Moving the Metal: The Auto Finance Podcast — Driving Digital Security: The FTC's Safeguards Rule Explained
Hosts: Brooke Conkle and Chris Capurso
Guests: Kim Phan and Aileen Ng
Recorded: June 24, 2025
Aired: July 8, 2025

Brooke Conkle:

Welcome to *Moving the Metal*, the premier legally-focused podcast for the auto-finance industry. I'm Brooke Conkle, a partner in Troutman Pepper Locke's Consumer Financial Services Practice Group.

Chris Capurso:

I'm Chris Capurso, an associate in Troutman Pepper Locke's Consumer Financial Services Practice Group.

Brooke Conkle:

Today, we'll be talking about the Gramm-Leach-Bliley Act and the FTC's Safeguards Rule with our special guests, Kim Phan and Aileen Ng. Before we jump in, let me remind you to please visit and subscribe to our blogs. We have two great ones that may be of interest to you, TroutmanFinancialServices.com and ConsumerFinancialServicesLawMonitor.com. Also, we have a bevy of other podcasts that you might find interesting. *The Consumer Finance Podcast*, which, as you might guess, is all things consumer finance related. *The Crypto Exchange*, devoted to trends, challenges, and legal issues in Bitcoin, blockchain, FinTech, and regtech. *FCRA Focus*, a podcast dedicated to all things credit reporting. *Unauthorized Access*, a deep dive into the personalities and issues in the privacy, data, and cybersecurity industry. Finally, *Payments Pros*, a great podcast focused exclusively on the payments industry. All of these insightful shows are available on your favorite podcast platform, so check them out.

Speaking of those platforms, if you like what you hear, please leave us a review and let us know how we're doing. We'd love to hear from you. Alternatively, please feel free to reach out to us directly. Our contact information can easily be found on the firm's website, troutman.com. If you enjoy reading our blogs, or listening to our podcasts, please also check out our financial services mobile app. To download, simply go to your iOS or Android App Store and search for Troutman Pepper Locke. Not only does our app have all of our blog content and podcast episodes in one handy place, it also has a listing of the firm's financially focused attorneys. Check it out and see what you think.

For today, as I mentioned, we'll be discussing the FTC's Safeguards Rule with our colleagues Kim Phan and Aileen Ng. Kim and Aileen, welcome to *Moving the Metal*.

Kim Phan:

Thank you for having us.

Aileen Ng:

Thank you. It's my first time and I'm excited to be here.

Brooke Conkle:

Well, Aileen, can you give us some background on the Safeguards Rule? What is it and what makes it important?

Aileen Ng:

Sure. This is coming up now, because on June 16, 2025, the Federal Trade Commission, the FTC, published its frequently asked questions, FAQs, to help auto dealers comply with the Federal Gramm-Leach-Bliley Act Safeguards Rule. These new FAQs specifically cover auto dealerships and address auto dealers' relationships with OEMs, original equipment manufacturers, and other third-party vendors. Essentially, the Safeguards Rule sets standards and requirements for how covered businesses must develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for protecting customer information.

Just for some brief background, the FTC Safeguards Rule was issued in 2003 implementing a part of the Federal GLBA and requires covered financial institutions, which is defined broadly to mean any business engaged in financial activities covering auto financing and auto leasing, to maintain safeguards to protect customer information. Shortly after, in about 2005, the FTC actually published FAQs to address compliance with the GLBA's privacy rule, applicable to auto dealers. The privacy rule is a complement to the Safeguards Rule. The Safeguards Rule actually has remained unchanged for about 20 years, despite our rapidly evolving cyber environment. The rule was amended in 2021 to modernize its requirements.

Some of these updates include having a qualified individual oversee and implement the information security program, developing a written risk assessments and incident response plan, and adding more prescriptive security measures, such as encrypting customer information and requiring multi-factor authentication for anyone accessing customer information. Then in 2023, an amendment was made to require covered financial institutions, including auto dealers, to report data breaches and other security events directly to the FTC. This is for notification events, which is a defined term that was added involving the unauthorized acquisition of customer information involving at least 500 customers, whose information was unencrypted. This breach notification requirement became effective last year in May of 2024.

We see these amendments over the last four years to the Safeguards Rule significantly enhancing cybersecurity requirements for covered financial institutions, including auto dealers, auto lenders. We see the rule incorporating some of the latest standards and technologies to safeguard and protect customer information.

Chris Capurso:

Kim, because no podcast these days is complete without discussing the administration change, how is the FTC's approach in this guidance, which is obviously under the Trump administration, how does that differ from the Biden era FTC that issued the updates in the first place?

Kim Phan:

Well, I think you can see very starkly the contrast between how the two administrations are approaching working with businesses. Some of the key elements that you can observe from the press release that the FTC issued when publishing this guidance is written in a way that's very business friendly, right? The FTC says they're committed to providing certainty to the marketplace. I think that was secretly a little dig. The prior FTCs will know it when we see it approach of enforcement, that essentially, issuing regulation through its enforcement actions, only articulating what companies have done wrong with regards to data security after the fact, typically after a data breach. That's a clear contrast to the strict liability scenario we saw under a prior administration.

They also said they want to minimize the burden to legitimate business. I think the current FTC is much more aware and tuned to the challenges that small businesses face in implementing the many types of safeguards that Aileen already mentioned, multifactor authentication, very technical controls that can be hard for smaller entities to implement. They also said that they want to ensure that the rule keeps pace with technology. That had been one of the early criticisms of a more prescriptive Safeguards Rule.

If you put in place very specific safeguards as the technology moves on, they become obsolete, or they become a roadmap for bad actors to navigate around what measures you've put into place. I think there's a lot more consideration from the FTC under this current administration that you can see and how they're articulating the obligations that are now required under GLBA.

Brooke Conkle:

Aileen, how do auto dealers fit into this picture? Are they covered? If so, what information would they have that is implicated by the rule?

Aileen Ng:

Yeah. Again, financial institutions under the GLBA is defined quite broadly to cover any business engaging in financial activities. Auto dealers that finance, or facilitate the financing of, conduct leasing of vehicles are covered financial institutions under the Safeguards Rule. For example, extending credit through a retail installment contract. Auto dealers that lease vehicles for more than 90 days are covered, because leasing is also a financial activity. Auto dealers that provide financial advice or counseling are also subject to the rule.

On the types of information covered under the rule or records, this is any record containing non-public, personally identifiable financial information about the customer. For those in the auto industry, this might include a list identifying all customers who financed, or leased a vehicle from

you, the applications that were submitted and approved for financing or leasing, and that contain information, like Social Security numbers, financial account information. The FAQs do clarify certain types of records that do not qualify as covered customer information. For example, a general list of names and addresses of all vehicle buyers in a given month would not qualify as customer information, because there's no information about financing, or leasing regarding that customer.

This includes also, a list of names that I've been collected to share with OEMs to send out recall notices, for example. Same with retail delivery reports, that include name addresses and VIN numbers. If there's no indication about whether the customer financed, or leased their vehicle, it is not covered. Same with general sales data reports, or other aggregate information about vehicle sales, also service or maintenance records about the vehicles, also not considered customer information.

Chris Capurso:

Kim, Aileen has mentioned OEMs a couple times. How does the safeguard rule apply to the relationship between auto dealers and OEMs?

Kim Phan:

Well, Chris, unfortunately, I'm going to have to give you the classic attorney answer. It depends. You have to assess the nature of the relationship between the dealer and the OEM. As we know, and I'm sure Brooke and you have already talked about on many prior podcasts, there's lots of different formulations about how these two different types of entities may interact with each other. In some cases, OEMs just provide inventory, right? Like, here are the cars, go sell them.

In other cases, there's a much deeper relationship, where an OEM may be providing additional services to the dealers, not just the inventory. For example, they may make available a CRM, customer relations management platform for the dealers to use. If that's the case, the auto dealers as financial institutions, if they're subject to this rulemaking, as Aileen was just describing, they are required to oversee the OEMs as their service providers. If the OEMs were providing additional services, all of the requirements of the safeguard rule with regard to oversight of service provider applies, meaning appropriate due diligence on the front-end, ensuring there's certain contractual language, as well as providing certain oversight, such as monitoring, auditing, that sort of thing.

However, even in the scenario where the relationship is just the OEM provides inventory of cars, there may still be additional requests for information that the OEMs may make of the dealers. For example, they may have a legitimate business purpose to say, “Hey, look, we want to keep track of your sales records to see how many of our vehicles you've been moving,” or for recall purposes. Or they may want to have delivery reports of how many vehicles arrived and how many got shipped out.

As long as those lists that the dealers are providing back to the OEMs are general in nature, right, this is how many of all vehicles we have sold, and have no indicators at all, whether or not the vehicle was sold for cash, sold with a financing option, or at least in some way, that's what

would trigger the application of the Safeguards Rule, if there's some financial data involved. Even in that case, where they're sending some information about the nature of the purchase, it was financed, it was leased, or some other scenario, if the OEM is directly at accessing, say, the CRM platform that they're providing, or they're otherwise have direct access to the auto dealer database, then the dealership has to have all these safeguards in place, the multi-factor authentication, segregating only that data the OEMs actually need and not all of the financing data. Logging the activity of any OEM authorized users.

In other scenarios, dealers might just be emailing the OEMs this data. If that's the case, they really should be doing something like a secure email, or sending it through an API, or something along those lines. Again, anything that has financial, non-public, personal information that is subject to the Gramm-Leach-Bliley Act, they need to be thoughtful about how this information is being relayed back and forth between the dealers and the OEMs.

Brooke Conkle:

Aileen, tell us a little bit about the notification requirements if there's a data breach.

Aileen Ng:

Yeah. Thanks, Brooke. As I mentioned earlier, the Safeguards Rule was amended in 2023 and became effective last year in May of 2024 to require covered financial institutions, including auto dealers, to directly notify the FTC of a data breach involving 500 or more customers, as soon as possible, but no later than 30 days after discovery of the breach.

Again, this specifically applies to a notification event, which is a defined term. Meaning a security breach involving the unauthorized acquisition of at least 500 customers' unencrypted information. Now, if the encryption key was also accessed during the breach, then this notification requirement also applies with respect to encrypted customer information. The date of discovery of the notification event is the first day that the event is known to the auto dealer, its employees, officers, or other agents. There is a knowledge standard here written within the rule for when that 30-day notification begins to run.

Chris Capurso:

Aileen, to follow up on that, how do the data breach notification requirements and the Safeguards Rule in general, how does all of this apply to service providers?

Aileen Ng:

Yeah, so the Safeguards Rule actually includes service provider as a defined term, unlike the GLBA privacy rule. There is an obligation for covered financial institutions, including auto dealers to have oversight over service providers, including in the event of any data breach, and that would also trigger reporting requirements as an agent of that covered financial institution.

Now, for in general, auto dealers covered financial institutions are required to conduct appropriate due diligence when selecting and retaining service providers to make sure that

they're capable of maintaining these safeguards. A good part of these newly released FAQs are dedicated to addressing this service provider relationship with auto dealers. This includes service providers must contractually agree to implement and maintain these safeguards, and auto dealers must periodically assess service providers based on the risk they present and the continued adequacy of the safeguards that they're using.

When a covered financial institution gives access to customer information to a service provider, the financial institution must monitor those safeguards. Regarding who qualifies as a service provider, the FAQs actually go into quite a bit of detail about this, because as I mentioned, a service provider is a defined term in the Safeguards Rule and not in the privacy rule. Essentially, a service provider is permitted to access customer information through its provision of services directly to a covered financial institution.

As an example, the FAQs expressly state that an OEM is not a service provider, unless it is providing direct services to a financial institution. That is, an OEM does not become a service provider simply because information is shared with them. In the recall notices example, a financial institution that shares names and addresses with an OEM to send recall notices in the future is not providing the financial institution a service and thus, is not a service provider.

If a financial institution shares a database of names and addresses combined with information. So, to oversee service providers, this Safeguards Rule has three main requirements for covered financial institutions. One, taking reasonable steps to select and retain service providers capable of maintaining safeguards. Two, requiring service providers to contractually agree to implement and maintain the safeguards. Three, periodically assessing the service providers based on the risk they possess.

This means that not all service providers are required to comply with all the requirements contained in the Safeguards Rule. The rule allows flexibility in how a financial institution oversees their service providers based on the size and complexity of the financial institution and the nature of the services provided by the service provider.

For example, a marketing company that has direct access to a covered financial institution's customer database versus a paper shredding company to dispose of records. The safeguards that the financial institution would require of each company would be quite different. The financial institution would not need to take measures to oversee the shredding company's network, because it does not have access to the database and network systems of the financial institution. For the marketing company who has access to the customer database, it would then be appropriate for the financial institution to require, for example, multi-factor authentication to gain access to that database.

Brooke Conkle:

Kim, there are a lot of different ways that auto dealers establish financing relationships. Some are financing directly through retail installment contracts. Some are providing financing and then selling the loans to third parties. Others are brokering loans. How does this Safeguards Rule apply in these various scenarios?

Kim Phan:

I definitely don't envy you and Chris, the hosting of this podcast, because as we've heard already, there's all kinds of different OEM relationships. There are all different kinds of service provider relationships. Now, there's all these different financing scenarios that auto dealers may be implementing. Something to keep in mind for the auto dealers listening to this podcast, we've talked a lot about what their actual requirements are under the Safeguards Rule, but here's a helpful tip. The safeguard rule applies only to customers as defined under the Gramm-Leach-Bliley Act. The GLBA is one of those statutes that draws a line between consumers, which is a broad category. Everyone is a consumer who's shopping for a car. A customer is only those individuals who actually enter into a financing arrangement. So, agree to a auto loan, usually a retail installment contract through a RIC, as they sometimes call through the auto dealer, or maybe through a leasing arrangement for that vehicle.

If a dealer is simply referring someone to an external lender, such as giving them a link and the person has to go to that lender's website and enter in all their information and apply and agree to a financing relationship separately, that's only a consumer relationship with the dealer. There is no customer relationship and the Safeguards Rule does not apply. Now, if a customer relationship is formed, meaning that the actual auto dealership is performing some sort of financial activity, like brokering a loan, accepting the application to issue a RIC, enter into the actual RIC agreement, and they are the line lender for the purposes of that loan. If that customer relationship is established, that's when the Safeguards Rule is triggered, and all of the obligations that we've discussed about on this podcast would then apply.

Keep in mind that even those dealers that may enter into a RIC with a customer and then has plans to immediately sell that loan to a third-party lender, any information that dealer collected from that customer, meaning the application, the issuing of the signed agreement, no matter how brief that customer relationship, and sometimes we're talking about days or minutes before it's resold to a third party, it doesn't matter. The Safeguards Rule once triggered, will continue to apply to that customer's non-public personal information held by the dealer.

But if the dealer wants to minimize their risks under the Safeguards Rule, the safeguard rule does not require that they keep any of that customer data. They can delete it immediately, subject to whatever legal, or business purposes they may have for that data, like auditing or some such. At a minimum, they have to delete it within two years after the last date the information was used in connection with that auto loan, or lease. There are ways that a dealer can minimize their obligations and risks under the Safeguards Rule. That's want to make sure to end on a bright note for them.

Chris Capurso:

That is a bright note to end on. We usually don't get really bright notes to end on, so that's great. With that, we'll wrap it up for today's podcast. Thank you to our audience for tuning in. We also want to thank Kim and Aileen for joining us. Don't forget to check out our blogs where you can subscribe to the entire blog, or just the specific content you find most helpful. That's the ConsumerFinancialServicesLawMonitor.com, and the TroutmanFinancialServices.com blogs. You can also check out our podcast at those blogs, including *FCRA Focus*, which is co-hosted by Kim. While you're at it, why don't you head on over to troutman.com and sign up for our

Consumer Financial Services mailing list, so that you can stay abreast of current issues, with our insightful alerts and advisories, and receive invitations to our industry insider webinars.

Of course, please mark your calendars for this podcast, *Moving the Metal*, which we will be releasing every two weeks in 2025. That'll generally be on the second and fourth Tuesdays of each month. As always, if you have any questions, or if we can help in any way, please reach out to us. Until next time.