CrowdStrike eBook

CROWDSTRIKE

A Guide for Auto Dealerships

Understanding and Implementing Requirements of the Federal Trade Commission Safeguards Rule

This document provides auto dealerships with an introduction to the U.S. Federal Trade Commission (FTC) Safeguards Rule, its objectives and an overview of the nine security requirements. It also provides useful recommendations to help you complete each Safeguards Rule requirement successfully.

In December 2021, the FTC amended its Safeguards Rule to include a new set of stringent data protection and security standards designed to better protect financial institutions from cyber threats. These rules are intended to secure and protect "information about your own customers as well as information about customers of other financial institutions that have provided data to you." The FTC also broadened the definition of a financial institution to include auto dealerships.

For auto dealerships, the Safeguards Rule represents a huge leap forward in protecting customer data and implementing a comprehensive security solution. Initially, auto dealerships were required to comply with the amended Safeguards Rule by December 2022. However, the compliance deadline was moved to June 9, 2023, to provide auto dealerships with more time to assess their business and implement an appropriate security program. Due to the complexity of the Safeguards Rule and its numerous requirements, many auto dealerships missed the June 9, 2023, deadline.

Whether you have started implementing the FTC Safeguards Rule but are not yet fully compliant, or if you have not started updating your dealership's security measures, CrowdStrike can help.

Why are auto dealerships required to be compliant?

Auto dealerships are a prime target for cybercriminals[1] because they are viewed as easy targets for cyberattack. [2]

Cybercriminals believe that most auto dealerships have the following characteristics:

- Open Wi-Fi networks
- Outdated IT infrastructure
- Insufficient processes to protect employee login information
- Easy access to personally identifiable information (PII)
- Availability of financial data
- Low cybersecurity awareness and lack of modern cybersecurity solutions

The FTC hopes to achieve three primary goals through the Safeguards Rule:

- Ensure the security and confidentiality of customer information
- Protect against threats to the security or integrity of customer information
- Protect against unauthorized access to information that could result in substantial harm or inconvenience to any customer [3]

How do you know if you must comply?

According to Section 314.2 of the FTC Safeguards Rule, dealerships that collect information on less than 5,000 consumers are exempt from the following three Safeguards Rule requirements:

- Performing and recording a written risk assessment
- Maintaining an Incident Response Plan
- Providing an annual report to the [auto dealership's] Board of Directors[4]

Auto dealerships that collect customer data on more than 5,000 consumers are required to comply.

[1]"Auto Dealers are Prime Targets for Hackers, Researchers Warn," Steve Zurier, February 8, 2023. Source
[2]"How to protect your car dealership from cyber-attacks," Karasavvas, Theodoros, February 7, 2023. Source
[3]"FTC Safeguards Rule: What Your Business Needs to Know" Source
[4]"FTC Safeguards Rule: What Your Business Needs to Know" Source

What are the risks of non-compliance?

In addition to leaving your business and customer data open to attack, if an auto dealership is non-compliant, under the Penalty Offense Authority, the FTC can seek civil penalties of up to $46,517 USD per violation and file a seven-figure FTC-backed civil lawsuit. Auto dealerships can suffer reputational damage if their customer information is stolen or compromised. The bottom line? Every auto dealership needs to comply with the Safeguards Rule as soon as possible.

Is it too late to get started?

The deadline was June 9, 2023

It's never too late to protect your customers' data and your business from attack. Whether you started implementing the FTC Safeguards Rule and your efforts have stalled, you're still in the process of meeting all nine Safeguards Rule requirements, or you haven't started, **CrowdStrike can help**.

CrowdStrike has expertise in successfully protecting automotive businesses with industry-leading security solutions, 24/7 monitoring, and robust reporting capabilities. CrowdStrike's seasoned security experts can help you address requirements of the Safeguards Rule.

Navigating the FTC Safeguards Rule in Plain English

To help you navigate and implement the requirements of FTC Safeguards Rule, this eBook provides a simplified guide to its provisions and offers easy-to-follow recommendations for protecting your business and your customers. CrowdStrike recommends you fully read the FTC Safeguards Rule and speak with your legal counsel about the requirements and how they impact your business before getting started. In addition, check out CrowdStrike's helpful webpage, Cybersecurity 101: Fundamentals of Cybersecurity, if you are unfamiliar with terminology in this document.

Rule #1

Designate a qualified individual to implement and supervise your company's information security program.

Addressing Rule 1 can be difficult if your company doesn't employ an IT resource or IT staff with the security experience needed to design, implement and provide ongoing oversight of a comprehensive security program. In larger organizations, a Chief Information Security Officer (CISO) or specialized IT security staff perform these tasks, but CISOs are in high demand and command a high salary — often beyond the budget of small or midsize businesses.

Recommendation: Consider partnering with a well-known cybersecurity company that provides full-time managed services. Managed security services providers (MSSPs) provide cybersecurity solutions and qualified staff to implement, oversee and report on your security program for the long term.

Note: Per the FTC Safeguards Rule, you are still required to assign a senior member of your staff to oversee the MSSP (or other security-related partners) because the FTC views your dealership as ultimately responsible for compliance with the Safeguards Rule.

Rule #2

Conduct a risk assessment.

Create an inventory of customer data — physical and digital — and the places in which that data resides. Next, assess your current security measures. The FTC requires that your risk assessment must be written down and include the criteria used to create the assessment. In addition, the Safeguards Rule requires that you conduct periodic risk assessments to mitigate future risk, as cyberthreats are constantly evolving.

The entirety of your information security program will be created in response to the findings in your risk assessment and the current cyber threat environment — you have to get this right. Creating a security risk assessment requires skills beyond the scope of a typical IT administrator or IT resource unless they have a specific background in cybersecurity.

Recommendation: If this is your first time conducting a risk assessment, the task may seem daunting. Hiring an MSSP or security firm to conduct a thorough risk assessment and provide you with a comprehensive written report of its findings is recommended to ensure you identify potential risks to customer data in your organization.

If you are concerned about your business's ability to conduct a thorough risk assessment, **CrowdStrike can help**. The CrowdStrike Technical Risk Assessment highlights security vulnerabilities, weaknesses and gaps in your IT environment across endpoint devices, applications and user identities. The assessment provides visibility into applications, accessibility and account management within your network, identifying vulnerabilities such as missing patches or poor password hygiene to enable you to proactively safeguard your network and customer data before a breach occurs.

However, if you want to conduct an in-house risk assessment, begin by following customer data throughout the customer life cycle at your dealership. Start where customer information is first gathered, then note every point at which customer data (credit score, Social Security number, bank account information) is recorded, processed and/or transmitted — to and from your dealership. Include external credit agencies, banks, lenders and any other organizations involved in a customer transaction. Also note physical locations where customer data may be stored (examples might include invoices, credit applications, etc.) and any other location where customer data is stored. Then address the ways each location with customer data can be accessed and/or is vulnerable to threats. Document your findings thoroughly.

Rule #3

Design and implement safeguards to control the risks identified through the risk assessment.

This rule is one of the most complicated to comply with if you do not have in-house IT security staff. To implement Rule 3, you need a resource with a technical background and security experience. Rule 3 includes the following components or controls.

- **Access controls:** Access controls include password protection on applications and servers that contain customer data, and requires locks on areas where physical data is stored. Furthermore, access to customer data must be limited to authorized users.
- **Multifactor authentication:** The Safeguards Rule requires that dealerships implement multifactor authentication (MFA) for employees, vendors and other individuals accessing networks that contain customer information.
- **Monitoring authorized users' activities:** Adopt policies and procedures to monitor and log authorized users' activity and detect unauthorized access, access attempts or use of customer information.
- **Encryption:** All customer data must be encrypted during transit via networks and at rest (places the data resides such as servers, in a public or private cloud, and within an application).
- **Disposal procedures:** Dealerships must create procedures for disposing customer data no later than "two years after the last date of use." You may retain customer information for more than two years if it is "necessary for business operations or other legitimate business purposes." [5]
- **Secure development procedures:** If your dealership has an IT team that develops software applications then you are required to adopt secure development practices. You must be able to test internally and externally developed applications. This requirement applies to all applications that transmit or store customer information.
- **Change management procedures:** Change management must be built into your information security program and include procedures that assess the security of your devices and networks.

Recommendations: If your dealership does not employ a CISO and does not plan to hire one, partner with security experts to implement, oversee and maintain these provisions. This not only ensures the Safeguards Rule is implemented properly, it also saves your dealership money on IT staffing. You can remain focused on your core business while the security provider manages your cybersecurity measures. In addition, adopt the principle of "least privilege" when granting access to individuals within your company. This helps ensure employees only have access to the systems and data required to do their jobs.

[5] https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Rule #4

Regularly monitor and test your safeguards.

You are required to conduct regular security testing or continuous network monitoring to detect security threats. The Safeguards Rule also requires annual penetration testing and twice-a-year vulnerability assessments.

Recommendations: Rule 4 will be difficult to implement without the assistance of a security partner or MSSP. CrowdStrike offers services that will perform regular security tests and monitor your network 24/7/365 to help you meet requirements of Rule 4. CrowdStrike provides standby access to CrowdStrike security consultants who have the expertise to enhance your security practices and train your IT team and employees using real-life simulation exercises. Two examples that meet the requirements of the Safeguards Rule include:

- **PENETRATION TESTING:** CrowdStrike Penetration Testing Services simulate real-world attacks on different components of your IT environment to test the detection and response capabilities of your people, processes and technology, and identify where vulnerabilities exist in your environment.
- **TABLETOP EXERCISES:** During a CrowdStrike Tabletop Exercise, experts guide your organization — both executive and technical participants — through a targeted attack scenario. This discussion-based exercise simulates a targeted attack in a time-compressed fashion, but without the risk and time required for a full adversary emulation.

Rule #5

Train your staff.

Provide your staff with security awareness training and offer regular refresher courses. Your security is only as good as your least vigilant staff member. Phishing scams, sophisticated malware and viruses constantly evolve and become more difficult to detect.

Recommendations: Look for an outside security vendor or an online security awareness platform to provide employee training and materials. Visit www.CISA.gov for free posters on the dangers of ransomware, which can be used inside your dealership to remind employees to stay vigilant, and take steps to create an employee cybersecurity awareness training program. You can partner with CrowdStrike to provide security training for employees at all levels.

Rule #6

Monitor your service providers.

This rule requires dealerships to proactively vet security providers and MSSPs before they are hired and closely evaluate software and cloud vendors that process, collect, store or access customer data on their behalf.

Recommendations: Ensure your vendor contract explicitly describes the security services they will provide and ensure your MSSPs are familiar with the FTC Safeguards Rule. Look for partners that understand compliance. Develop and implement policies that govern the evaluation and ongoing compliance management of all service providers. Finding a security service provider with experience in the automotive industry enables speed-to-value when creating and implementing a customer information security program. CrowdStrike has that experience.

Rule #7

Keep your information security program current.

In business, change is constant. Changes in personnel, IT systems, CRM systems, applications and new business processes have the potential to create risk and impact security measures. Ensure you implement security software that deters threats and, at minimum, protects your business and customers from malware, ransomware and viruses.

Recommendation: When you draft your security strategy, ensure you build in flexibility to account for change and/or modifications without placing customer data at risk. Ensure your security provider is an industry leader and its solutions protect you from today's threats. CrowdStrike offers a next-generation antivirus (NGAV) solution that can stop viruses and sophisticated malware that doesn't require placing code on your systems.

Rule #8

Create a written Incident Response Plan.

It is essential that your Incident Response Plan details how your dealership will respond and recover if it is breached by cybercriminals or if your data is mishandled. The Safeguards Rule requires you to create an **Incident Response Plan** that includes the following:

- Written goals of your information security plan
- Internal processes in the event of a security breach
- Clear roles, responsibilities and levels of decision-making authority in case of a security breach
- Designated channels for communication and information-sharing inside and outside your company
- Processes to fix identified weaknesses in your systems
- Procedures for documenting and reporting security events and your company's response if you experience a breach
- Processes for conducting a postmortem of the event, making revisions to your Incident Response Plan if needed, and updating your information security program to prevent another cyber event.

Recommendations: Ensure there are multiple physical and digital copies of your Incident Response Plan in case of a security breach. If you use a partner to maintain your cybersecurity solutions, ensure the partner is familiar with your incident response protocols. Learn useful steps here: https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/

Rule #9

Require the "Qualified Individual" to report to your Board of Directors.

The FTC requires someone within your organization to report annually on the state of security to your dealership's Board of Directors. The report must include a performance assessment of your information security strategy as well as your business's compliance with the FTC Safeguards Rule. Other specifics that should also be included are the results of periodic risk assessments throughout the calendar year, risk management protocols, test results, a list of security events (if any occur) and any planned updates to your IT systems or to your information security program.

Recommendation: For most dealerships, completing the FTC Safeguards Rule will require partnering with a leading security provider to implement and manage a comprehensive cybersecurity solution. Ensure you choose a security provider with comprehensive security solutions and managed services that monitor, defend and protect your business and your data. Ensure your security partner has experience with compliance requirements (both business and technical) and will be able to generate all of the reports required by the Safeguards Rule. Familiarity with the Safeguards Rule will also help ensure the best outcome for your dealership. Consider CrowdStrike Falcon® Complete managed detection and response (MDR) to provide 24/7 protection.

About CrowdStrike Falcon Complete

Falcon Complete is a sophisticated security solution delivered by CrowdStrike's team of experts to protect endpoints, cloud workloads, identities and data. It also delivers unparalleled security by providing next-gen antivirus (NGAV) protection, CrowdStrike Falcon® Insight XDR extended detection and response, CrowdStrike Falcon® Identity Threat Protection and CrowdStrike® Falcon OverWatch™ managed threat hunting combined with the expertise and 24/7 engagement of the Falcon Complete team.

How CrowdStrike Falcon Complete Helps Protect Auto Dealerships

For auto dealerships with limited IT or security personnel, the Falcon Complete solution and security team provide the following benefits:

- Actively manages and monitors your IT environment, remotely remediating security incidents in minutes.
- Protects your critical data whether on-premises or in the cloud.
- Protects your endpoints (laptops, servers, desktops, smart tablets, phones and more).
- Provides identity management to ensure only authorized employees access your data.
- Solves the challenges of implementing and running an effective security program without the difficulty and costs associated with building one internally.

According to Forrester, CrowdStrike's "exceptional" Falcon Complete MDR service "blends products, platforms, and services seamlessly for customers." For assistance with implementing requirements under the Safeguards Rule, don't hesitate to contact us for more information.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **www.crowdstrike.com/**

Follow us: **Blog** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**