identified list of legitimate business reasons – in the deal jacket using something like the NADA Form. Include supporting documentation if you are deviating from the standard rate markup.

3. Develop and implement a Compliance Management System.

Recommended Practice

> A best practice is to delegate a senior level official or manager to oversee the development and implementation of the CMS, approved by senior management.

All dealerships should create and implement a compliance management system (CMS) that addresses the various issues addressed in this guide including, but not limited to: Privacy, Safeguards, Data Destruction, Red Flags, Fair Credit, Fair Lending, UDAP, Advertising and Marketing, Customer Complaints, Record Retention, and other subjects. All employees should be trained on the applicable laws, as well as the dealer's policy on each respective issue, such as its process for accepting and responding to consumer complaints. A best practice is to delegate a senior level official or manager to oversee the development and implementation of the CMS. The senior leadership of the dealership should approve of the CMS and be made aware of any compliance-related issues. A periodic audit of the CMS should be conducted at least annually in order to identify any potential issues or active violations, and the CMS should be updated to resolve those issues and violations. The senior leadership should also be involved in any corrective or remedial measures.

4. Review FTC, CFPB, and other industry guidance.

Recommended Practice

> Review FTC, CFPB, and other industry guidance to stay on top of regulatory changes.

We also recommend that the dealer delegate an employee or senior official or work with outside counsel to monitor federal and state laws applicable to the auto industry. This is a dynamic industry with ongoing regulatory changes at the federal and state level. Dealers minimize risks of violating changing regulations if they monitor those changes and update their CMS accordingly. This includes signing up for automated alerts with news aggregators and signing-up for newsletters from the CFPB and FTC using the links in the Additional Resources section below.

Additional Resources

CFPB, Consumer Financial Protection Circulars
https://www.consumerfinance.gov/compliance/circulars/

CFPB, Consumer Complaint Database
https://www.consumerfinance.gov/data-research/consumer-complaints/

CFPB, Negative Equity Findings from the Auto Finance Data Pilot (June 2024)
https://www.consumerfinance.gov/data-research/research-reports/data-spotlight-negative-equity-findings-from-the-auto-finance-data-pilot/

CFPB, 2023 Fair Lending Report of the CFPB (June 2023)
https://files.consumerfinance.gov/f/documents/cfpb_fair-lending-report_2023-06.pdf

CFPB, Our Auto Finance Data Pilot (February 2023)
https://www.consumerfinance.gov/about-us/blog/our-auto-finance-data-pilot/

CFPB, Compliance Management Review
Examination Procedures (August 2017)
https://www.consumerfinance.gov/compliance/supervision-examinations/compliance-management-review-examination-procedures/

CFPB, Compliance Bulletin and Policy Guidance
on Service Providers (October 2016)
https://www.consumerfinance.gov/compliance/supervisory-guidance/compliance-bulletin-and-policy-guidance-2016-02-service-providers/

CFPB, Compliance Management System Requirements (August 2013)
http://files.consumerfinance.gov/f/201308_cfpb_supervisory-highlights_august.pdf

Consumer Federation of America, Letter to CFPB Regarding
Enhancing Data in Auto Financing (August 2024)
https://consumerfed.org/wp-content/uploads/2024/08/Auto-Data-Letter-to-CFPB-8.5.24.pdf

FTC, Vendor Security
https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/vendor-security

NADA-NAMAD-AIADA, Fair Credit Compliance Policy and Program
https://www.nada.org/regulatory-compliance/nada-fair-credit-guidance

NADA-NAMAD-AIADA, Fair Credit Compliance
Policy and Program Certification Form
https://www.nada.org/media/4558/download?inline#page=22

Online Platforms and Sales

Online platforms provide dealers more opportunities to promote and sell their inventory to consumers however, the risk can be higher for misleading customers. Find out what policies and practices you should implement in relation to your web presence.

Learn what you need to know about promoting or selling cars online →

Did You Know?

Advertising a low price for a vehicle online but informing customers in person that only a higher price is available may subject you to UDAP enforcement actions from regulators and other liability. Learn more at Lawsuits & Enforcement

Compliance Tip

If you post a vehicle for sale online, ensure warranty information, a Buyer's Guide and other information required by law is provided in the same posting and is easy for customers visiting the post to access and review. See more Compliance Tips

Watch List for 2025

Regulators are increasing their review of dealers' online car sales for potential UDAP. For example, in 2024, the FTC obtained $1 million from a former online used car dealer for misleading consumers with promises of multiple inspections, fast delivery, and other information posted on the dealer's website that turned out to be inaccurate.

Recommended Practice

Make sure your terms of use, privacy policy, and electronic signatures policy are accessible on each page of your website and easy for a customer to notice through clear and conspicuous text.
See more Recommended Practices

Breakout Sections

Online Platforms and Sales

The online marketplace offers car dealers new and exciting opportunities for growth. But with these opportunities come additional challenges, compliance obligations, and risks. As such, you must be mindful of the ever-changing legal and data security landscape to ensure that your online practices do not lead to regulatory actions, governmental investigations, or consumer lawsuits.

As dealers continue to expand their operations online, the auto industry should expect increased attention from regulators and plaintiffs' attorneys. There are a few reasons for this heightened surveillance, including: (1) the rapid rise of online car sales; (2) the complex nature of car buying, which often requires financing and significant amounts of paperwork; and (3) the ample opportunities for consumer fraud, deception, and confusion in online sales.

As with traditional in-person car sales, online sales require the dealer to comply with various state and local regulations. When moving part of your sales efforts online, you must not violate federal, state, or local laws related to advertising, dealer inventory, product disclosures, financing, vehicle pick-up or delivery, vehicle service contracts, fees, or titling and registration.

This Topic addresses several issues relevant to online sales: (1) terms of use and privacy policies; (2) disclosures and advertising; (3) signature requirements; (4) ADA compliance; (5) jurisdiction; and (6) lawsuits and enforcement.

Terms of Use & Privacy Policies

Your Compliance Management System (CMS) addressed in Topic 12 should also include policies and procedures covering online sales. As noted in Topic 12, some of the necessary policies and procedures may already be in place. You may, however, need to review them with a lawyer to determine whether updates or revisions are necessary given your expansion into the online marketplace.

For example, a "terms of use" agreement sets forth the obligations and procedures governing the relationship between you and any consumer using your website or platform.

Did You Know?

A "terms of use" agreement can provide protection to dealers who may face claims from consumers about their websites.

Terms of use typically contain provisions delineating, among other things, the scope of services, data sharing, prohibited conduct, consent to contact the consumer, warranties, indemnification, and arbitration.

A privacy policy is another important document for dealers selling cars online.

Did You Know?

A "privacy policy" describes how the dealer collects, manages, uses, and discloses customer data provided online.

This policy discloses how a company collects, manages, uses, and discloses customer data. Common components of a privacy policy include:

- Types of Information Received or Collected (e.g., vehicle information, financials, address, social security number, IP address, etc.);
- When Information is Collected (e.g., online forms, automatically, recorded calls, etc.);
- Use of Information (e.g., credit checks, targeted advertising, legal purposes, etc.);
- Sharing Information with Third Parties (e.g., business partners, affiliates, vehicle inspectors, vehicle history providers, other service providers, government agencies, etc.);
- Internet-Based Advertising (e.g., targeted advertising based on consumers' interests);
- Ways to Limit Information Collection (e.g., opt-outs, unsubscribe, etc.);

- Accessing Consumers' Personal Information;
- Third-Party Links;
- Data Security;
- State-Specific Disclosures (e.g., California);
- Children's Policy (e.g., indicate that you do not target children with your websites or sales platform);
- Users Outside of the U.S.;
- Changes to the Privacy Policy (e.g., when and how changes are made); and
- Contact Information (e.g., specific email, address, phone number).

A best practice is to include a link to your terms of use and privacy policy on every page of your website. At minimum, these policies should be displayed on the homepage. And, as always, the terms of use, privacy policy, and other legal documents should not be created just to "check the box." Rather, you should strive to create policies that accurately reflect your obligations and procedures, and then ensure that such policies are implemented properly.

Disclosures & Advertising

The disclosure and advertising requirements addressed in other Topics are applicable to online sales. Many states also have specific requirements for online advertising. Accordingly, you should consult a knowledgeable attorney on how to minimize your risks when selling cars to customers online.

You should review your online disclosures and advertising periodically to ensure that they do not contain false, deceptive, or misleading information. This will require you to consider many factors as part of a "totality of the circumstances" approach.

- **Federal Disclosures.** There are specific disclosures required by various federal laws. For example, if you run a credit report on a consumer, the Fair Credit Reporting Act (FCRA) requires certain disclosures (e.g., pre-screen opt-out notice). Another example is the Truth in Lending Act (TILA), which requires certain disclosures for loan advertisements containing "triggering terms" (e.g., finance charge). You must operationalize these disclosures as part of your online sales process.
- **Buyer's Guide.** Be sure to post the FTC's Used Car Buyers Guide and comply with the Used-Car Rule (see Topic 7). While the FTC has not issued official guidance on how dealers should comply with the Used Car Rule when selling cars online, the FTC did mention in a 2022 article that a consumer is "entitled" to a Buyer's Guide "if [they] buy a used car online." **The FTC also stated in a recent complaint against a former online used car dealer that the dealer failed to "prominently and conspicuously display or properly complete a Buyer's Guide on used vehicles offered for sale to consumers on its website.**

Did You Know?

A Buyers Guide should be displayed and/or made available for each used car sold online.

- **Summaries.** You should consider providing a summary of terms and/or frequently asked questions (FAQs) related to program eligibility, the sales process, and vehicle financing. This would include information related to inventory, the online platform, credit applications, credit inquiries, financing terms, down payments, and monthly payments. Review your FAQs on a regular basis to make sure the information provided is still accurate.
- **Pre-Qualified.** If you include advertisements or banners regarding pre-qualified offers (e.g., "Get Pre-Qualified for an Auto Loan"), it should substantiate the pre-qualification amounts and any related rates. If you or the lender require consumers to meet other requirements, you should make clear to the consumer that the offer is not guaranteed if he or she does not meet additional underwriting criteria.

- **Testimonials/Endorsements.** As detailed in Topic 7, never use testimonials or endorsements that are fake, misleading, or make claims that you could not legally make. If reviews are posted of your products or services, ensure the reviews are not from you or your employees, which could be seen as a deceptive practice.

- **Links. Add a notice to alert consumers if they are leaving your website or platform by clicking a link you provided**

Recommended Practice

> Add a notice to alert consumers if they are leaving your website or platform by clicking a link you provided, ensuring they are aware of being redirected to an external site with potentially different privacy policies, security measures, and terms of service.

(e.g., "When you click this link, you will leave our platform and will go to a website that is not controlled by us. We provided this link for your convenience. We do not guarantee any products or services that are offered on other websites. Other websites may not reflect our same privacy policies and security procedures.").

- **APR.** If you advertise finance charges or other rates, then state them as an "Annual Percentage Rate," using that term.
- **Phrasing.** Avoid using phrases such as "lowest costs," "lowest rates," "quickest service," "easy payments," or "repayment in easy installments," which could be seen as potentially misleading to consumers who may not be eligible for such claims.
- **Other Representations.** Avoid making statements or representations with reference to the speed or ease of procuring a loan,to freedom from credit inquiries, or to any other implied differentiation in policy or loan service, unless you will comply with the representation made.
- **Transparency.** Disclose your relationship with lenders, relevant third parties, fees, and other terms and conditions.
- **Formatting.** As detailed in Topic 7, consider the prominence, presentation, placement, and proximity of disclosures on your website (i.e., make disclosures clear and conspicuous through text boxes, interactive text, and/or pop-outs).
- **Language.** If specific language is not required by federal or state law, consider using **disclosures** and disclaimers that are not overly verbose or complicated to make them easy for consumers to understand.

Compliance Tip

> Make sure to adapt the presentation and formatting of disclosures on mobile platforms to be easily viewable.

- **Apps/Mobile Website.** Confirm that the presentation and formatting of disclosures made available on a mobile platform have been appropriately adapted for that platform so consumers can fully view them.

Signature Requirements

When executing sales contracts, loan agreements, vehicle titles, or other legal documents, auto dealers must adhere to signature requirements. Given the unique nature of car sales, states may require certain hard-copy signatures or hard-copy documents. An attorney can help guide you through state laws and DMV regulations concerning signatures for sale, loan, and vehicle documents.

Also, as addressed in Topic 3, the E-Sign Act allows documents to be signed electronically where certain disclosure, consent, and other requirements are satisfied. These issues should be addressed in an electronic signatures and records policy posted on your website.

ADA Compliance

Website accessibility lawsuits have been on the rise for several years. These lawsuits are brought under the federal Americans with Disabilities Act (ADA) and generally allege that a company's website does not provide full and equal enjoyment for all consumers regardless of any disability they may have.

Unfortunately, courts are split regarding the ADA's application to websites.

Regulatory agencies have also struggled to provide binding and consistent guidance. **To minimize risk, many businesses have implemented the Website Content Accessibility Guidelines (WCAG), the universally accepted standards created by online accessibility experts.**

Compliance Tip

Consult the Website Content Accessibility Guidelines for methods of making your website more accessible.

To provide reasonable accessibility and avoid ADA website lawsuits, you should publish an accessibility statement on your website. Among other things, this statement would: (i) announce your commitment to providing an accessible website; (ii) indicate what standards have been implemented (e.g., WCAG); (iii) solicit feedback from website users and provide contact information for obtaining feedback; (iv) outline procedures for assessing consumer complaints and requests for accommodation; and (v) provide alternate means for users to obtain information (e.g., telephone support). A corresponding website accessibility policy will assist you in implementing this statement.

Jurisdiction

Online sales can create unique jurisdictional issues should a dispute arise with an out-of-state customer. As noted in Topic 3, when a dispute with an out-of-state customer arises, the customer will often attempt to sue the dealer in the customer's home state. The customer may claim that the dealer is not licensed in the home state and/or that the law of the home state should apply.

The types of online activity that are sufficient for a court to establish jurisdiction over a party continue to emerge. When faced with jurisdictional and "choice of law" issues for online sales, most courts examine several factors, including: (i) contractual provisions (e.g., governing law and venue provisions); (ii) the auto dealer's state of incorporation and principal place of business; (iii) the customer's state of residence; and (iv) the auto dealer's contacts with the forum state (e.g., targeted websites, state-specific advertising, communications sent into the state, sale and loan documents signed in the state, etc.).

By including governing law and choice of venue provisions in your contracts, you can improve the chances that your "choice of law" and/or "choice of venue" will control any dispute between you and an out-of-state customer. You can also include an arbitration clause in your contracts requiring customers to arbitrate their claims rather than litigate them in court. **As such, you should work with your attorney to review the governing law, venue, and arbitration provisions in your contracts.**

Compliance Tip

Address in your online policies whether claims involving your website must be arbitrated and must be resolved in a particular state.

Lawsuits & Enforcement

Online car retailers are increasingly facing lawsuits, enforcement actions, and complaints due to incorrect paperwork, title and registration delays, and other purchasing issues.

Watch List for 2025

Lawsuits and enforcement actions against online car dealers are on the rise. It is important to consult with your legal counsel regarding issues that are unique to online sales.

These lawsuits, enforcement actions, and complaints demonstrate the importance of prioritizing compliance and customer satisfaction in the online marketplace.

- **Arizona Enforcement Action.** In August 2024, an auto dealer group and its general manager agreed to pay $2.6 million to settle a lawsuit brought by the FTC and the State of Arizona alleging deceptive pricing in relation to its online advertisements, among other wrongful actions.

The dealers allegedly advertised low prices for their vehicles online and then informed consumers who visited the dealership that the advertised prices were no longer available.

Did You Know?

Advertising a low price for a vehicle online but informing customers in person that the price is not available may subject you to UDAP liability.

- **Texas Enforcement Action.** In July 2024, a former online used car dealer agreed to pay $1 million to settle a lawsuit brought by the FTC. **The lawsuit alleged that the online dealer failed to display warranty information near the cars posted on its website**,

Compliance Tip

Provide warranty information directly near a vehicle you post for sale online.

omitted a Buyer's Guide from display on cars, deprived customers of the option to cancel their car purchases and receive refunds, delayed delivery of purchased cars beyond an advertised delivery timeframe and advertised that the cars had passed "multiple inspections" when they had not. The FTC also required that the online dealer cease its deceptive advertising, document all claims about its promised shipping times, and follow all other applicable regulations the dealer was alleged to have violated.

- **Pennsylvania Class Action.** In May 2023, consumers filed a class action in Pennsylvania against an online car seller, alleging that the seller had delayed transferring vehicle titles to consumers who purchased vehicles from the seller, which led to the vehicles being repossessed after the seller stopped paying for the untitled and unregistered vehicles. The consumers also claimed that the seller's delay harmed its competitors by depriving them of vehicle sales when those competitors comply with title and registration laws when selling vehicles.
- **Multi-State Enforcement Action.** In December 2022, a used and online car seller and 36 State Attorney Generals announced that they had reached a $1 million settlement concerning non-disclosure of vehicle recalls. The Attorney Generals alleged that the seller had failed to disclose open safety recalls to consumers before the purchase of a vehicle. The seller was required to pay a monetary penalty, include hyperlinks for vehicles advertised online, provide QR codes for vehicles on the lot that link directly to any open recalls, and give consumers a disclosure of any open recalls on a vehicle to sign before the seller presents any other sales paperwork for the vehicle. The seller also agreed to stop representing vehicles as "safe."
- **North Carolina Class Action.** In November 2022, various used car dealers sued an online car seller in North Carolina for, among other things, advertising car sales in places where the seller was not actually located, failing to deliver titles, pushing hidden costs to consumers, and employing unlicensed salespeople. The seller eventually obtained dismissal of the case because the used car dealers had failed to state any legally cognizable claim.
- **Florida Administrative Complaints.** In June 2022, the Florida Department of Highway Safety and Motor Vehicles lodged an administrative complaint against a used and online car retailer for allegedly violating state law by failing to turn over titles and registrations to new buyers within 30 days. The complaint alleged that the retailer had failed to make timely transfers in at least 47 vehicle purchases.
- **Los Angeles Civil Lawsuit.** In August 2021, an online car seller agreed to pay $850,000 to various district attorney's offices in California to settle a civil lawsuit alleging that the company was operating in California without a dealer's or transporter's license. During the investigation, the district attorneys also learned that the seller violated California law by selling cars without providing inspection reports to consumers prior to sales.
- **Michigan Probation.** In October 2022, an online car seller was placed on 18-month probation by the Michigan Department of State for violating Michigan's vehicle registration laws, including improper use of temporary registrations, failure to have properly assigned certificate of title in immediate possession, improper odometer disclosures, and failure to properly maintain police books or washout systems.

- **Texas Citations & Fines.** In November 2021, a Texas news organization identified more than 30 citations and $10,000 in fines for an online car seller's violations of state registration laws between 2019 and 2021. Those violations included delaying transfer of vehicle title and registration to consumers, which left many consumers with expired temporary tags.
- **North Carolina Dealer License Issues.** In August 2021, an online car seller's dealer license in Wake County, North Carolina was revoked for 180 days for violations of dealer licensing laws, including failure to deliver titles to the DMV, selling a motor vehicle without a state inspection, and using out-of-state temporary tags/plates for a vehicle sold to a North Carolina resident.
- **BBB Alerts.** The Better Business Bureau (BBB) has issued an alert for an online car seller regarding its license suspension in Michigan described above. The BBB has also issued an alert for a different online car retailer given a national pattern of complaints since 2020 regarding (i) delivery of purchased vehicles that did not match the online photos; (ii) title and registration delays; (iii) warranty issues; (iv) misleading CARFAX reports; and (v) customer service problems.

Recommended Practices

1. **Develop and implement appropriate website policies that govern the use of your website.**

Recommended Practice

> Create and implement appropriate website policies to protect your dealership against claims relating to website and data use.

A terms of use, privacy policy, and electronic signatures policy should all be posted on your website. Make sure these policies address any potential complaints or formal disputes related to the use of information on your website, such as, if those complaints or disputes could only be resolved by arbitration. Your employees should fully understand and act in accordance with these policies. You should also routinely update your policies to conform with changes in the law and best practices.

2. **Perform periodic reviews of your website.**

Recommended Practice

> Perform periodic reviews of your website to ensure it provides fair and accurate information.

Your website must not contain false, deceptive, or misleading information, and its policies and information should be reasonably accessible to users. Periodic reviews of your website will help ensure that your products and services align with your disclosures and advertising. Make sure to apply Web Content Accessibility Guidelines to your website's design and content.

3. **Monitor lawsuit and enforcement trends in the online car sales industry. Lawsuits and enforcement actions disrupt normal business operations and are expensive.**

Recommended Practice

> Monitor lawsuit and enforcement trends in the online car sales industry to learn what practices to avoid.

By monitoring those issues plaguing others in the online car sales industry, you can improve your operations and limit the business and reputational risks that come with noncompliance.

4. **Keep your pricing consistent both in store and in advertisements.** Regulators have brought enforcement actions against dealers who promote a lower price in advertisements but then offer a higher price in store. Such practices may be considered by regulators to be a bait-and-switch UDAP that could subject the dealer to fines and other penalties.

Additional Resources

World Wide Web Consortium, Web Content Accessibility Guidelines 2.2 (October 2023)
https://www.w3.org/TR/WCAG22/

FTC, Buying a Used Car From a Dealer (August 2022)
https://consumer.ftc.gov/articles/buying-used-car-dealer

Penalties for Violation of Federal Consumer Credit Laws and Regulations

Note: The following is a quick reference to potential federal penalties for certain key tasks referenced in the Compliance Guide to be performed by your dealership. It is not intended as an exhaustive or official analysis of all penalties that may be assessed for a violation. You should consult your attorney with any questions you may have for your particular situation. Please also note that some of the penalties identified below are subject to periodic adjustment, and the amounts reflected below are indicative of a particular period in time only (**November 2024**) and may be subject to change.

Also note that most states have their own laws in connection with the federal laws outlined below, with additional penalties that may be imposed, as well as other causes of action that may be brought by consumers. You should consult your counsel for advice on the impact of state laws on your business practices.

Privacy Notices

Gramm-Leach-Bliley Act (GLB), Federal Trade Commission (FTC) Privacy Rule, and Fair Credit Reporting Act (FCRA)

- **The FTC enforces the Privacy Rule and GLB.** It may seek injunctive relief with potential for damages of up to $51,744 per violation if FTC enters into an enforcement decree. 16 C.F.R. § 1.98.
- **FCRA violations (FTC):** $4,857 for a knowing violation, which constitutes a pattern or practice of violations. 15 U.S.C. § 1681s(a)(2)(A); 16 C.F.R. § 1.98. Any violation of the FCRA also violates FTC Act § 5, with potential for damages of up to $51,744 per violation if FTC enters into an enforcement decree. 15 U.S.C. § 1681s(a)(1); 16 C.F.R. § 1.98.
- **FCRA violations (private right of action):** For negligent violations under private action, actual damages and the costs of the action together with reasonable attorney's fees. 15 U.S.C. § 1681o. For willful violations under private action, actual damages or statutory damages of not less than $100 and not more than $1,000 per violation; punitive damage liability with no cap; and costs of the action together with reasonable attorney's fees. 15 U.S.C. § 1681n.

Credit Application

Equal Credit Opportunity Act (ECOA), Regulation B, and FCRA

- **ECOA violations (FTC):** The FTC can enforce violation of ECOA as a violation of the FTC Act, with potential for damages of up to $51,744 per violation if the FTC enters into an enforcement decree. 15 U.S.C. § 1691c(c); 16 C.F.R. § 1.98.
- **ECOA violations (DOJ):** If unable to obtain compliance, the FTC may refer ECOA violations to the U.S. Department of Justice (DOJ). The DOJ may pursue a civil action if creditors are engaged in a pattern or practice of violations, and may obtain relief as appropriate, including actual and punitive damages and injunctive relief. 15 U.S.C. § 1691e(g)-(h).

- **ECOA violations (private right of action):** Individuals may seek recovery individually or as a class for actual damages. In addition, punitive damages are available but limited to $10,000, but in a class action total recovery must not exceed the lesser of $500,000 or 1% of the dealer's net worth. Equitable and declaratory relief are also available. Costs and reasonable attorney's fees also can be recovered by individuals or a class. 15 U.S.C. § 1691e; 12 C.F.R. § 202.16.
- **FCRA violations (FTC):** $4,857 for a knowing violation, which constitutes a pattern or practice of violations. 15 U.S.C. § 1681s(a)(2)(A); 16 C.F.R. § 1.98. Any violation of the FCRA also violates FTC Act § 5, with potential for damages of up to $51,744 per violation if FTC enters into an enforcement decree. 15 U.S.C. § 1681s(a)(1); 16 C.F.R. § 1.98.
- **FCRA violations (private right of action):** For negligent violations under private action, actual damages and the costs of the action together with reasonable attorney's fees. 15 U.S.C. § 1681o. For willful violations under private action, actual damages or statutory damages of not less than $100 and not more than $1,000 per violation; punitive damage liability with no cap; and costs of the action together with reasonable attorney's fees. 15 U.S.C. § 1681n.

Risk-Based Pricing Rule Notice

FCRA

- $4,857 for a knowing violation, which constitutes a pattern or practice of violations. 15 U.S.C. § 1681s(a)(2)(A); 16 C.F.R. § 1.98. Any violation of the FCRA also violates FTC Act § 5, with potential for damages of up to $51,744 per violation if FTC enters into an enforcement decree. 15 U.S.C. § 1681s(a)(1); 16 C.F.R. § 1.98. No private right of action. 15 U.S.C. § 1681m(h)(8).

Red Flags Rule

FCRA

- $4,857 for a knowing violation, which constitutes a pattern or practice of violations. 15 U.S.C. § 1681s(a)(2)(A); 16 C.F.R. § 1.98. Any violation of the FCRA also violates FTC Act § 5, with potential for damages of up to $51,744 per violation if FTC enters into an enforcement decree. 15 U.S.C. § 1681s(a)(1); 16 C.F.R. § 1.98. No private right of action. 15 U.S.C. § 1681m(h)(8).

OFAC SDN List Clearance

Trading With the Enemy Act (TWEA), International Emergency Economic Powers Act (IEEPA), Antiterrorism and Effective Death Penalty Act (AEDPA), Foreign Narcotics Kingpin Designation Act (FNKDA), Clean Diamond Trade Act (CDTA)

- Civil penalties per violation:
  - TWEA violations: Up to $108,489.
  - IEEPA violations: Up to the greater of $368,136 or twice the amount of the underlying transaction.
  - AEDPA violations: Up to the greater of $97,178 or twice the amount of which a financial institution was required to retain possession or control.
  - FNKDA violations: Up to $1,829,177.
  - CDTA violations: Up to $16,630.

  31 C.F.R. § 501, App. A.
- Criminal penalties:
  - **TWEA violations:** Fines up to $250,000 for individuals and $1,000,000 for organizations or twice the pecuniary gain or loss from the

violation and up to 20 years imprisonment. 31 C.F.R. § 501.701(b).

- **IEEP violations:** Imprisonment for not more than 20 years and a fine of not more than $1,000,000. 50 U.S.C. § 1705.
- **AEDPA violations:** Up to $500,000 per count against corporations, and up to 10 years imprisonment and $250,000 per count for individuals. 18 U.S.C. § 2332d; 18 U.S.C. § 3571; 31 C.F.R. § 596.701.
- **FNKDA violations:** Up to 10 years imprisonment and fine of not more than $10,000,000. 31 C.F.R. § 598.701.
- **CDTA violations:** Up to $50,000 and up to 10 years imprisonment. 19 U.S.C. § 3907.

Adverse Action Notices

ECOA (including Regulation B) and FCRA

- **ECOA violations (FTC):** The FTC can enforce violation of ECOA as a violation of the FTC Act, with potential for damages of up to $51,744 per violation if the FTC enters into an enforcement decree. 15 U.S.C. § 1691c(c); 16 C.F.R. § 1.98.
- **ECOA violations (DOJ):** If unable to obtain compliance, the FTC may refer ECOA violations to the U.S. Department of Justice (DOJ). The DOJ may pursue a civil action where creditors are engaged in a pattern or practice of violations, and obtain relief as appropriate, including actual and punitive damages and injunctive relief. 15 U.S.C. § 1691e(g)-(h).
- **ECOA violations (private right of action):** Individuals may seek recovery individually or as a class for actual damages. In addition, punitive damages are available but limited to $10,000, but in a class action total recovery must not exceed the lesser of $500,000 or 1% of the dealer's net worth. Equitable and declaratory relief are also available. Costs and reasonable attorney's fees also can be recovered by individuals or a class. 15 U.S.C. § 1691e; 12 C.F.R. § 202.16.
- **FCRA violations (FTC):** $4,857 for a knowing violation, which constitutes a pattern or practice of violations. 15 U.S.C. § 1681m(h)(8); 15 U.S.C. § 1681s; 16 C.F.R. § 1.98. Any violation also violates FTC Act § 5, with potential for damages of up to $51,744 per violation if FTC enters into an enforcement decree.
- **FCRA violations (private right of action):** Potential private right of action exists. For negligent violations, actual damages. For knowing violations, actual damages or statutory damages up to $4,857 per violation, and punitive damage liability with no cap. 15 U.S.C. § 1681s(a)(1); 16 C.F.R. § 1.98.

Credit Disclosures in RISC

Truth In Lending Act (TILA) and Regulation Z

- Regulator may adjust the account of the person to whom credit was extended so that such person is not required to pay a finance charge in excess of the charge disclosed, or the dollar equivalent of the annual percentage rate disclosed, whichever is lower. 15 U.S.C. § 1607(e).
- Private right of action (for certain violations):
  - Court costs.
  - Actual damages.
  - For individual actions, twice the amount of the finance charge.
  - For class actions, up to the lower of $1,000,000 or 1% of the creditor's net worth.

  15 U.S.C. § 1640(a).
- For willful and knowing violations, fine of up to $5,000, 1 year imprisonment, or both. 15 U.S.C. § 1611.
- Assignees are liable to the extent the violation is apparent on the face of the disclosure statement. 15 U.S.C. § 1641.

Table of Contents

Disclosures in Lease Agreement

Consumer Leasing Act (CLA) and Regulation M

- Regulator may adjust the account of the person to whom credit was extended so that such person is not required to pay a finance charge in excess of the charge disclosed, or the dollar equivalent of the annual percentage rate disclosed, whichever is lower. 15 U.S.C. § 1607(e).
- Private right of action:
    - Court costs.
    - Actual damages.
    - For individual actions, 25% of total monthly payments, with a minimum of $200 and maximum of $2,000.
    - For class actions, up to the lower of $1,000,000 or 1% of the creditor's net worth.

  15 U.S.C. § 1640(a).
- For willful and knowing violations, fine of $5,000, 1 year imprisonment, or both. 15 U.S.C. § 1611.
- Assignees are liable to the extent the violation is apparent on the face of the disclosure statement. 15 U.S.C. § 1641.

IRS Form 8300 Filing for Cash Deals

Internal Revenue Code

Effective for forms required to be filed on or after January 1, 2025:

- Generally, for negligent failure to timely file a complete and accurate Form 8300 or to furnish notice to persons on whom Form 8300s were filed, the penalty is $330 per return with an aggregate annual limit of $1,329,000 for persons with average annual gross receipts not exceeding $5 million and $3,987,000 for persons with average annual gross receipts exceeding $5 million. 26 U.S.C. § 6721; IRS Form 8300 Reference Guide.
- For intentional disregard of filing requirements, the penalty is the greater of (1) $33,220 or (2) the amount of cash received in the transaction not to exceed $132,500 per failure. For failure to furnish notice to persons on whom Form 8300s were filed due to intentional disregard, the penalty is $660 per failure or, if greater, 10% of the aggregate amounts of the items required to be reported. 26 U.S.C. § 6721; 26 U.S.C. § 6722; IRS Form 8300 Reference Guide.

Used Car Rule Buyers Notice

FTC Used Car Rule

- Up to $51,744 per violation. 16 C.F.R. § 455.1; 16 C.F.R. § 1.98.
- Possible state AG claims under UDAP and motor vehicle sales laws.
- Possible UDAP or fraud claims under state law.

Odometer Tampering

Federal Odometer Act

- The Department of Transportation can impose penalties of up to $13,300 per violation, subject to a $1,330,069 cap for a related series of violations. 49 C.F.R. § 578.6(f)(1).
- In a private party civil action where the violation involves the intent to defraud, liability is the greater of three times the actual damages or $13,300. 49 C.F.R. § 578.6(f)(2).

Telemarketing Restrictions

FTC Telemarketing Sales Rule (TSR) and Telephone Consumer Protection Act (TCPA)

- **TSR violations:** Up to $51,744 for each violation; redress to injured

Table of Contents

consumers; disgorgement of ill-gotten gains earned from the unlawful conduct. 16 C.F.R. § 310.3; 16 C.F.R. § 310.4; 16 C.F.R. § 1.98.

- **TSR violations:** For auto dealers who are subject to CFPB regulation, (1) violations that are not reckless or knowing are subject to per-day penalties of up to $7,034; (2) reckless violations are subject to penalties of up to $35,169 per day; (3) knowing violations are subject to penalties of up to $1,406,728 per day. 12 U.S.C. § 5565(a), (c); 12 C.F.R. § 1083.1.
- **TCPA violations (private action):** Up to $500 in statutory damages; up to $1,500 in statutory damages for willful or knowing violations. 47 U.S.C. § 227.
- **TCPA violations (regulator action):** Civil penalty up to $24,496 per violation or per day of continuing violation for violations of provisions other than Truth in Caller ID Act, subject to a cap of $183,718. 47 U.S.C. § 503; 47 C.F.R. § 1.80.
- **TCPA violations (civil forfeiture penalties for violations of the Truth in Caller ID Act):** $14,067 per violation, $42,200 per day for each day of continuing violation up to $1,406,728 for any single act or failure to act. 47 U.S.C. § 227(e); 47 C.F.R. § 1.80.
- **TCPA violations (criminal penalties):** A fine for willful and knowing violations of not more than $10,000 for each violation or $30,000 for each day of a continuing violation, or imprisonment of not more than 1 year or both; for repeat violations following an initial conviction, an individual could be fined not more than $10,000 or imprisoned not more than 2 years, or both. 47 U.S.C. § 227(e); 47 U.S.C. § 501.

Safeguarding Customer Information and Secure Disposal

GLB, FCRA, FTC Safeguards Rule, FTC Disposal Rule

- **GLB violations:** The FTC enforces the Safeguards Rule and the Disposal Rule. It may seek injunctive relief, with potential for damages of up to $51,744 per violation if FTC enters into an enforcement decree. 16 C.F.R. § 1.98
- **FCRA violations (FTC):** $4,857 for a knowing violation, which constitutes a pattern or practice of violations. 15 U.S.C. § 1681s(a)(2)(A); 16 C.F.R. § 1.98. Any violation of the FCRA also violates FTC Act § 5, with potential for damages of up to $51,744 per violation if FTC enters into an enforcement decree. 15 U.S.C. § 1681s(a)(1); 16 C.F.R. § 1.98.
- **FCRA violations (private right of action):** For negligent violations, actual damages and the costs of the action together with reasonable attorney's fees. 15 U.S.C. § 1681o. For willful violations, actual damages or statutory damages of not less than $100 and not more than $1,000 per violation, punitive damage liability with no cap, and costs of the action together with reasonable attorney's fees. 15 U.S.C. § 1681n.

Warranty Disclosures

Magnuson-Moss Warranty Act

- May constitute an FTC § 5 UDAP violation, with potential for damages of up to $51,744 per violation if FTC enters into an enforcement decree. 15 U.S.C. § 45(m)(1); 16 C.F.R. § 1.98.
- Consumer can recover actual damages, and remedies available under state law. 15 U.S.C. § 2310(d).

Unfair or Deceptive Practices (UDAPs)

FTC Act

- **FTC:** Up to $51,744 per violation. 15 U.S.C. § 45(m)(1); 16 C.F.R. § 1.98.

Unfair, Deceptive, Abusive Acts or Practices (UDAAP)

Consumer Financial Protection Act

- **CFPB:** Up to $1,406,728 per day for knowing violations against independent and buy-here-pay-here dealers for violations. 12 U.S.C. § 5531; 12 U.S.C. § 5565(c); 12 C.F.R. § 1083.1.

Combating Auto Retail Scams (CARS) Rule

FTC CARS Rule

- **FTC:** Up to $51,744 per violation. 12 U.S.C. § 5519(d); 15 U.S.C. § 45(m)(1); 16 C.F.R. § 463.1; 16 C.F.R. § 1.98.

Military Borrowers

Military Lending Act (MLA)

- Private right of action for actual damages of not less than $500 per violation, punitive damages, equitable or declaratory relief, reasonable attorney's fees, court costs, and any other relief provided by law. 10 U.S.C. § 987(f)(5).
- Violating contracts are void from inception. 10 U.S.C. § 987(f)(3).
- Arbitration agreements are unenforceable. 10 U.S.C. § 987(f)(4).
- Knowing violations are misdemeanors, punishable by fines starting at $5,000, up to 1 year imprisonment, or both. 10 U.S.C. § 987(f)(1); 18 U.S.C. § 3571.

Driver's Privacy Protection Act

Driver's Privacy Protection Act (DPPA)

- Private right of action for actual damages, but not less than liquidated damages in the amount of $2,500; punitive damages upon proof of reckless or willful disregard for the law; reasonable attorney's fees; and preliminary and equitable relief as the court deems appropriate. 18 U.S.C. § 2724(b).
- Criminal fines under federal law. 18 U.S.C. § 2723; 18 U.S.C. § 3571.

CFPB Small Dollar Rule

Short-term loans payable within 45 days; longer-term single-payment or installment loans with balloon payments; and installment loans with an annual percentage rate over 36% repayable with a leveraged payment mechanism

Relief may include:

- rescission or reformation of contracts;
- refund of moneys or return of real property;
- restitution;
- disgorgement or compensation for unjust enrichment;
- payment of damages or other monetary relief;
- public notification regarding the violation, including the costs of notification;
- limits on the activities or functions of the person; and
- civil money penalties of:
  - $7,034 per day that the violation continues.
  - If reckless violation, $35,169 per day that the violation continues.
  - If knowing violation, $1,406,728 per day that the violation continues.

12 U.S.C. § 5565(a), (c); 12 C.F.R. § 1083.1.

Glossary

A

Adverse Action

A decision on an application that is adverse or unfavorable to the interests of the consumer, including a refusal to grant credit in substantially the amount or on substantially the terms requested in a credit application unless the creditor makes a counteroffer and the consumer uses or accepts the credit offered in the counteroffer.

Also, the termination of, or unfavorable change to, an existing credit account or an action taken in connection with a credit application or an account that is adverse to the interests of the consumer. Unwinding or re-contracting a spot delivery deal can be an example of this "unfavorable change" type of adverse action.

Adverse Action Notice

Under the ECOA, any creditor "who in the ordinary course of business regularly participates in a credit decision, including setting the terms of credit," needs to notify a consumer in writing of adverse action taken on a credit application if it cannot offer financing to the consumer within 30 days after receiving the completed application. This includes an auto dealer that participates in the credit process such as by negotiating financing, rehashing, or marking up "buy rates."

Under the FCRA, an adverse action notice must be provided if the adverse action was based in whole or in part on information contained in a consumer report and must identify the credit bureau whose report was used. A FCRA adverse action notice must also include the customer's credit score used by the creditor and additional information, including up to four to five "key factors" that adversely affected the credit score if the credit score was used in taking the adverse action.

The ECOA and FCRA notices can be combined into one adverse action notice form that must include mandatory language from the ECOA, Regulation B, and the FCRA.

Affiliate

Any company that is related by common ownership or common corporate control with another company. A non-affiliate is any company that has no such common ownership or control.

Affiliate Marketing Rule

An FTC Rule published under the 2003 FACT Act that requires you to give a notice and opt-out rights to your customers if you share any customer information with your Affiliates such as sister dealerships, in-house insurance agencies, or a parent group. You must give the customer the right to opt out of your Affiliates using any shared information for marketing or solicitation purposes.

The notice need only be given once every five years, unlike a FCRA-GLB privacy notice that may need to be given once every year that the consumer remains a customer. It is a best practice to include the Affiliate Marketing Rule notice together with your dealership's privacy notice and to use a "safe harbor" FTC form of privacy notice to do so.

Appeal

A process by which a judgment issued by a court is submitted for review by a court of higher authority to decide whether the judgment should be approved, reversed, or remanded back to the lower court for further proceedings.

Arbitration

A process by which a dispute is decided by a private individual or panel of individuals under a set of agreed-upon rules instead of through a lawsuit. Arbitrators do not tend to strictly follow legal precedent in making their decisions. Grounds to appeal arbitration awards are very limited.

Table of Contents

B

Bait-and-Switch

A fraudulent marketing tactic in which a business advertises a particular product or low price to lure customers to the business with the goal of substituting them for a different product or higher price. Bait-and-switch tactics by auto dealers are prohibited by the CARS Act and are viewed as UDAP by federal and state regulators.

Balloon Payment

A final lump-sum payment due at the end of a finance contract or lease that is more than two times the amount of the regularly scheduled payment. The lump sum payment must be disclosed at the time of sale and financing.

Bank Secrecy Act

A federal anti-money laundering law that requires reporting to the Treasury Department of certain suspicious activity transactions and currency transactions in excess of $10,000 on IRS/FinCEN Form 8300. This form can be filed electronically. Dealers should also report to the Financial Crimes Enforcement Network (FinCEN) in the Treasury Department transactions that may involve money laundering of funds from illegal activity even if the total of such funds does not meet the $10,000 threshold.

Bring Your Own Device (BYOD)

“Bring Your Own Device”, a shorthand for employees using personal smartphones, tablets, and other remote devices for business purposes. If your dealership permits employees to combine business and personal use on non-dealership issued equipment of any type, you need to implement hardware and software protocols on the devices, restrict certain uses and permissions to safeguard customer information, and protect against unauthorized access to or use of the dealership’s and its customers’ information. BYOD policies should be addressed in your Safeguards and Data Destruction programs.

C

California Consumer Privacy Act (CCPA)

Enacted in 2018, the CCPPA creates new consumer rights concerning the access to deletion of and sharing of personal information that is collected by businesses. The rule creates unprecedented obligations for entities collecting and selling consumer data.

CAN-SPAM Act

A federal law that regulates sending of email messages. It requires the sender to include an opt-out provision with certain types of email communications (such as marketing or promotional messages), to be honored within 10 business days. The law also bans false or misleading header information, prohibits deceptive subject lines, requires commercial email to be identified as an advertisement, and requires the sender to include a valid physical postal address.

If a customer opts out of receiving email from you, you thereafter cannot sell, lease, exchange, or otherwise transfer or release that email address to any third party including through any transaction or transfer that contains the email address.

Car Buyer’s Bill of Rights

Consumer protection laws in certain states. These laws generally give consumers additional rights and may, among other things, require dealers in affected states to make additional written disclosures to consumers with respect to certain charges, aftermarket products, and providing standards for selling “certified” used vehicles.

Class Action

A legal process by which one person sues a defendant on behalf of a class of similarly situated persons for damages or other relief for all persons included within the class. A class action requires the class members to have received similar treatment from the defendant and be too numerous to include in an individual lawsuit. Class arbitration is a similar process before an arbitrator or panel of arbitrators instead of a judge.

Closed-End Lease

In a closed-end lease, the lessee is not obligated to buy the vehicle at end of term. However, some closed-end leases offer lessees a purchase option at the end of the lease term, either for a pre-specified amount or fair market value. Compare Open-End Lease.

Combating Auto Retail Scams (CARS) Rule

The FTC's Rule pursuant to the Dodd-Frank Act implementing its authority to regulate UDAP in the auto industry. The rule requires auto dealers to cease misrepresenting material information that would affect a consumer's choice to buy a car, disclose the offering price of the car separate from optional add-ons, avoid charging a consumer for add-on products that provide no benefit to the consumer, retain all records necessary to demonstrate compliance with the Rule for at least 24 months, and stop misrepresenting dealers' affiliations with military or government organizations, among other requirements. The Rule becomes effective September 30, 2025, subject to pending litigation that may delay or cancel the effective date.

Compliance Management System (CMS)

A system of policies, procedures, and operational practices that is designed to promote compliance with applicable laws and regulations. A CMS should be developed by a senior officer at a dealership and should be approved by the dealership's Board of Directors or, if it does not have a Board, its executive officers and dealer principals. The CMS should address employee training, consumer complaints, vendor management, and other topics.

Consent Decree/Consent Order

A formal settlement between a company and a regulator such as the FTC or CFPB in response to an actual or threatened regulatory administrative or enforcement proceeding. Most FTC consent orders subject the company to 20 years of regulatory oversight by the agency, require external reviews and certifications of its policies and conduct, and can impose fines or restitution penalties for conduct that the FTC deems to have violated applicable laws or regulations.

A consent order is often followed by civil lawsuits raising the same allegations that led to the consent order. Any violation of an FTC consent order is typically subject to a fine under Section 5 of the FTC Act. CFPB consent orders have generally required restitution to affected consumers along with penalties. CFPB consent orders have often required total payments, penalties, and customer remuneration well in excess of $100,000.

Consumer

An individual who initiates the process of seeking a financial product or service from your dealership to be used primarily for personal, family, or household purposes. For example, if someone applies for credit to finance a vehicle purchase for personal use at your dealership, he or she is a "consumer," even if credit is not extended to that individual.

Consumer Financial Protection Bureau (CFPB)

Formerly known as the Consumer Financial Protection Bureau or CFPB, an independent federal agency established by the 2010 Dodd-Frank Act to supervise certain institutions, enforce consumer protection regulations, and issue new regulations under many federal consumer protection laws (including TILA, ECOA, FCRA, and FDCPA). The Federal Reserve Board (the Fed) retains authority to issue statutory regulations under the consumer protection laws within the CFPB's jurisdiction to the extent they affect auto dealers. Dodd-Frank also authorizes the CFPB to publish rules and enforce violations constituting unfair, deceptive, or abusive trade practices.

The FTC may enforce conduct similar to the CFPB's authority under its unfair or deceptive practices authority under Section 5 of the FTC Act.

Consumer Leasing Act (CLA)

A part of the federal Truth in Lending Act that governs disclosures in consumer lease transactions. The authority for the Bureau of Consumer Financial Protection's and the Federal Reserve Board's Regulation M, this is one of the laws for which rulemaking authority (except with respect to franchised auto dealers) was transferred to the CFPB.

Consumer Reporting Agency (CRA)

Also known as a "credit bureau." Any person or entity which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

Cosigner

A person who agrees to be liable on a loan, lease, or credit sale if the borrower or co-borrower does not pay. Typically, the cosigner does not have an interest in the vehicle but is liable on the credit agreement. Dealers must give cosigners special notices under the FTC's Credit Practices Rule (as well as under certain state laws) at the time of cosigning.

Credit Discrimination

A practice by which members of one or more "protected classes" under ECOA (race, color, religion, national origin, sex, marital status, age, receipt of public assistance, or exercise of consumer credit rights) are denied credit or provided worse credit terms than other similarly qualified persons who are not in a protected class. Credit discrimination is generally proven by either a "disparate treatment" (knowing or intentionally discriminating) or a "disparate impact" or "effects test" in which a facially neutral practice (e.g., marking up buy rates) is statistically demonstrated to result in higher pricing to the members of the protected class. Knowledge or intent to discriminate is not required in a disparate impact case.

Credit Sale

A transaction in which a seller agrees to sell an item to a consumer for a set or variable price in a fixed number of installment payments over time, instead of requiring a cash payment in full up front. Most auto financing is done by a dealer making credit sales to consumers and then assigning its rights to collect the installment payments to a bank or financial institution. Also called closed-end credit. Sometimes referred to as a three-party credit transaction (dealer, financial institution, and consumer). Compare to Loan.

Credit Score

A numerical representation of a consumer's credit report intended to determine the non-payment risk that a consumer might pose to a potential creditor. The scoring algorithm takes into account many factors, such as credit history, recent credit inquiries, open credit lines, recent credit activity, and debt-to-income ratio. It also factors in whether a consumer pays bills on time or has outstanding or delinquent balances on existing credit accounts.

Credit scores are consumer reports within the meaning of the FCRA and need to be disclosed in adverse action notices if used in any way in making a credit decision.

Also, a credit score disclosure notice indicating a credit applicant's current credit score along with information about the date and provider of the score is one way to comply with the FTC's Risk-Based Pricing Rule.

Customer

A consumer who signs a credit or lease agreement, purchases an insurance product, or otherwise obtains a financial product or service from your dealership. A consumer who receives and accepts credit becomes a customer.

Customer Identification Program (CIP)

A Customer Identification Program prescribed by the USA Patriot Act by which a creditor establishes formal policies and procedures for verifying the identity of its customers and preventing money laundering. Auto dealers that act as agents for a bank (such as in originating two-party paper) are required to implement the bank's CIP.

D

Dealer Management System (DMS)

A management system used by dealership employees that consists of software that enables the dealer to efficiently manage all aspects of its operations.

Deferred Down Payment

A creditor may defer payment of all or a portion of the down payment in a transaction provided the deferred down payment is paid in full by the second scheduled installment payment and is not subject to any finance charges. However, check your lender agreement as it may contain a representation and warranty that you received the entire down payment for each assigned contract.

If you assign the contract with the down payment still owing, you will be in breach of that representation and warranty and may be required by the lender to repurchase the contract. Also known as "pick-up" payment.

Department of Justice (DOJ)

The federal executive department of the U.S. government, responsible for the enforcement of the law and administration of justice in the United States, which is headed by the Attorney General. The DOJ has authority to bring lawsuits against auto dealers for violations of most federal consumer credit laws and regulations.

Depreciation

Reduction in a vehicle's value due to age, mileage, and wear and tear. The "Residual Value" is the predicted value of the vehicle at the end of a lease term established at the beginning of the lease assuming normal wear and tear.

Disparate Impact Credit Discrimination

A claim for credit discrimination under ECOA that does not require any knowledge or intent to discriminate on the part of the dealer. Also referred to as the "effects test." There are three parts to the analysis:

Under a disparate impact analysis, a neutral business practice (such as marking up a lender's buy rate) is examined to determine if application of the practice has a disproportionately negative effect on a protected class of persons under ECOA, these being: (1) race, color, religion, national origin, sex, marital status, or age (provided the applicant has the capacity to contract); (2) because all or part of the applicant's income derives from any public assistance program; or (3) because the applicant has in good faith exercised any right under the federal Consumer Credit Protection Act.

If so, the burden then shifts to the creditor to show the practice meets in a significant way, the legitimate goals of the business. There is no requirement that the challenged practice be essential or indispensable, only significant and non-discriminatory.

If so, the burden then shifts to the regulator to show that the business goals can be met by means that are less disparate in their impact. If the regulator cannot show this, then there is no disparate impact credit discrimination because a significant, non-discriminatory business reason is the cause of the rate differential.

The Dodd-Frank Act

The Dodd-Frank Wall Street Reform and Consumer Protection Act, the comprehensive banking reform and consumer protection law passed by

the Congress and signed by President Obama on July 21, 2010. The Act reforms many aspects of bank regulation and authority and establishes the CFPB as the agency in the Federal Reserve Board to protect consumers, re-write regulations under many consumer protection acts, and enforce violations concurrently with the DOJ, FTC, and state Attorneys General. The Dodd-Frank Act also streamlines the process for the FTC to promulgate rules relating to unfair and deceptive practices by auto dealers.

Drivers Privacy Protection Act (DPPA)

A law prohibiting disclosure by state Departments of Motor Vehicles (DMVs) or other authorized persons of personal information consisting of that which identifies an individual, including an individual's photograph, Social Security number, driver identification number, name, address (but not the five-digit zip code), telephone number, and medical or disability information from DMV records or otherwise without the individual's prior written consent. Exceptions exist to verify or correct information about the individual and for certain motor vehicle safety or theft situations. Resale or redisclosure of the information by a recipient is highly limited. Penalties include potential criminal liability and a private cause of action for actual damages plus punitive damages, attorney's fees, and equitable relief.

E

Enforcement Action

A court proceeding initiated by an agency or other governmental body against a person or entity to enforce laws or regulations. For example, the FTC, CFPB, and State Attorneys General regularly bring enforcement actions against auto dealers and auto lenders for violation of laws and regulations prohibiting unfair or deceptive acts or practices.

Equal Credit Opportunity Act (ECOA)

As implemented by the Consumer Financial Protection Bureau's and the Federal Reserve Bureau's Regulation B, ECOA prohibits discrimination in all aspects of a credit transaction on the basis of race, color, religion, national origin, sex, marital status, age, the fact that all or part of an applicant's income is derived from any public assistance program, or the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act ("protected classes"). On March 21, 2021, the CFPB issued an interpretive rule clarifying that sexual orientation and gender identity discrimination are also prohibited under the Equal Credit Opportunity Act (ECOA) and Regulation B, as both involve the consideration of sex. ECOA also requires creditors to send credit decisions and any adverse action notices to consumers. Rulemaking authority for ECOA was transferred from the Federal Reserve Board to the CFPB as of July 21, 2011 for all creditors except franchised auto dealers. The Federal Reserve Board retains ECOA rulemaking authority as it pertains to franchised auto dealers.

E-SIGN Act

A federal law that permits electronic signatures to substitute for paper signatures in most consumer and commercial transactions. It enables electronic contracting of motor vehicle retail installment sales and leases, and it requires consent disclosures to the consumer and communications indicating a "reasonable demonstration" of a consumer's ability to receive electronic communications along with their electronically communicated consent to conduct business electronically in consumer transactions such as auto finance.

F

FACT Act

The Fair and Accurate Credit Transactions Act. A 2003 federal law that amended the FCRA and provided consumers with certain additional credit report disclosure rights and identity theft protections. Through the FACT Act amendments, the FCRA restricts affiliate use of shared information for marketing or solicitation purposes; requires notices of credit score information under the Risk-Based Pricing Rule; provides new identity

theft protections by requiring dealers to implement a written Identity Theft Prevention Program under the Red Flags Rule; gives consumers the right to access their credit reports once per year from each national consumer reporting agency (Equifax, Experian, and TransUnion) for free; expands consumer rights to dispute items in credit files; and requires detailed consumer notices on credit applications and credit reports, among other things. Also requires credit and debit card electronic receipts to truncate all but the last five card numbers and not print the card expiration date.

Fair Credit Reporting Act (FCRA)

The FCRA governs the permissible uses of credit reports and requires disclosures to consumers when a credit report is used in making an adverse credit decision. It also requires giving consumers opt-out rights with respect to sharing of consumer report information with affiliates or the use of shared information by affiliates for marketing or solicitation purposes. The FCRA contains requirements for credit bureaus and reporting creditors to make credit reports more accurate, to correct inaccurate reporting, and to not report or re-report erroneous items. It enables prescreening unless the consumer has opted out of all credit bureau prescreening. In addition, the FCRA is the law pursuant to which the Red Flags Rule, Risk-Based Pricing Rule, and the Disposal Rule were issued.

Federal Communications Commission (FCC)

A federal agency that regulates and enforces consumer communications laws, including the TCPA. The FCC regulates telemarketing, which includes calls, text messages, and other marketing communications, from businesses to consumers, including telemarketing from auto dealers to their customers. The FCC primarily does this through implementing regulations and guidance relating to the TCPA and enforcing the TCPA's do-not-call list, prior express written consent, and other requirements.

Federal Odometer Law

A federal law that prohibits the manipulation of odometer devices and mileage readings on them. It requires a person transferring ownership of a vehicle to give to the person obtaining ownership a written disclosure of the odometer's mileage reading. If the transferor knows the odometer reading is incorrect or inaccurate, he must state in the disclosure that the actual mileage is unknown. For used cars, the odometer disclosure typically is made on the vehicle's title. The law also prohibits persons from tampering with an odometer. Dealers are required to retain written odometer disclosures for five years. The federal Department of Transportation issues regulations implementing the requirements of the law.

Federal Trade Commission (FTC)

A federal agency that regulates and enforces consumer credit and privacy laws, among other duties. The FTC is the regulator for franchised auto dealers on consumer protection, privacy and data safeguards, and identity theft prevention as well as other consumer protection laws and regulations. The FTC is authorized to supervise franchised auto dealers and bring enforcement actions for violation of federal consumer protection laws and regulations including under its general authority in Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices. The Dodd-Frank Act streamlined the process for the FTC to issue new regulations concerning unfair and deceptive practices by auto dealers.

G

Global Positioning System (GPS)

GPS is a technology that provides location and time coordinates to a satellite to signal the location of an individual vehicle, or any other item equipped with GPS-supported technology. Utilizing GPS technology in a vehicle allows a creditor to identify the location of a vehicle serving as its collateral and assists the creditor in physically recovering or repossessing the vehicle upon default or theft by locating the vehicle without having to conduct a costly search.

Gramm-Leach-Bliley Act (GLB)

A federal law requiring auto dealers, creditors, and other "financial institutions" to protect and safeguard the privacy of customers' nonpublic personal information and not share such information with third parties unless the customer is given notice and the opportunity to opt out of sharing the information. GLB also requires giving a consumer a privacy notice describing the dealer's information collection, use, and sharing practices when a customer first provides personal information and annually thereafter if the person is still a credit customer. Consumers who do not become customers must be given a privacy notice before you begin sharing their information. The FTC regulates auto dealers' compliance with GLB and has published its Privacy Rule and Safeguards Rule to implement the GLB requirements. The Safeguards Rule mandates using administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information in its gathering, retention, and disposal, in both electronic and paper form.

Gross Capitalized Cost

The total selling price of the leased vehicle including negotiated selling price plus optional equipment such as GAP coverage and anti-theft devices. Also referred to as "cap cost."

Guaranteed Auto Protection (GAP)

GAP is optional consumer protection that covers the difference between what the car is worth and what the customer owes on the car. It comes into play if the car is stolen or totaled (damaged to the point that repair would cost more than the car is worth) while the owner is still making payments. Whether or not GAP is insurance and requires an insurance license to be sold is determined by state law. In New York, for example, a dealer can sell the consumer a "GAP waiver" that is not insurance and covers a total loss due to theft or casualty. In so doing, the dealer must disclaim the right to claim against the consumer for the GAP amount and is limited to selling the GAP waiver for the insurance cost to the dealer of obtaining the GAP insurance for itself.

I

Identity Theft Prevention Program (ITPP)

See Red Flags Rule.

Identity Theft or Identity Fraud

Under federal criminal law, identity theft takes place when someone knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or in connection with, any unlawful activity such as fraud. Under this definition, a name or Social Security number is considered a "means of identification." So is a credit card number, mobile telephone number, electronic serial number, or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual. Unlike traditional identity theft, where someone steals and misuses a person's actual identity, a perpetrator of Synthetic Identity Fraud (SIF) starts with a single piece of legitimate personal data (e.g., social security number) and builds a fake identity around it using false information such as an address or phone number.

Information Security Program

The administrative, technical, and physical safeguards you use to access, collect, distribute, process, protect, secure, store, use, transmit, or otherwise handle nonpublic personal information of consumers and customers. This Program must also contain provisions dealing with how you will respond in the event of a security breach. The term also refers to written documents and procedures evidencing these safeguards. Also called a Safeguards Program.

Inquiry

A request to a consumer reporting agency for a credit report. Only persons having a "permissible purpose" under the FCRA or consumers requesting their own credit report may obtain a credit report in response

to an inquiry. Inquiries, other than consumer inquiries of their own credit report, appear on the consumer file, are reported in subsequent credit reports, and are used as factors in credit scoring algorithms.

IRS/FinCEN Form 8300

A form required to be filed with the IRS within 15 days of completing a cash sale or multiple cash sales in related transactions (generally multiple transactions within 24 hours or which you know or should know are connected) for which the customer paid cash or cash equivalents (cashier's checks, travelers checks, bank drafts, and money orders, if they have face amounts of $10,000 or less, but not a personal check or the proceeds of a bank auto finance loan) totaling in excess of $10,000. The Form 8300 can be filed electronically and is required to be filed electronically for certain filers. Regulations require informing a customer on whom you filed a Form 8300 that you did so by January 31 of the following calendar year. Keep a copy of all filed Forms 8300 for five years.

J

Junk Fax Prevention Act of 2005

A federal law that prohibits sending unsolicited facsimile advertisements to persons unless the person consents in writing to receive fax advertisements or the sender has a "prior business relationship" with the recipient and the recipient has not opted out of receiving faxes from the sender. Senders of unsolicited faxes must include a clear and conspicuous notice on the first page on how the recipient can opt out of future faxes from the sender at no cost. Persons who opt out must be removed from all fax lists within 30 days.

L

Loan

In contrast to a credit sale, a transaction in which a bank or financial institution directly lends a consumer money and the consumer agrees to pay the loan back with interest over time. Sometimes referred to as a two-party credit transaction (financial institution and consumer). Dealers may act as agents for financial institutions in originating two-party loans for consumers. Compare Credit Sale.

M

Magnuson Moss Warranty Act (MMWA)

A federal law that governs written warranties in connection with the sale of consumer products including automobiles. The Act requires disclosures concerning express and implied warranties and restricts disclaimers of implied warranties if a dealer offers a written warranty or sells a service contract within 90 days of the vehicle sale. The law contains mandatory disclosure language for warranties, including what vehicle systems are covered, which ones are not, the duration of the warranty, how a customer gets warranty service, and what obligations the customer has as a condition to warranty service. This law also prohibits certain acts and provides consumers with remedies for breaches of warranties including the ability to bring class actions and recover damages and attorney's fees. Pursuant to the E-Warranty Act, which became law in 2015, and the FTC's rules issued in 2016, warrantors and sellers can opt to provide warranty disclosures electronically if they comply with certain requirements.

Mediation

A process by which an individual selected by the parties facilitates negotiations between the parties to guide them toward a mutual resolution. Rather than issue binding decisions, mediators assist parties with agreeing on terms of a binding settlement agreement. The agreement may later be enforced in court.

Menu Selling

A process by which each customer who has agreed to purchase or lease

a vehicle is presented with a document indicating each optional aftermarket item available from the dealership along with its price and its effect on the customer's monthly payment. A menu should disclose groupings of aftermarket offerings (e.g., Platinum Package, Gold Package, Silver Package) the same way. The customer initials an acceptance or decline for each product.

Metadata

Data behind data in electronic documents, such as emails and Microsoft Office documents. Properties of electronic documents can reveal who created the document, when it was created, accessed, and who it was distributed to, plus changes made along the way. Additional metadata can be gleaned from computer systems forensics analyses. Metadata can be valuable in litigation and is the reason why most electronic discovery requests seek electronic documents to be produced in their native (original) form, as opposed to a printed or electronic image format (e.g., .pdf or .tif format).

Military Lending Act

A federal law that imposes limitations on the cost and terms of certain extensions of credit to service members and their dependents. 10 U.S.C. § 987; 32 C.F.R. Part 232. The Military Lending Act does not apply to credit that is expressly intended to finance the purchase of a motor vehicle when the credit is secured by the vehicle being purchased. In December 2017, the Department of Defense released guidance clarifying that whether a transaction qualifies for this purchase-money exception depends upon what the credit beyond the purchase price of the motor vehicle is used to finance. More specifically, "financing costs related to the object securing the credit will not disqualify the transaction from the exceptions, but financing credit related costs will disqualify the transaction from the exceptions." The Department of Defense did not define the term "credit-related cost," but provided two examples: GAP insurance and credit insurance. The CFPB has established an Office of Servicemember Affairs to educate service members about credit and to coordinate complaints by and responses to service members and their families about consumer credit, including auto finance credit.

N

National Do Not Call Registry

An FTC list of telephone numbers populated by consumers who have indicated their desire not to receive telemarketing calls. States also maintain do-not-call registries and your dealership should maintain (and honor) an internal do-not-call list of persons who have asked that the dealership not call them. Exclude all such persons from telemarketing lists.

Negative Equity

A term used to describe a consumer whose trade-in vehicle is worth less than their credit pay-off balance for the car. Negative equity can be paid off and financed in a vehicle purchase or lease transaction. However, TILA requires negative equity to be disclosed either by reducing the consumer's down payment (but not below $0) or itemizing the amount of negative equity separately in the Amount Financed list of Amounts Paid to Third Parties. Negative equity should never be added to increase the cash price of the vehicle, and dealers who do so may be subject to class action liability. Also called "upside down" or "under water."

Nonpublic Personal Information (NPI)

Personally identifiable financial information provided by a consumer to a dealer or otherwise obtained by the dealer and any list or grouping of consumers derived from any personally identifiable financial information that is not publicly available. This includes any information a consumer provides on a credit application, or any information derived from a consumer report or credit transaction. It also includes lists of credit customers or even the fact of a customer being a credit customer. Information you collect through a "cookie" in connection with an inquiry about a financial product or service can also be nonpublic personal information. The

term does not include anonymized and aggregated information that does not contain personal identifiers such as names, addresses, Social Security numbers, driver's license numbers, or account numbers.

Notification Events

Events in which unencrypted customer information involving 500 or more consumers is acquired without authorization. When such events occur, the FTC requires the person or entity from whom the information was acquired to report the event as soon as possible and no later than 30 days after discovery of the event. This notification requirement is part of the FTC's Safeguards Rule.

O

Office of Foreign Asset Controls (OFAC)

An agency of the United States Department of the Treasury under the auspices of the Under Secretary of the Treasury for Terrorism and Financial Intelligence. OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign states, organizations, and individuals. Among other things, OFAC publishes the SDN List which is a frequently updated list of persons with ties to blocked countries or persons with whom you cannot do any business per the USA Patriot Act. See SDN List.

One-to-One Consent Rule

The FCC's rule interpreting the TCPA's definition of "prior express written consent" to mean "an agreement, in writing, that bears the signature of the person called or texted that clearly and conspicuously authorizes no more than one identified seller to deliver or cause to be delivered to the person called or texted advertisements or telemarketing messages using an automatic telephone dialing system or an artificial or prerecorded voice." The rule also requires that "[c]alls and texts must be logically and topically associated with the interaction that prompted the consent and the agreement must identify the telephone number to which the signatory authorizes such advertisements or telemarketing messages to be delivered." The rule becomes effective on January 27, 2025.

Open-End Lease

In contrast to a closed-end lease, a lease that obligates the lessee customer to purchase or arrange for the sale of the vehicle at the end of the lease term.

Opt Out

The right of a consumer under GLB and the FCRA to remove themselves from information sharing with third parties and certain information sharing and all information usage by Affiliates of a dealer. Whenever a consumer has a right of optout (e.g., Affiliate Marketing Rule, sharing credit information with Affiliates, sharing any information with a third party), a dealer must wait 30 days from the day it delivered its privacy notice informing the consumer of their opt-out rights before sharing the consumer's information and only then provided the consumer does not opt out within the 30 days. This is true even if the consumer does not choose to opt out during the 30 days. The only exception to the requirement to wait 30 days before using or sharing the customer's information is for service providers involved in the customer transaction or joint marketing agreements with other financial institutions to market a financial product or service, provided these are disclosed to the customer in the privacy notice. Whenever a consumer opts out of any information sharing or Affiliate marketing, it is a best practice to opt them out of all databases that are shared with Affiliates or third parties. A "safe harbor" model privacy notice has been published by the FTC.

P

Payday, Vehicle Title, and Certain High-Cost Installment Loans Rule

A federal rule that imposes limits on (i) short-term loans payable within 45 days; (ii) longer-term single-payment or installment loans with

balloon payments; and (iii) installment loans with an annual percentage rate over 36% repayable with a leveraged payment mechanism. The Final Rule includes an express exclusion for "certain purchase money security loans," which it defines as "[c]redit extended for the sole and express purpose of financing a consumer's initial purchase of a good when the credit is secured by the property being purchased, whether or not the security interest is perfected or recorded."

Payment Card Industry Data Security Standard (PCI-DSS)

Applicable to merchants such as auto dealers who accept credit or debit cards for payment. PCI-DSS includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures to protect customer credit and debit card account data. Among other things, merchants are prohibited from storing information contained on the magnetic stripe of cards or the three-digit CVC/CVV code imprinted on the signature panel of cards or debit card PINs or access codes. Card information must be captured and transmitted over encrypted media, and terminals must print only the last five digits of a card number and cannot print the card expiration date. Merchants who violate PCI-DSS are subject to penalties from the card associations and networks and may incur civil liability as well. Nevada has also made compliance with PCI-DSS a requirement of Nevada law. Nevada has essentially adopted the PCI-DSS as its legal standard for card security.

Permissible Purpose

According to the FCRA, a dealer must have a "permissible purpose" to pull a customer's credit report. A customer's written consent is always the best permissible purpose. However, the FCRA lists several other conditions for permissible purpose without the customer's written consent (although certain states like Vermont require a written consent in all cases). Otherwise, subject to its contract with a consumer reporting agency, a dealer can pull the credit report without the customer's written consent only if it is clear to both the customer and the dealer that the customer is initiating the financing or lease of a vehicle and the dealer has a legitimate business need for the credit report, such as to arrange financing requested by the consumer. However, a customer merely walking into a showroom does not give the dealer a permissible purpose to pull the customer's credit report.

Phishing

Social engineering techniques used in cyberattacks by identity thieves to "fish" for personal information on the internet. Generally done by creating fake emails and websites that appear legitimate but are designed to attempt to get users to disclose their personal information or click on a web link which puts a keylogger virus or other malware on their PC that tracks their keystrokes on banking or other websites to gain personal and login information. "Vishing," or voice phishing, involves using phone calls or voice messages to get the consumer to reveal personal information. "Smishing," or SMS phishing, involves the use of text messages to induce the consumer to reveal personal information or go to websites that will download a virus onto their mobile device. "Spear phishing" is a type of phishing message directed to targeted company executives and directors that may indicate the desire to purchase or partner with the company and include an attachment such as a claimed Non-Disclosure Agreement to initiate discussions.

Preemption

A doctrine by which certain federal laws such as the Federal Arbitration Act, TILA, ECOA, and FCRA preempt and override inconsistent state laws on the same subject. Also, a doctrine created by courts construing the National Bank Act for federally regulated financial institutions to do business uniformly in all states by using their home state law to preempt certain other states' laws. The 2010 Dodd-Frank Act limited preemption of state consumer protection laws to banks and not their subsidiary or affiliated corporations and only when application of the state law would discriminate against the national bank or prevent or significantly interfere with the national bank's exercise of its powers, such determination to be made on a case-by-case basis by the Office of Comptroller of the Currency. Certain other federal laws also expressly preempt state laws.

Privacy Notice (FCRA-GLB Privacy Notice)

An initial or annual notice concerning your collection and sharing of personal information that is required to be given to your consumers and customers under GLB and the FTC Privacy Rule. The FCRA also requires notices that give the consumer the right to opt out of Affiliate sharing of credit information, and its Affiliate Marketing Rule requires a notice that gives consumers the right to opt out of Affiliates using any shared information for marketing or solicitation purposes. The required privacy notices are typically combined into one FCRA-GLB Privacy Notice, although the Affiliate Marketing privacy notice can be given separately. Model privacy notice forms have been issued by the FTC, and use of one of these forms is intended to provide a "safe harbor" from liability. Of course, a dealer's practices of collecting and sharing consumer information must comply with what is disclosed in its privacy notice.

Privacy Rule

The FTC's rule pursuant to the GLBA that implements the GLBA's privacy provisions. The rule enables businesses to give one privacy notice to a consumer to cover the GLBA and the FCRA privacy requirements and opt-out provisions, as well as the Affiliate Marketing Rule notice requirements. The rule also requires that if a business maintains a credit relationship with a customer (e.g., a buy-here-pay-here auto dealer), the business must give another privacy notice to the customer annually during the term of their credit relationship.

Privacy Policy

A disclaimer from a website owner to a user describing how the website owner collects, manages, uses, and discloses user data. Common components of a privacy policy include types of information received or collected, use of information, data security, third-party links, and other information. The policy should be displayed on the website and easily accessible to the user.

Puffery

A seller's exaggerated expression of its subjective opinion about the merits of a product, as opposed to a factual description of a characteristic of a product. One court described puffery as "exaggerated advertising, blustering, and boasting upon which no reasonable buyer would rely." A factual statement about a vehicle is not likely to be considered puffery. Puffery is a subjective, fanciful boast or some vague generality about how wonderful a vehicle is as opposed to a factual representation about the vehicle. Puffery is generally not legally actionable whereas factual representations, if material and relied upon by the customer, can be legally actionable as misrepresentations or deceptive trade practices. Puffery does not include misrepresentations or claiming benefits vehicles do not possess or any statement made for the purpose of deceiving prospective purchasers.

R

Rebate Stacking

A deceptive advertising practice in which a dealer prices a vehicle after applying a series of rebates that few, if any, customers will qualify for. An example is pricing a vehicle and indicating a reduction for "rebates" where the rebates include recent college grad, military, returning lessee, loyalty, and perhaps other rebates for which few, if any, consumers can meet all of the qualifications. Itemize rebates and do not reduce the purchase price in advertising except for rebates that are available to substantially all of your customers.

Red Flags

Any pattern, practice, or specific activity that indicates the possible existence of identity theft at your dealership. The FTC's Red Flags Rule identifies 26 potential red flags, including consumer report fraud alerts, credit freeze notices, unusual credit activity, inconsistent information provided in comparison to ID cards, and more.

Red Flags Rule

Required by the FCRA and implemented via the FTC's rulemaking authority, auto dealers must develop and implement a written Identity Theft Prevention Program (ITPP) designed to detect, prevent, and mitigate identity theft in connection with establishing or maintaining consumer credit accounts and business accounts that present identity theft risks. The Red Flags Rule is not a "one size fits all" rule. Your ITPP must be appropriate to the size and complexity of the dealership and the nature and scope of its activities. The plan must identify relevant red flags; develop procedures to detect the presence of any red flags in credit transactions; prescribe ways to respond appropriately to any red flags that are detected; and be periodically updated to address new risks and experiences with identity theft. The dealership's Board of Directors must approve the dealership's initial ITPP and designate a senior dealership officer to develop, oversee, implement, and administer the ITPP. The Rule also requires oversight of service providers, annual reporting to the Board or senior management, and training of all employees who participate in the ITPP. The FTC revised its Guide to the Red Flags Rule to emphasize the need for annual review and oversight by the Board or senior management and to make appropriate changes based on experiences with attempted identity theft or new insights gleaned from studies and other materials. The FTC has identified Red Flags as a priority area.

Reseller

A consumer reporting agency that assembles and merges information contained in the database of another consumer reporting agency or multiple consumer reporting agencies and does not itself maintain a database of the assembled or merged information from which new consumer reports are produced.

Retail Installment Sales Contract (RISC)

The document that a dealer signs with a consumer to sell and finance the sale of a vehicle under the time-price doctrine. Compare "Credit Sale" with "Loan." The dealer will then sell the RISC and the consumer's obligations to make payments under the RISC to a bank or finance company except for buy-here-pay-here dealers who hold RISCs and collect payments from buyers directly. Requirements for RISCs are set forth in state motor vehicle retail installment sales acts as well as in the federal Truth in Lending Act (TILA).

S

Safeguards Rule

The FTC's rule pursuant to GLB that requires dealers to develop and implement a comprehensive written Information Security Program to secure, safeguard, and protect nonpublic personal information (NPI) on consumers and customers in all forms of media. The Safeguards Rule requires a dealer to designate a named individual as the Program Manager responsible for implementing and managing the program including ongoing training and monitoring of employees on the need to protect customer information. A Safeguards Program must include a security incident and breach incident response plan and address all prospective threats to the security of nonpublic personal information maintained by the dealership. The Information Security Program must be periodically updated to address new security threats and regulatory guidelines.

SDN List

Specially Designated Nationals and Blocked Persons List maintained by OFAC. OFAC's list contains persons, countries, and organizations with which U.S. entities are prohibited from doing any business. Every customer – cash and credit – must be checked against the SDN List at the time the customer relationship is established. If there is a definitive match, you must call OFAC and cannot do business with the individual or entity until the hit is cleared. OFAC updates the SDN List as often as several times a month and publishes it on its website. Penalties for noncompliance are substantial and can range in the millions and result in imprisonment.

Security Freeze

A consumer's right to prohibit their credit file, including their credit report and credit score, from being accessed by new creditors. Although state laws may vary, consumers may freeze their files either for free or for a fee throughout the U.S. This right is available to all consumers. A consumer can initiate a security freeze online, by phoning, or sending a certified letter to each national credit bureau where the consumer wants his or her file frozen. A freeze can be temporarily "lifted" relatively quickly by the consumer contacting the credit bureau or using a special PIN provided by the credit bureau to the consumer when the file was first frozen.

Servicemembers Civil Relief Act

A federal law that imposes a 6% rate cap on pre-service credit obligations during the member's period of military service. This includes secured credit such as motor vehicle financing for members of the military and their dependents. A service member or their dependent may also terminate an auto lease if the service member, after the lease is executed, enters military service for a period of 180 days or more. A service member or his dependent may also terminate an auto lease entered into while the service member was on active duty if the service member receives military orders for a permanent change of station outside the continental U.S. or a deployment of 180 days or more. For any lease termination, the vehicle must be returned to the lessor within 15 days of delivering the notice of termination. During the period of military service, a vehicle cannot be repossessed without a court order.

Single Document Rule

Provisions of state laws (for example, Minnesota and California) that require all of the agreements of the dealer and buyer to be contained in a single document, typically the RISC. The purpose of this rule is to prohibit dealers from relying on separate agreements containing financing terms which contradict those disclosed in the RISC or required by law. Courts in some states have held that the single document rule may not require everything to be on one piece of paper and permit multiple, contemporaneous pieces of paper such as, for example, a deferred down payment agreement or a buyer's order.

Social Media

Websites such as Facebook, LinkedIn, YouTube, and X (formerly known as Twitter) where consumers share information with other people in a virtual community. Companies can establish social media pages to promote their products and services interactively as well as purchase advertising on social media sites to target specific types of users. Social media sites are widely used by consumers who reveal preferences and interests and can raise challenges for auto dealers when a disgruntled consumer posts negative information about the dealership to a social networking site. Employees also use social media. A best practice is to adopt a social media policy that focuses on engaging consumers, participating, influencing, and monitoring social media sites. Employee posts on social media sites should be addressed in the social media policy as they may qualify as protected free speech particularly if related to unions or other concerted activity. All advertising rules and requirements that apply to media advertising generally also apply to social media advertising including ensuring that any disclaimers are clear and conspicuous in relation to the devices that will likely be used to view the ad (cell phone, tablet, laptop, etc.).

Starter Interrupt

A starter interrupt is technology or a device that is typically installed on the vehicle at the time of the extension of credit or reinstatement after default and repossession. Starter interrupt technology allows a creditor to remotely disable the starter on a vehicle if the buyer fails to comply with the terms of a credit agreement. A starter interrupt cannot disable a vehicle while the vehicle is in operation. The technology can include payment reminder and pre-disablement warnings.

Sweepstakes

A "game of chance" in which consumers enter to win prizes picked at random. A sweepstakes must have a "no purchase necessary" means

of entry (typically by mailing in a postcard) and sweepstakes rules must state the date the sweepstakes ends, the odds of winning, or that the odds depend on the number of entries received. Certain states require bonding of certain consumer sweepstakes, and other states have specific disclosure requirements. In contrast, a "game of skill" involves winning a prize by objectively outperforming other contestants in a universally assigned task (e.g., employee who sells the most vehicles in a month). Federal law requires the sweepstakes disclosure to provide that no purchase is necessary and making a purchase does not increase one's chances of winning, as well as giving the consumer a way to remove themselves from future mailings from the sweepstakes sponsor.

T

Telemarketing

At the federal level, telemarketing is regulated by two sources: (i) the Telephone Consumer Protection Act (TCPA), which is enforced by the Federal Communications Commission (FCC); and (ii) the Telemarketing Sales Rule (TSR), which is enforced by the FTC and in some instances the CFPB (which treats violations of the TSR as an unfair, deceptive, or abusive act or practice). First, the TCPA requires, among other things, obtaining a consumer's prior express written consent to deliver prerecorded telemarketing calls to landlines and cell phones as well as requiring prior written consent to the use of an auto dialer to make telemarketing calls or send marketing text messages to cell phone numbers (text messages are considered a form of calling). The FCC requires that the prior written consent identify the specific phone number to which it applies and indicate that the consent cannot be required as a condition of the purchase of a product or service. This consent must also include the consumer's signature. Second, the TSR, requires, among other things, disclosures in telemarketing campaigns and prohibits specific deceptive or abusive telemarketing acts or practices that are proscribed by the Rule. For example, the TSR prohibits telemarketing to persons whose phone numbers are on the National Do Not Call Registry, subject to limited exceptions. It also enables a consumer to opt out of a company's telemarketing. The FCC's regulation of telemarketers under the Telephone Consumer Protection Act establishes a second set of federal standards regulating telemarketing. Please note that some of the FCC's standards are identical to the FTC's. In other cases, the FCC and FTC regulate the same conduct but in different ways.

Terms of Use

An agreement between a website owner and a user that establishes the rules of the user's engagement with the website. The user must agree to the terms of use agreement in order to use the website. The agreement should be displayed on the website and easily accessible to the user.

Trigger Leads

A prescreening product sold by credit bureaus to dealers and lenders and used in the auto finance context. When a creditworthy consumer's credit report is accessed by an auto dealer, doing so may trigger a notice to the trigger leads buyer (another dealer or lender) who also receives the consumer's cell phone number to call the consumer and counteroffer him or her on the spot.

Truth in Lending Act (TILA)

The federal Truth in Lending Act (TILA) includes the federal Consumer Leasing Act, together with Federal Reserve Board (for auto dealers) and Consumer Financial Protection Bureau (for other creditors) Regulations Z and M. TILA provides for mandatory consumer disclosures in credit and leasing transactions and the advertising of credit. Regulation M covers consumer leasing transactions. Regulation Z covers credit sales, open-end credit (e.g., credit cards or lines of credit), and loans.

U

Uniform Electronic Transactions Act (UETA)

Adopted in 49 states and the District of Columbia, this law provides

a framework for conducting transactions electronically instead of by paper. UETA is the state counterpart to the federal E-SIGN Act. The one state that has not adopted the UETA is New York, which had already enacted its Electronic Signatures and Records Act to make legal electronic signatures in New York.

Unconscionability

A doctrine used to void contracts or provisions of contracts as being unfair and void against public policy and used particularly by plaintiffs' lawyers in challenging the enforceability of arbitration and class action waiver clauses in consumer finance contracts. Unconscionability consists of both an absence of meaningful choice for the party opposing enforceability of the agreement such as a non-negotiable contract (so-called procedural unconscionability) combined with contract terms that are unreasonably favorable to the other party (substantive unconscionability).

Unfair or Deceptive Acts or Practices (UDAP)

Section 5 of the FTC Act prohibits "unfair methods of competition and unfair or deceptive acts and practices in or affecting commerce" against consumers. These types of practices generally involve false or misleading information communicated to consumers that is likely to cause those consumers to suffer financial loss or other injury. The CFPB's Dodd-Frank Act similarly prohibits unfair, deceptive, or "abusive" acts or practices. Companies must also be mindful of state laws prohibiting UDAPs.

The USA Patriot Act

A post-9/11 law requiring, among other things, that certain creditors verify the identity of every customer, establish formal anti-money laundering programs, and report suspicious activity. Dealers are currently exempt from these requirements but are subject to other requirements under the USA Patriot Act, including reporting of certain currency transactions (see IRS/FinCEN Form 8300) and OFAC requirements (see Office of Foreign Asset Controls (OFAC) and SDN List).

Used Car Rule

An FTC rule requiring dealers to prominently and conspicuously post a Buyer's Guide on all used cars prior to the car being offered for sale or lease. The Buyer's Guide must disclose detailed warranty information and contain other consumer disclosures. If the sale negotiations are conducted in Spanish, a Spanish version of the Buyer's Guide must be posted on the car. The Used Car Rule does not apply in Maine or Wisconsin, where similar state regulations require posted disclosures on used vehicles. Other states may have additional requirements for posting disclosures on used vehicles.

W

Wavier

An intentional relinquishment or abandonment of a known right, claim, or privilege against another person or entity. For example, dealers may often require a customer to waive his or her right to bring a class action against the dealer in order to purchase a vehicle from the dealer.

Warranty

A promise by the manufacturer or seller of a vehicle to make repairs or correct defects during a defined period of time. Warranties can be express or implied, full or limited, and are a part of the cost of the vehicle. The warranty terms must be clearly and conspicuously summarized, with the full warranty terms made available to the customer under the MMWA. Separate vehicle protection coverage that a customer pays for, in addition to the vehicle price, is a "service contract," and different legal rules apply to warranties and service contracts. Implied warranties are governed by state law but cannot be disclaimed by a dealer who offers a written warranty or sells the customer a service contract within 90 days of the vehicle sale.