News FROM IIADA

September 22

Administrative Office.
P.O. Box 356
West Branch, IA 52358

Phone 319-643-5403

Fax: 319-643-5403

Email:iiada2@netins.net

Auction News

Dealer's Choice AA
www.dcaa.com

Plaza Auto Auction
www.plazaaa.com

Tri-State AA – Cuba City
www.tsaaonline.com

Manheim Omaha AA
www.manheim.com

Adesa Des Moines
www.adesa.com

Manheim-Minneapolis-MAA
www.manheim.com

Manheim Northstar
www.manheim.com

Des Moines Auto Auction
www.dsmaa.com

SUPPORT FOR THE MIDWEST AUTO AUCTIONS IS GREATLY APPRECIATED.

Dealer Education Classes for October

October 4, 2022 - Tuesday Hawkeye Community College ZOOM 09:00AM - 02:00PM

October 6, 2022 - Thursday Northeast Iowa Community College **Calmar** 12:00PM - 05:00PM

October 7, 2022 - Friday Northeast Iowa Community College **Cresco** 09:00AM - 02:00PM

October 11, 2022 - Tuesday Kirkwood Community College **Cedar Rapids** 09:00AM - 02:00PM

October 13, 2022 - Thursday Des Moines Area Community College South Ridge **Des Moines** 09:00AM - 02:00PM

October 18, 2022 - Tuesday North Iowa Area Community College ZOOM 09:00AM - 02:00PM

October 19, 2022 - Wednesday Western Iowa Tech Community College **Sioux City** 09:00AM - 02:00PM

October 20, 2022 - Thursday Northwest Iowa Community College **Sheldon** 09:00AM - 02:00PM

October 21, 2022 - Friday Iowa Lakes Community College **Emmetsburg** 09:00AM - 02:00PM

October 26, 2022 - Wednesday Des Moines Area Community College ZOOM 09:00AM - 02:00PM

October 27, 2022 - Thursday Southeastern Community College **Burlington** 12:00PM - 05:00PM

October 28, 2022 - Friday Indian Hills Community College **Ottumwa** 09:00AM - 02:00PM

October 31, 2022 - Monday Kirkwood Community College ZOOM 09:00AM - 02:00PM

IOWA INDEPENDENTAUTOMOBILE DEALERS ASSOCIATION

https://www.iowaiada.com/5-hour-dealer-education

On-Line Dealer Education Manual

To search within the document: "Control+F" (or "Command+F" on a Mac) is the keyboard shortcut for the Find command. If you're in a document or in a web browser, pressing the Ctrl key + the F key will bring up a search box in a corner of the screen. You can then type in a keyword or phrase to find places where that word or phrase is used in the text, often helpful for locating relevant sections.

SR-22 insurance stops and the impact on dealers

Here is the link to the website where customers may enter their information, including driver's license number, to see if any restrictions exist: https://mymvd.iowadot.gov/Account/Login

HOW WILL DEALERS BE IMPACTED FOR INITIAL TITLE AND REGISTRATION APPLICATIONS?

If a dealer submits a title and registration application on behalf of a customer that has an unresolved SR-22 stop, the county will return the paperwork to the dealer and state that the customer is ineligible to title and register the vehicle. The county may let the dealer know that the deal is being returned due to an initial title and registration stop, and that the customer should contact the DOT or the county treasurer for information of how to resolve the transaction. The county may also let the dealer know that to perfect a security interest for the untitled vehicle may submit Form 411046, the Application for Notation of Security Interest, with the applicable fee to the county treasurer. The county has a procedure to process the security interest without issuing a title.

A dealer who has a Power of Attorney for a customer with an SR-22 stop will be unable to title and register on the customer's behalf.

Any customer who has a delay in submitting a title application due to an SR-22 issue may be subject to title and registration penalties if the application is not ultimately submitted within 30 days of acquiring the vehicle. The county treasurer's office will determine the receipt date of the application and apply penalties if required.

HOW WILL LIENHOLDERS BE IMPACTED?

MVD is aware that one purpose in securing a title is to ensure that a security interest (or "lien") is perfected. Iowa Code 321.50 specifies that the date of delivery of the application for notation of security interest or of delivery of the application for certificate of title which lists the security interest shall be the date of perfection for the lien, regardless of the date of the title. The lien application is Form 411046, the Application for Notation of Security Interest, and the applicable fee.

ARE THERE PROCESSES A DEALER CAN ADOPT PRIOR TO THE MOTOR VEHICLE SALE TO IDENTIFY IF A CUSTOMER MAY BE UNABLE TO TITLE AND REGISTER A VEHICLE DUE TO AN SR-22 STOP?

Yes, there are a few options to identify prior to the sale if an SR-22 stop may keep a vehicle from being titled and registered in the customer's name:

1. The revocation or suspension of a driver's license may mean the driver's license was surrendered or taken and the customer will be unable to provide the driver's license. This may be helpful information for a dealer as well while a dealer is conducting a test drive. There are additional reasons a customer may not have a valid driver's license and would caution it should not be assumed that a person without a driver's license necessarily has an SR-22 stop.
2. If the customer has a driver's license, the driver's license may have an S restriction and state on the back of the driver's license that the S restriction relates to an SR-22 requirement. The S restriction means the SR-22 is on file with the DOT but it may not cover this class of vehicle (such as a motorcycle SR-22 would not cover a passenger vehicle SR-22) and in any event would need to be updated with the newly-purchased vehicle's information within 30 days of purchase.
3. The customer may input their driver's license information at the following website to see if there is a restriction on the driver's license: https://mymvd.iowadot.gov/Account/Login?ReturnUrl=%2fCompliance
4. The dealer may contact the DOT Driver's License Info Center or email driver.services@iowadot.us for the customer's driver's license status. The dealer will need to provide the customer's name and DL number.

Why the new FTC provisions would hurt dealers and the car buying experience – Brett Scott, NIADA

The National Independent Automobile Dealers Association (NIADA) says that a recently proposed rule by the Federal Trade Commission "would place extensive restrictions on the sale, financing, and leasing of motor vehicles." Today on Inside Automotive, we're pleased to welcome Brett Scott, Vice President of Government Affairs for the National Independent Automobile Dealers Association, to share the concern they're hearing from dealers and what action the association plans to take.

When Scott came into his role as Vice President of Government Affairs last year, one of his top priorities was to ensure that NIADA members had the opportunity to get a seat at the table with Washington's regulatory heavy-hitters. Since last January, the NIADA has held multiple successful meetings with Federal regulators.

One of the most significant problems Scott sees with the proposed restrictions is their vagueness of scope. In order to be an NIADA member, dealers must already follow strict guidelines regarding vehicle purchasing transparency and online car buying. According to Scott, these rules would "add redundancy" and potentially make the car process less efficient.

The proposal aims to effectively ban the use of bait-and-switch claims, fraudulent or surprise junk fees (including gap insurance,) and would require the full upfront disclosure of cost and conditions. The new rules would create three times as much paperwork, Scott says.

Along with other automobile associations, the NIADA and its members will submit comments to FTC regarding this matter. If you would like to submit a comment, visit the Federal Register here. Other ways you can make your voice heard are by getting involved with your state association or the National Automobile Dealers Association.

FTC Safeguards Rule: What Your Business Needs to Know

Tags:

Finance

Privacy and Security

Data Security

Gramm-Leach-Bliley Act

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. The Safeguards Rule took effect in 2003, but after public comment, the FTC amended it in 2021 to make sure the Rule keeps pace with current technology. While preserving the flexibility of the original Safeguards Rule, the revised Rule provides more concrete guidance for businesses. It reflects core data security principles that all covered companies need to implement.

This publication serves as the small entity compliance guide under the Small Business Regulatory Enforcement Fairness Act. Your best source of information is the text of the Safeguards Rule itself.

In reviewing your obligations under the Safeguards Rule, consider these key compliance questions.

Who's covered by the Safeguard Rule?

The Safeguards Rule applies to financial institutions subject to the FTC's jurisdiction and that aren't subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6805. According to Section 314.1(b), an entity is a "financial institution" if it's engaged in an activity that is "financial in nature" or is "incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C § 1843(k)."

How do you know if your business is a financial institution subject to the Safeguards Rule? First, consider that the Rule defines "financial institution" in a way that's broader than how people may use that phrase in conversation. Furthermore, what matters are the types of activities your business undertakes, not how you or others categorize your company.

To help you determine if your company is covered, Section 314.2(h) of the Rule lists 13 examples of the kinds of entities that *are* financial institutions under the Rule, including mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that aren't required to register with the SEC. 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.

Section 314.2(h) of the Rule lists four examples of businesses that *aren't* a "financial institution." In addition, the FTC has exempted from certain provisions of the Rule financial institutions that "maintain customer information concerning fewer than five thousand consumers."

Here is another key consideration for your business. Even if your company wasn't covered by the original Rule, your business operations have probably undergone substantial transformation in the past two decades. As your operations evolve, consult the definition of financial institution periodically to see if your business could be covered now.

What does the Safeguards Rule require companies to do?

The Safeguards Rule requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. The Rule defines customer information to mean "any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates." (The definition of "nonpublic personal information" in Section 314.2(l) further explains what is – and isn't – included.) The Rule covers information about your own customers and information about customers of other financial institutions that have provided that data to you.

Your information security program must be written and it must be appropriate to the size and complexity of your business, the nature and scope of your activities, and the sensitivity of the information at issue. The objectives of your company's program are:

- to ensure the security and confidentiality of customer information;
- to protect against anticipated threats or hazards to the security or integrity of that information; and

to 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.

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.

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.

The FTC more information about the Safeguards Rule and general guidance on data security.

GLOSSARY

Here are some definitions from the Safeguards Rule. Consult 16 C.F.R. § 314.2 for more definitions.

Authorized user means any employee, contractor, agent, customer, or other person that is authorized to access any of your information systems or data.

Customer information means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

Encryption means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.
Financial institution means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C § 1843(k). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.

Information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
Information system means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.
Multi-factor authentication means authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; (2) Possession factors, such as a token; or (3) Inherence factors, such as biometric characteristics.
Nonpublic personal information means: (i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
Penetration testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.
Security event means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.
Service provider means 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.
May 2022

To help you determine if your company is covered, Section 314.2(h) of the Rule lists 13 examples of the kinds of entities that *are* financial institutions under the Rule, including mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that aren't required to register with the SEC. 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. Section 314.2(h) of the Rule lists four examples of businesses that *aren't* a "financial institution." In addition, the FTC has exempted from certain provisions of the Rule financial institutions that "maintain customer information concerning fewer than five thousand consumers."

Here is another key consideration for your business. Even if your company wasn't covered by the original Rule, your business operations have probably undergone substantial transformation in the past two decades. As your operations evolve, consult the definition of financial institution periodically to see if your business could be covered now.

What does the Safeguards Rule require companies to do?

The Safeguards Rule requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. The Rule defines customer information to mean "any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates." (The definition of "nonpublic personal information" in Section 314.2(l) further explains what is – and isn't – included.) The Rule covers information about your own customers and information about customers of other financial institutions that have provided that data to you.

Your information security program must be written and it must be appropriate to the size and complexity of your business, the nature and scope of your activities, and the sensitivity of the information at issue. The objectives of your company's program are:

- to ensure the security and confidentiality of customer information;
- to protect against anticipated threats or hazards to the security or integrity of that information; and

to 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?

FTC Safeguards Rule for Auto Dealerships

In October, 2021, the FTC issued its final amendments to the FTC Safeguards Rule. The Rule contains a significant number of new and expanded procedural, technical, and personnel requirements that auto dealerships must comply with by December 9, 2022.

The Safeguards Rule ("Rule) is a federal data security rule that requires auto dealers to have measures in place to keep customer information secure. Auto Dealers are required to develop their own safeguards. Dealers are responsible for taking steps to ensure that their service providers and affiliates comply with following rules:

Rule 1 - Qualified Individual - 16 CFR 314.4(a)

Auto Dealers must designate a qualified individual responsible for overseeing, implementing, and enforcing your information security program.

Rule 2. Written Risk Assessment - 16 CFR 314.4(b)

Requires that a new Risk Assessment document be created, which identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. A written risk assessment must be completed initially and on a periodic basis after that.

Rule 3: Access Controls- 16 CFR 314.4(c)(1)

Requires dealers to implement and periodically review access controls

Rule 4: Data and Systems Inventory - 16 CFR 314.4(c)(2)

Auto Dealers must identify and manage the data, personnel, devices, systems, and facilities that enable the dealership to achieve business purposes in accordance with their business objectives and risk strategy.

Rule 5: Data Encryption - 16 CFR 314.4(c)(3)

Encrypt all customer information held or transmitted by auto dealerships both in transit over external networks and at rest.

Rule 6: Secure Development Practices - 16 CFR 314.4(c)(4)

Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;

R

Rule 7: Multi-Factor Authentication - 16 CFR 314.4(c)(5)

Auto dealers must implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;

Rule 8: Secure Data Disposal Procedures - 16 CFR 314.4(c)(6)

Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained and periodically review your data retention policy to minimize the unnecessary retention of data;

Rule 10: Change Management Procedures - 16 CFR 314.4(c)(7)

Auto Dealers must adopt procedures for change management which govern the addition, removal, or modification of elements of an information system.

Rule 11: Systems Monitoring & Logging - 16 CFR 314.4(c)(8)

Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

Rule 12: Intrusion Detection - 16 CFR 314.4(d)(1)

Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

Rule 13: Continuous Monitoring/ Periodic Penetration Testing & Vulnerability Assessments - 16 CFR 314.4(d)(2)

For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:

Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and 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.

Rule 14: Security Awareness Training - 16 CFR 314.4(e)

Implement policies and procedures to ensure that personnel are able to enact your information security program by:

Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;

Providing information security personnel with security updates and training sufficient to address relevant security risks; and

Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

Rule 15: Oversee Service Providers - 16 CFR 314.4(f)

Oversee service providers, by:

Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;

Requiring your service providers by contract to implement and maintain such safeguards; and

Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

Rule 16: Periodic Review of Security Program - 16 CFR 314.4(g)

Evaluate and adjust your information security program in light of the results of the testing and monitoring; any material changes to your operations or business arrangements; the results of risk assessments performed; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

Rule 17: Written Incident Response Plan - 16 CFR 314.4(h)

Auto dealers must adopt a written incident response plan that is specifically designed to promptly respond to, and recover from any security event materially affecting the confidentiality, integrity, or availability of customer information in dealership control.

Rule 18: Annual Report to Board - 16 CFR 314.4(i)

Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such a report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:

The overall status of the information security program and your compliance with this part;

Material 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

AutoJini can help meet Safeguard Rule requirements

AutoJini/Octadyne Systems, Inc. has been providing IT services for 20+ years. We have worked with our technology providers to provide a complete solution which will help your dealership to comply with FTC Safeguard Rule. Please call us at 1-877-460-0255 or email sales@autojini.com for more information.

#	Rule	AutoJini	MDR	Dealership
1	Qualified Employee			x
2	Written Risk Assessment	x		
3	Access Controls	x		
4	Data and Systems Inventory	x		
5	Data Encryption	x		
6	Secure Development Practices	x		
7	Multi-Factor Authentication	x		
8	System Monitoring & Logging	x		

AutoJini

Phone: (515) 232-2024

sales@octadyne.com Contact AutoJini For addition information.

9	Secure Data Disposal Procedures	x		
10	Change Management Procedures	x		
11	Systems Monitoring & Logging		x	
12	Intrusion Detection		x	
13	Continuous Monitoring/ Periodic Penetration Testing & Vulnerability Assessments		x	
14	Security Awareness Training	x		
15	Oversee Service Providers	x		
16	Periodic Review of Security Program	x		
17	Written Incident Response Plan	x		
18	Annual Report to Board			x

AutoJini

Phone: (515) 232-2024

sales@octadyne.com Contact AutoJini For addition information.

What's Old Is New Again — The FTC's 1975 Mail, Internet, or Telephone Order Merchandise Rule Is Popular Once More

By Eric L. Johnson*

If you're lucky to live long enough, you may get to see the "old" things that were popular in your youth come back around and turn "new" again. Much to my wife's chagrin, I've hit the point in my life where those polo shirts with the stand-up collars that I wore in the '80s are finally coming back into style again. I've been telling her for years that there was a reason to hang on to them!

The concept of something old that's become new again was recently highlighted by an alert from the National Automobile Dealers Association in connection with the Federal Trade Commission's Mail, Internet, or Telephone Order Merchandise Rule.

Let's start with the old. This rule has been around since 1975. Originally, it was written and issued to cover just orders through the mail. However, it was amended in 1993 to include telephone orders and again in 2014 to include Internet orders.

Now, if you're not familiar with the rule, it requires sellers who solicit buyers to order merchandise through the mail, by phone, or via the Internet to make disclosures to the buyers regarding the shipment time for the ordered merchandise. Historically, the rule generally hasn't been relevant to dealers. However, much like my old polo shirts, what's old is new again, and there may be some life left in this old rule after all. Dealers are faced with the perfect storm of a chip shortage that's caused delays on the delivery of new vehicles, more dealers are engaging in remote delivery of vehicles, and dealers are increasingly accepting reservations for vehicle orders.

So, what does the rule require? Well, when you advertise merchandise (like a vehicle) that can be ordered by a buyer over the phone or the Internet for shipment to that buyer, you must either state when the merchandise will be delivered or have a reasonable basis for believing that you can ship the merchandise within 30 days of a completed order. This is sometimes called the "30-day rule." If a shipment is delayed and you learn that you can't ship the merchandise within the time you said you would or within 30 days, then you must either get the customer's consent to a delayed shipment or promptly refund all the money the customer paid. A customer's silence on this first notice may be treated as a consent to delay. You can notify the customer via telephone, fax, mail, or email as long as you notify the customer of the delay reasonably quickly.

Also, whenever you change the shipment date by providing a notice of the delay, you must have a reasonable basis for the new shipment date or a representation that you don't know when you can ship the merchandise.

To top it off, the rule provides that you bear the burden of showing that you're complying with the rule. Therefore, keeping good records of your compliance is a must. Records may include each individual order showing the date you received the order, the contents of and date you provided any delay option notice, the date you received any customer cancellation, the date of any shipment and the merchandise shipped, and the date of any refund and the merchandise for which the refund was made.

Even though this is an old rule with little enforcement activity, the FTC recently announced enforcement actions against two companies that the FTC claimed violated the rule in their marketing of certain personal protective equipment during the height of the pandemic. Violation of the rule constitutes an unfair method of competition and an unfair or deceptive act or practice. If you violate the rule, you can be sued by the FTC for injunctive relief, penalties of up to $46,517 per violation, and consumer redress. The FTC won its lawsuits against both entities on motions for summary judgment and added $3.08 million from one seller and $14.6 million from the other to its coffers to use for consumer refunds.

The FTC is serious about enforcing its rules, and dealers have been in its crosshairs recently, so you need to take this rule seriously. Fortunately, the FTC has a fairly robust, free, and easy-to-read Business Guide to the rule. You should download or print that guide and get it in front of your lawyer ASAP to see if the rule could apply to you or your dealership's operations. You don't want to be the FTC's next target.

Now, where did I put those '80s hair band concert t-shirts?

***Eric L. Johnson** is a partner in the Oklahoma office of Hudson Cook, LLP. He can be reached at 405.602.3812 or by email at ejohnson@hudco.com.

Auction News

Adesa – Sioux Falls

www.adesa.com.

Manheim Kansas City

www.manheim.com

Greater Rockford AA

www.graa.net

Quad City Auto Auction

www.qcaa.com

Lincoln Auto Auction

www.lincolnautoauction.com

IIADA EVENTS:

2020 Annual Meeting

TBA - 2020

NIADA EVENTS:

June 15-18, 2020

NIADA Convention

Las Vegas – MGM Grand

KEEP US INFORMED

DON'T FORGET TO LET IIADA KNOW IF YOUR E-MAIL, ADDRESS OR PHONE NUMBER CHANGES