Automobile Dealers and the FTC's Safeguards Rule

Frequently Asked Questions

The Federal Trade Commission (FTC) has developed these FAQs to help automobile dealers comply with the Gramm-Leach-Bliley Act and the FTC's Safeguards Rule. The following questions and answers discuss the requirements of the Safeguards Rule and apply it to specific situations that automobile dealers may face. These FAQs are meant to supplement the compliance materials available on the FTC website, including the FTC's business explainer: FTC Safeguards Rule: What Your Business Needs to Know | Federal Trade Commission. You might also want to familiarize yourself with the FTC's Privacy Rule FAQs for automobile dealers: The FTC's Privacy Rule and Auto Dealers: Frequently Asked Questions ("Privacy Rule FAQs"). Please note that this document represents the views of FTC staff and is not binding on the Commission.

A. SAFEGUARDS RULE 101

1. What is the FTC's Safeguards Rule?

The FTC's Safeguards Rule, which dates back to 2003, requires financial institutions to maintain safeguards to protect customer information. The FTC issued the Rule to implement the requirements of the Gramm-Leach-Bliley Act, and it applies to financial institutions subject to the FTC's authority. That includes most automobile dealers who finance or lease automobiles.

In 2021, the FTC amended the Safeguards Rule to provide more specific guidelines for financial institutions and to ensure that the Rule keeps pace with current technology. The amended Safeguards Rule requires financial institutions to have written information security programs to protect the customer information they have and certain safeguards, which are listed below.

A further amendment in 2023 requires financial institutions to report to the FTC certain data breaches and security incidents involving their customer information. That requirement took effect in May 2024.

2. What does the Safeguards Rule require automobile dealers to do?

The Safeguards Rule requires automobile dealers who are financial institutions to develop, implement, and maintain a comprehensive written information security program that is sufficient to protect customer information. We discuss all of that in more detail below, but the bottom line is that you should determine what customer information you have, and then plan and implement your information security program around that – so if you are a large company with significant amounts of customer information that many employees need to access, your written information security program will probably be more robust than it would be if you only keep a little bit of customer information in one place. You also need to maintain your program, meaning you should monitor its effectiveness and update it if necessary.

3. What automobile dealers qualify as "financial institutions"?

"Financial institutions" are businesses that are significantly engaged in financial activities or activities incidental to such financial activities. That covers more entities than you might imagine, because it focuses on the kinds of activities a business engages in rather than on how the business might describe itself. In addition, businesses that engage in both financial activities and non-financial activities are still financial institutions if they significantly engage in the financial activities.

Automobile dealers who finance (or facilitate the financing of) automobiles for consumers are financial institutions for purposes of the Safeguards Rule, since lending money is considered a financial activity under the relevant federal law. 12 U.S.C. § 1843(k). Automobile dealers also qualify as financial institutions if they lease automobiles for longer than 90 days, since leasing is considered financial activity as well. 13 C.F.R. § 314.2(h)(2)(ii).

4. What is "customer information"?

Generally, under the FTC's Safeguards Rule, customer information is any record containing nonpublic personal information about a customer of a financial institution that is handled or maintained on or on behalf of the financial institution or its affiliates. Let's unpack that definition.

- Under the Safeguards Rule, a "consumer" is anyone who seeks a financial product or service from you that is primarily for their own personal, family, or household use.
- That includes anyone who applies to you for credit or who gives you nonpublic personal information so you can determine whether they qualify for financing – for example, to finance or lease an automobile.
- If you provide financing to or arrange financing for the consumer, then you are entering into a continuing relationship with the consumer.
- Once there is a "continuing relationship," the consumer becomes your "customer."
- Any non-public personally identifiable information the customer provided to obtain the financing is "customer information" that you have to protect under the FTC's Safeguards Rule.
- "Customer information" also includes any information that is derived from personally identifiable financial information, such as a list identifying all the customers who financed their automobiles with you. See 16 C.F.R. § 314.2(l)(1) (definition of "nonpublic personal information"); § 314.2(d) (defining "customer information" as "any record containing nonpublic personal information about a customer of a financial institution. . . .").

Given those definitions, certain types of records are always going to be customer information and covered by the Safeguards Rule:

- Applications you approved for financing or leasing (that include information like the customer's name, address, Social Security number, and financial account information).
- Spreadsheets of the names and addresses of customers who financed or leased automobiles from you.

- Financial information related to individual consumers who financed or leased automobiles from you.

Other types of records do not qualify as "customer information," and the Safeguards Rule will not apply to them unless they are combined with customer information:

- Names and addresses that you collect from everyone (so long as the information doesn't indicate whether they financed or leased their automobiles) – for example, to share with an Original Equipment Manufacturer (OEM) for the purpose of sending recall notices.
- General sales data reports or other aggregate information about your automobile sales that isn't derived from how the automobiles were financed or leased.
- Service or maintenance records for automobiles that you sold, leased, or generally serviced.

5. What is an "information security program"?

The Safeguards Rule defines an "information security program" as the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

In other words, your information security program is all of the processes and procedures you follow to protect your customer information. That includes the ways you collect and store customer information, as well as how you share it with other companies and how you get rid of it when you no longer need it.

6. How do I know if my information security program is "sufficient to protect" my customer information?

The Safeguards Rule says that your written information security program must be reasonably designed to achieve the following goals:

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

In particular, your written program should contain administrative, technical, and physical safeguards that are appropriate for your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.

The Safeguards Rule also spells out ten different elements that you should include in your program to meet those goals (which are each explained in more detail at 16 C.F.R. § 314.4), including:

- *Designate a qualified individual to oversee and implement the program*. The individual can be one of your employees or someone who works for an affiliate or service provider.

- *Base the program on a written risk assessment that identifies reasonably foreseeable internal and external risks to your customer information and assesses the safeguards you have in place*. The risk assessment should lay out the criteria you used to identify risks, as well as how you assessed your current systems and how you will mitigate the risks you identified. You should also periodically re-assess the risks and your safeguards to make sure you are focusing on current threats.

- *Design and implement safeguards to control those risks.* Such safeguards include access controls, encryption of customer information at rest and in transit, multifactor authentication for anyone who accesses your information system, and logging and monitoring activity, among other things.

- *Regularly monitor and test how well your safeguards are working.* You should continuously monitor information systems. If you cannot continuously monitor, then you must conduct annual penetration testing and vulnerability assessments at least every six months.

- *Adopt policies and procedures to ensure your personnel can enact your information security program.* This should include security awareness training for everyone and specialized training for staff who actually carry out the information security program.

- *Oversee your service providers.* You should take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information, require them to agree in the contract to implement and maintain those safeguards, and periodically assess them based on the risk they present and the continued adequacy of their safeguards.

- *Keep your information security program current.* Make adjustments and improvements based on the results of your monitoring, penetration testing, and risk and vulnerability assessments. Also consider whether material changes to your business or other circumstances necessitate changes to your program.

- *Create a written incident response plan.* This should be your blueprint for how to respond to and recover from any security incident that affects the confidentiality, integrity, or availability of your customer information. Among other things, the plan should lay out your internal processes for responding to a security event (including the roles, responsibilities, and levels of decision-making authority for your team), identify requirements for remediations of any weaknesses you identify in your information system, and spell out any documentation and reporting procedures.

- *Require your designated Qualified Individual to report to your Board of Directors or other governing body for your business.* The reporting should be in writing, and it should happen regularly (at least annually). It should include the overall status of the

program and how you have complied, and identify and address any material matters related to the information security program (such as risk assessments, service provider arrangements, and security events).

- *Notify the Federal Trade Commission about breaches*. If you do have a breach that results in the loss or exposure of customer information – which the Safeguards Rule refers to as a "notification event" – you may need to notify the FTC about it within 30 days. This is a new requirement in effect as of May 2024, and we discuss it more below.

The Safeguards Rule requires you to secure information systems that contain customer information as well as those that are ***connected*** to a system containing customer information. In effect, unless you maintain two separate networks that are not connected, the protections that you need to provide for customer information on your network will also protect other information on your network. The Rule also requires you to implement physical security safeguards, such as locking file cabinets where paper records are stored.

7. How do I know if I have a "notification event"?

The Safeguards Rule requires financial institutions to notify the FTC as soon as possible – and no later than 30 days after discovery – of a security breach involving the unauthorized acquisition of at least 500 consumers' unencrypted information. This is known as a "notification event" under the Safeguards Rule.

For purposes of the Rule, "unencrypted information" includes unauthorized *access* to unencrypted information as well as unauthorized *acquisition*. And if the encryption key was also accessed, it covers encrypted customer information. Unauthorized acquisition will be presumed unless you have reliable evidence to show that there has not been, or could not reasonably have been, unauthorized acquisition of the customer information in question.

B. SPECIFIC SITUATIONS FOR AUTOMOBILE DEALERS

1. As an automobile dealer, I already comply with the Privacy Rule. Do the requirements of the Safeguards Rule differ from the Privacy Rule requirements?

Yes. As discussed above, the FTC's Safeguards Rule requires most automobile dealers that arrange financing or lease automobiles to develop, implement, and maintain a comprehensive information security program to safeguard customer information, which generally will include any nonpublic personal information you collect from customers for whom you have arranged the financing or leasing of an automobile.

The Privacy Rule, on the other hand, generally requires automobile dealers to provide notices about their information practices to both consumers who sought leasing or financing and customers who actually obtained the lease or financing, as well as to comply with certain limitations on disclosure of nonpublic personal information. In particular, the Privacy Rule requires a financial institution to provide a notice of its privacy policies and practices with respect to both affiliated and nonaffiliated third parties, and to allow the individual to opt out of the disclosure of the

individual's nonpublic personal information to a nonaffiliated third party if the disclosure is outside of the exceptions.

Under the Privacy Rule, customer information or consumers' information can be disclosed to nonaffiliated third parties pursuant to that rule's requirements. For example, with certain exceptions, the Privacy Rule requires you to give consumers the right to opt out of having their nonpublic personal information disclosed to a nonaffiliated third party. This is in 16 C.F.R. § 313.10. If the consumer does not opt out after you have provided the required notice and a reasonable opportunity to opt out, you may disclose that nonpublic personal information to the third party. But whether the consumer opts out or not, if the consumer is a customer – someone you have a continuing relationship with – you are obligated under the Safeguards Rule to protect that customer's nonpublic personal information that you maintain.

In short, the Privacy Rule addresses your consumer and customer information collection and sharing practices, while the Safeguards Rule addresses how you must protect the customer information you collect and maintain.

2. Are automobile dealers obligated to treat consumer and customer information the same way under the FTC's Safeguards Rule and the Privacy Rule?

No. Your obligations to protect customer information under the Safeguards Rule are distinct from your obligations under the Privacy Rule to provide notices and opt-outs to consumers and customers.

First, it's important to remember that not every individual who contacts your automobile dealership is going to qualify as a "consumer," not to mention becoming a "customer," for purposes of these two rules. If you collect a name and address from everyone who buys a car from your dealership, regardless of whether they seek financing from you, that is not consumer information or customer information.

Generally, the FTC's Privacy Rule applies to automobile dealers who:

- Extend credit (for example, through a retail installment contract) in connection with the purchase of an automobile for personal, family, or household use;
- Arrange to finance or lease an automobile for personal, family, or household use; or
- Provide financial advice or counseling to individuals.

If you engage in these activities, any personal information that you collect to provide these services is covered by the Privacy Rule. The Privacy Rule applies even if you collect personal information about someone in connection with the potential financing or leasing of an automobile but that person never fills out a formal application.

Consumers may provide you with personally identifiable financial information in the context of applying to finance or lease an automobile from you. When you broker or arrange for that financing, you enter into a continuing relationship with that consumer, and they become your customer. In short, a customer is a consumer with whom you have a continuing relationship.

The Privacy Rule does not apply if an individual:

- Simply expresses an interest in buying an automobile from you;
- Asks general questions about financing or leasing;
- Buys an automobile from you with cash; or
- Arranges financing elsewhere.

That's because in these instances, the individual never even becomes a "consumer" under the Privacy Rule, much less a "customer."

The Safeguards Rule only applies to "customer information." Customer information, as explained above, is nonpublic personal information about a consumer who seeks a financial product or service from you that is primarily for their own personal, family, or household use. If you provide financing to the consumer, then you are entering into a continuing relationship with the consumer, and the consumer becomes your customer – so the information they provided to get the financing becomes "customer information" that you are obligated to protect under the Safeguards Rule. And at that point, you are also in a "customer relationship" with the consumer under the Privacy Rule.

3. Can a company be considered a service provider for purposes of the Safeguards Rule and not the Privacy Rule, or vice versa?

"Service provider" is not a defined term under the Privacy Rule, but the Safeguards Rule defines the term "service provider" to mean "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part." The Safeguards Rule says that when you give a service provider access to customer information, you must monitor the safeguards that service provider uses to protect that information. The Rule discusses ways you can do that at 16 C.F.R. § 314.4(f). But the bottom line is that to be a service provider under the Safeguards Rule, the other company must be providing you with a service that involves access to customer information.

A company that is a "service provider" for purposes of the Safeguards Rule might also qualify as a service provider under the Privacy Rule, but they do not entirely overlap. If you disclose information to a company pursuant to the Privacy Rule's service-provider exception (in 16 C.F.R. § 313.13), for example, then that company would be a service provider for purposes of the Safeguards Rule as well. But even if you do not avail yourself of the Privacy Rule's service-provider exception, a company within the Safeguards Rule's definition would still be a service provider under the Safeguards Rule.

4. Will an OEM always be a service provider under the Safeguards Rule? For example, if I provide an OEM with information to enable a customer to receive recall notices, is the OEM automatically a service provider?

No – an OEM will not be a service provider under the Safeguards Rule unless they are providing you with services. An OEM does not become your service provider just because you share information with them. If they are not providing you with services, they are not a service provider, and the Safeguards Rule would not require you to oversee the OEM's safeguards. For example, a company that collects customer names and addresses from you so the company can use them in

recall notices in the future would not be providing you with a service, and so would not be considered a service provider in connection with that activity.

However, as discussed above, you would need to conduct a separate analysis to determine if you need to comply with the Privacy Rule's notification and consent requirements before you share information with the OEM. That is also discussed more in our Privacy Rule FAQs.

5. Can I send OEMs records like (i) customer lists with names and addresses and (ii) Retail Delivery Reports that include names, addresses, and VIN numbers without violating the Privacy Rule or the Safeguards Rule?

It depends. If you collect a name and address from everyone who is buying a car from you – whether they seek financing or seek a lease from you or not – and you provide that list to an OEM, the name and address information by itself would not be covered by the Privacy Rule or the Safeguards Rule. The same is true for Retail Delivery Reports that include a name and address and a VIN number. It's neither consumer information nor customer information.

If you disclose name and address information together with information obtained in the financing process – even information simply indicating that the consumer has applied for or received financing – then that information is covered by the Privacy Rule, and you need to comply with the privacy notice and opt-out requirements of the Privacy Rule.

With respect to the Safeguards Rule, the name and address information by themselves are neither consumer information nor customer information, as noted above. You are not obligated to protect, say, a record such as a paper document that includes individuals' names and addresses alone. If that document indicates whether those individuals obtained financing from you, however, then that information *is* customer information and you would have an obligation to protect that information under the Safeguards Rule. Also remember that, even if a particular record is not customer information, if you keep customer information on your network you need to implement safeguards to protect your network generally. You would also have to oversee the OEM's safeguards if you disclose that information to an OEM that is acting as a service provider.

6. What if I keep all of the information I collect from individuals – people who have expressed interest in buying a vehicle, people who have applied for financing, and people who have obtained financing – in one comprehensive database that includes their name and address together with information about the vehicle they purchased, their Social Security number, the financial information they provided, etc.? How do the Privacy Rule and Safeguards Rule apply to this commingled data? What happens if I use the database to generate lists of individuals who have purchased vehicles from my dealership and disclose that list to the OEM?

The database itself and lists generated from the database are not the same records, and may require different treatment. Because the database includes "customer information" (including Social Security numbers and other financial information you obtained as part of the financing process), you are obligated to protect it under the Safeguards Rule. Among other things, that means you should control access to it.

Because the database includes "customer information," you will need to comply with the Privacy Rule if you provide the database to an OEM, unless an exception applies. However, a list that you generate from the database that consists of the names and addresses of everyone who purchased a vehicle from you would not be customer information subject to the Safeguards Rule *or* the Privacy Rule, even if you pulled the list from the commingled database, as long as the list does not indicate that the individuals sought or obtained financing or leasing from you, or include other personal nonpublic information about them (such as Social Security Numbers, income and banking information, or other financial information).

7. What if I store all of the information that I collect from individuals, including financing information, sales reports, and other information, in one place, and I give a service provider direct access to it? Do I have to monitor the service provider's safeguards with regard to the information that is not "customer information"?

Yes. Under the Safeguards Rule, you have an obligation to protect customer information. You also have obligations with respect to securing information systems that contain customer information or that are connected to a system containing customer information. If you provide a service provider direct access to your system, appropriate oversight of the service provider would include addressing the risk that the service provider's direct access to your information system would pose.

8. If I share customer information with a nonaffiliated company who is not a service provider – say, I disclose it with the customer's consent under 16 CFR § 313.15 to allow the customer to obtain a rebate or tax credit – do I have to monitor the nonaffiliated company's safeguards?

No. If that other company is not a service provider, you have no ongoing obligation under the Safeguards Rule to oversee that third party's security, even if the nonpublic personal information that you disclosed to that company is "customer information" under the Safeguards Rule.

9. What do I need to do to comply with the Safeguards Rule when it comes to service providers? Do I have to require my service providers to implement all ten of the specific measures that the Safeguards Rule requires me to implement?

It depends. Under the Safeguards Rule, a "service provider" is "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part." This could include any third parties you contract with to provide services that are related to customer information. For example, companies that help you process transactions, send out marketing materials, or shred paper documents could be service providers under the Safeguards Rule. The third party must be providing you a service to qualify as a service provider, though, and the service has to relate to customer information. As noted above, often the information you are sharing (for example, names and addresses of all of your customers where there's no indication how the customer paid for their car) is not actually customer information.

Financial institutions are required to oversee their service providers because poor data security practices by the service provider could enable a bad actor to access your customer information on that service provider's information system. Or if the service provider has direct access to your network, the service provider's poor data security could allow a bad actor directly into your network. A financial institution will comply with the Safeguards Rule requirements to oversee their service providers by doing three things:

- Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
- Requiring its service providers by contract to implement and maintain such safeguards; and
- Periodically assessing its service providers based on the risk they present and the continued adequacy of their safeguards. 16 C.F.R. § 314.4(f).

Your obligation to oversee the service provider does not mean that you have to get the service provider to agree to meet all of the Safeguards Rule requirements that apply to you as a financial institution, though. The Safeguards Rule gives you the flexibility to select service providers whose safeguards are appropriate for the customer information they will be using. The Commission noted when adopting the final rule that "the exact steps required depend both on the size and complexity of the financial institution and the nature of the services provided by the service provider." 86 Fed. Reg. 70296.

For example, if an automobile dealer provides an outside marketing company direct access to customer information on the financial institution's information systems, the marketing company's poor security for its own information system may enable a hacker to access the customer information that the financial institution maintains. And if an automobile dealer retains a shredding company to ensure the secure disposal of paper records, the company's access to customer information on those documents presents a risk that the financial institution must consider and address. However, the safeguards the financial institution would require the marketing company to take would differ from the requirements that would apply to the shredding company. In particular, the financial institution would not need to take measures to ensure that the shredding company's network security is appropriate if the shredding company does not have access to the financial institution's network.

Your own obligations as a financial institution may dictate that you select service providers capable of meeting certain specific safeguard requirements, depending on the nature of the services they are providing and the customer information you are sharing with them. For example, the Safeguards Rule requires you as a financial institution to implement access controls – including multi-factor authentication or something that is reasonably equivalent – for any individual accessing your information systems. 16 C.F.R. § 314.4(c)(5). If you are giving a service provider direct access to your network, they should be required to use multi-factor authentication for that access because they are individuals accessing your information systems. Likewise, the Safeguards Rule requires you as a financial institution to use encryption (or an effective compensating control) to protect all of your customer information both at rest and in transit. 16 C.F.R. § 314.4(c)(3). If

you are using a service provider to store and process customer information on your behalf, they should be required to encrypt that customer information as well.

10. If I do not "hold the paper" or take possession of customers' car loans, do I have a "continuing relationship" with the customer? If I no longer have a continuing relationship, does the Safeguards Rule still require me to protect the information received from the customer?

Yes. If your dealership arranges or brokers a loan for a consumer, then you are in a "continuing relationship" with that consumer for purposes of safeguarding the customer information they provided to you. The personally identifiable financial information the customer, or another financial institution, provided to you in order for you to arrange or broker the loan or financing is "customer information" subject to the Safeguards Rule. It remains customer information even after the end of the customer relationship (e.g., if you no longer hold the note) – in other words, you must continue to protect customer information that you obtained from a customer, even if they are no longer a customer, for as long as you have that customer information in your possession. You can securely dispose of the customer information at any point, however, and should do so once you no longer have a business need to keep it.