PDS has compiled the following summary regarding FTC Safeguard Rule and the requirements assigned to our clients identified as a 'financial institution' under the 2021 amended rules. We have highlighted the areas under the Information Security Program description where we have identified if the safeguard is met satisfactorily or if mitigation is required. Yellow highlights are areas we identified that your company needs to take action. Green are areas where PDS has you covered and blue areas are where we may be deficient and additional investment in technologies may be required. Please review this summary and we are happy to work with you on reaching compliance.

What is the Purpose of the FTC's Safeguard Rule?

As the name suggests, the purpose of the Federal Trade Commission's Standards for Safeguarding Customer Information – the Safeguards Rule, for short – is to ensure that entities covered by the Rule maintain safeguards to protect the security of customer information.

Why does this apply to auto-dealerships?

Broader definition to what is a financial institutions under the Rule, including finance companies. The 2021 amendments to the Safeguards Rule add a new example of a financial institution – finders. Those are companies that bring together buyers and sellers and then the parties themselves negotiate and consummate the transaction.

What is required of a "financial institution"?

The Safeguards Rule requires covered financial institutions to develop, implement, and maintain an **information security program** with <u>administrative</u>, <u>technical</u>, and <u>physical</u> safeguards designed to protect customer information.

What are the objectives of an Information Security Program?

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

What does a reasonable information security program look like?

Section 314.4 of the Safeguards Rule identifies nine elements that your company's information security program must include. Let's take those elements step by step.

a. ***Designate a Qualified Individual to implement and supervise your company's information security program.*** The Qualified Individual can be an employee of your company or can work for an affiliate or service provider. The person doesn't need a particular degree or title. What matters is real-world know-how suited to your circumstances. The Qualified Individual selected by a small business may have a background different from someone running a large corporation's complex system. If your company brings in a service provider to implement and supervise your program, the buck still stops with you. It's your company's responsibility to designate a senior employee to supervise that person. If the Qualified Individual works for an affiliate or service provider, that affiliate or service provider also must maintain an information security program that protects your business.

b. ***Conduct a risk assessment.*** You can't formulate an effective information security program until you know what information you have and where it's stored. After completing that inventory, conduct an assessment to determine foreseeable risks and threats – internal and external – to the security, confidentiality, and integrity of customer information. Among other things, your risk assessment must be written and must include criteria for evaluating those risks and threats. Think through how customer information could be disclosed without authorization, misused, altered, or destroyed. The risks to information constantly morph and mutate, so the Safeguards Rule requires you to conduct periodic reassessments in light of changes to your operations or the emergence of new threats.

c. ***Design and implement safeguards to control the risks identified through your risk assessment.*** Among other things, in designing your information security program, the Safeguards Rule requires your company to:

1. **Implement and periodically review access controls.** Determine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it.

2. **Know what you have and where you have it.** A fundamental step to effective security is understanding your company's information ecosystem. Conduct a periodic inventory of data, noting where it's collected, stored, or transmitted. Keep an accurate list of all systems, devices, platforms, and personnel. Design your safeguards to respond with resilience.

3. **Encrypt customer information on your system and when it's in transit.** If it's not feasible to use encryption, secure it by using effective alternative controls approved by the Qualified Individual who supervises your information security program.

4. **Assess your apps.** If your company develops its own apps to store, access, or transmit customer information – or if you use third-party apps for those purposes – implement procedures for evaluating their security.

5. **Implement multi-factor authentication for anyone accessing customer information on your system.** For multi-factor authentication, the Rule requires at least two of these authentication factors: a knowledge factor (for example, a password); a possession factor (for example, a token), and an inherence factor (for example, biometric characteristics). The only exception would be if your Qualified Individual has approved in writing the use of another equivalent form of secure access controls.
6. **Dispose of customer information securely.** Securely dispose of customer information no later than two years after your most recent use of it to serve the customer. The only exceptions: if you have a legitimate business need or legal requirement to hold on to it or if targeted disposal isn't feasible because of the way the information is maintained.

7. **Anticipate and evaluate changes to your information system or network.** Changes to an information system or network can undermine existing security measures. For example, if your company adds a new server, has that created a new security risk? Because your systems and networks change to accommodate new business processes, your safeguards can't be static. The Safeguards Rule requires financial institutions to build change management into their information security program.

8. **Maintain a log of authorized users' activity and keep an eye out for unauthorized access.** Implement procedures and controls to monitor when authorized users are accessing customer information on your system and to detect unauthorized access.

d. ***Regularly monitor and test the effectiveness of your safeguards.*** Test your procedures for detecting actual and attempted attacks. For information systems, testing can be accomplished through continuous monitoring of your system. If you don't implement that, you must conduct annual penetration testing, as well as vulnerability assessments, including system-wide scans every six months designed to test for publicly-known security vulnerabilities. In addition, test whenever there are material changes to your operations or business arrangements and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

e. ***Train your staff.*** A financial institution's information security program is only as effective as its least vigilant staff member. That said, employees trained to spot risks can multiply the program's impact. Provide your people with security awareness training and schedule regular refreshers. Insist on specialized training for employees, affiliates, or service providers with hands-on responsibility for carrying out your information security program and verify that they're keeping their ear to the ground for the latest word on emerging threats and countermeasures.

f. ***Monitor your service providers.*** Select service providers with the skills and experience to maintain appropriate safeguards. Your contracts must spell out your security expectations, build in ways to monitor your service provider's work, and provide for periodic reassessments of their suitability for the job.

g. ***Keep your information security program current.*** The only constant in information security is change – changes to your operations, changes based on what you learn during risk assessments, changes due to emerging threats, changes in personnel, and changes necessitated by other circumstances you know or have reason to know may have a material impact on your information security program. The best programs are flexible enough to accommodate periodic modifications.

h. ***Create a written incident response plan.*** Every business needs a "What if?" response and recovery plan in place in case it experiences what the Rule calls a security event – an episode resulting in unauthorized access to or misuse of information stored on your system or maintained in physical form. Section 314.4(h) of the Safeguards Rule specifies what your response plan must cover:

- The goals of your plan;
- The internal processes your company will activate in response to a security event;
- Clear roles, responsibilities, and levels of decision-making authority;
- Communications and information sharing both inside and outside your company;
- A process to fix any identified weaknesses in your systems and controls;
- Procedures for documenting and reporting security events and your company's response; and
- A *post mortem* of what happened and a revision of your incident response plan and information security program based on what you learned.

i. ***Require your Qualified Individual to report to your Board of Directors.*** Your Qualified Individual must report in writing regularly – and at least annually – to your Board of Directors or governing body. If your company doesn't have a Board or its equivalent, the report must go to a senior officer responsible for your information security program. What should the report address? First, it must include an overall assessment of your company's compliance with its information security program. In addition, it must cover specific topics related to the program – for example, risk assessment, risk management and control decisions, service provider arrangements, test results, security events and how management responded, and recommendations for changes in the information security program.