TADA
Texas Automobile Dealers Association

1108 Lavaca, Suite 800
Austin, TX 78701
512-476-2686
www.tada.org

To: TADA Members
From: Karen Phillips
Date: April 22, 2022
Re: FTC Final Rule
"Safeguards Rule"

MEMORANDUM

Background

Standards for Safeguarding Customer Information
(16 CFR Part 314)

The Federal Trade Commission (FTC) amends the Standards for Safeguarding Customer Information, a/k/a "Safeguards Rule,"[1] by adding requirements for a more specific security program that is based on the dealership's risk assessment and incorporates requirements such as controlling access to customer information, multi-factor authentication and encryption, among other requirements as discussed below.

Congress enacted the Gramm Leach Bliley Act in 1999. The Act includes a requirement that a financial institution, which includes a dealership, provide customers with information about their privacy practices and implement security safeguards to protect the security, confidentiality, and integrity of customer information.

The FTC adopted the Safeguards Rule, effective May 23, 2003; however, the new amendments (86 FedReg 70,0062 - 70,067 (*Proposed*), 70,272-70,308 (Adopted)) give specific and more detailed requirements for a financial institution's information security program.

---

[1] 16 CFR Part 314; Public Law 106-102, 113 Stat 1338 (1999); *See* 15 U.S.C. 6801(b); 15 U.S.C. 6805(b)(2).

A review of the earlier Safeguards Rule with a template for a written comprehensive information security program (WISP) and red flags requirements can be found on the TADA website:

1. Go to www.tada.org
2. On the Legal/Regulatory drop down tab, choose "FTC Red Flags Webinar."
3. Sign in as required. If you do not recall your login/password, please contact Janet Hale at jhale@tada.org

To become familiar with the *new* requirements, please review this summary of the new requirements as outlined below.

Definitions that are specific to the Safeguards Rule are included for your reference and are available on **pages 9-12.**

EFFECTIVE DATE

(16 CFR § 314.5)

The rule is effective January 10, 2022.

A delayed effective date of December 9, 2022, includes:

- Appointing a Qualified Individual (§ 314.4(a))
- Conducting a written risk assessment (§ 314.4(b)(1))
- New elements of the information security program (§ 314.4(c)(1)-(8))
- Requiring continuous monitoring or annual penetration testing and biannual vulnerability assessment (§ 314.4(d)(2))
- Requiring training for personnel (§ 314.4(e))
- Requiring periodic assessment of service providers (§ 314.4(f)(3))
- Requiring a written incident response plan (§ 314.4(h))
- Requiring annual written reports from the Qualified Individual (§ 314.4(i))

Current compliance requires:

- Regular testing or monitoring of the effectiveness of current safeguard controls, systems, or procedures (§ 314(d)(1))
- Overseeing service providers by taking steps to select, retain, and require specific contractual terms (§ 314.4(f)(1)-(2))
- Adjust the dealership's information security program after reviewing the testing and monitoring (§ 314.4(g))
- Periodic written risk assessments (§ 314.4(b)(2))

Purpose and Scope
(16 CFR § 314.1)

The Safeguards Rule applies to **all** customer information in the dealership's possession, including information from individuals that the dealership has a customer relationship as well as with customer information provided to the dealership from other sources.

STANDARDS for Safeguarding Customer Information
(16 CFR § 314.3)

The information security program must include the **ELEMENTS** discussed below (*See* § 314.4) and achieve the following objectives:

1. Insure the security and confidentiality of customer information.
2. Protect against any anticipated threats or hazards to the security or integrity of customer information.
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

ELEMENTS of the Information Security Program

(16 CFR § 314.4)
The new Final Rule provides that a dealership's information security program consist of the following elements:

I. Designate a Qualified Individual

(§ 314.4(a))

This person is responsible for overseeing and implementing the dealership's information security program and enforcing the program.

The Qualified Individual may be an employee, an affiliate, or a service provider.

If using a service provider, the dealership shall:

1. Retain responsibility for compliance;
2. Designate an employee for oversight; and,
3. Require that the information security program protects the dealership.

II. Written risk assessment

(§ 314.4(b))

- (1) The information security program is based on a written risk assessment

that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in unauthorized disclosure, misuse, alteration, destruction, or other compromise of customer information.

■ (2) Periodically perform risk assessments that re-examine the 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 customer information.

III. <u>Implement safeguards to control the risks</u> identified in the risk assessment. (§ 314.4(c))

1. **Control the Access on All Customer Information**–electronic <u>and</u> paper
   - **Limit** to authorized users.
   - **Restrict** employee access to information needed to perform duties.
   - **Restrict** vendor access to information necessary to perform required duties/functions.
2. **List Data Inventory & Classification**
   - Inventory customer information–where it is kept and how it can be accessed.
   - Inventory systems on which data is collected, stored, or transmitted.
3. **Encrypt Customer Information**
   - In transit over external networks; and,
   - At rest, i.e., data that is stored for later retrieval.
   - This requirement includes dealership's **<u>and</u>** employee's smartphones, ipads, and computers which contain any customer information.
4. **Secure Dealership's Development Practices**
   - Verify that internal and external applications used to handle customer information are secure.
   - Request and review security test results of third-party software providers.
5. **Multi-Factor Authentication**
   - Required whenever **<u>any</u>** individual accesses any dealership information system–includes employees, customers, vendors.
   - May adopt equivalent controls if the Qualified Individual

approves.

6. **Information Disposal Procedures**
   - Securely dispose of customer information.
   - **Immediately dispose of customer information on dealership's loaner vehicles, rental vehicles, and WiFi.**
   - Retain customer information as required by law or regulation, or as necessary for business operations; otherwise, securely dispose of it within 2 years after the last date it is *used* in connection with a product or service to the customer.
7. **Managing Change Regarding Dealership Information System**
   - If making additions to the information system, develop procedures to assess the security of devices, networks, and other items relating to the information system.
   - Develop procedures to assess the impact of removing items or revising the information system.

   EX: Is the dealership changing vendors relating to the information system? This change requires an evaluation to assess the security of the new system including written risk assessment.
8. **System Monitoring**
   - Log user activity.
   - Implement policies & procedures to monitor the activity of authorized users and detect unauthorized access or use or tampering with customer information by users.
   - Limit access to electronic records **and** paper records.

IV. Regularly test or monitor the effectiveness of the safeguards' controls, systems, and procedures, including those safeguards to detect actual and attempted attacks or intrusions into the information systems.
(§ 314.4(d)(1))

- **Test Information Systems**
  - Perform a vulnerability assessments at least once every 6 months and whenever there are material changes to systems.
  - Perform a vulnerability assessment whenever circumstances may have a material impact on the information security program.
- **Incident Response**
  - **General employee training**

- Provide personnel with security awareness training that is updated to reflect risks identified by the risk assessment.
  EX: Pfishing

• Use qualified information security personnel.
- Ensure security personnel are qualified for their positions and adequately staffed.
- A service provider can satisfy this requirement.

• Specific training for information security personnel.
- Changing nature of threats on information systems for which they are responsible.
- Service provider may meet information security needs–should include assurances that personnel are trained in current security practices.

• Verify that security personnel are taking steps to maintain current knowledge on security issues.
- Continuing education on recent developments.
- Required security research.
- Annual assessment of knowledge of threats related to the information system.

V. SERVICE PROVIDER OVERSIGHT

(§ 314.4(f))

• REQUIRE SERVICE PROVIDERS, BY CONTRACT, TO IMPLEMENT AND MAINTAIN SAFEGUARDS

EX: Insurance companies; service contract companies; OEMs; financial institutions.

• Periodically assess service providers based on:

1. The risk they present; and,
2. The continued adequacy of their safeguards.

VI. Evaluate & Adjust Information Security Program

(§ 314.4(g))

• After required testing, if there are material changes to the operations or business that have a material impact on the information security program, amend the information security program accordingly.

VII. Written Incident Response Plan[2]

(§ 314.4(h))

- Develop and implement a written incident response plan.
- Plan should address security events that materially affect the confidentiality, integrity, or availability of customer information in the dealership's control.
- State lines of responsibility.
- Include:
    1. Goals of the plan.
    2. The internal process for responding to a security event.
    3. The definition of roles, responsibilities and levels of decision-making authority.
    4. External and internal communications and information sharing.
    5. Identify requirements for the remediation of any identified weaknesses in the information systems and associated controls.
    6. Document and report security events and related incident response activities.
    7. Evaluate & revise, if necessary, the incident response plan following a security event

VIII. Notify FTC of Security Events

(314.4(j)) (86 FedReg 70062 (*Proposed*)) Expected to be adopted as proposed.

- Determine if customer information has been or will be misused.
- If a misuse of customer information has occurred or is reasonably likely to occur and at least 1,000 consumers are affected or reasonably likely to be affected, notify the FTC ASAP and no later than 30 days after discovery.
- Notify the FTC electronically through a form that is expected to be posted on the FTC website, https://www.ftc.gov after adoption.
- The notice includes:

---

[2]*See*, e.g., FTC, Data Breach Response: A Guide for Business (2019), www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

NIST, Guide for Cybersecurity Event Recovery (2016), nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

Orion Cassetto, Incident Response Plan 101: How to Build One, Templates and Examples, Exabeam: Information Security Blog (November 21, 2018), www.exabeam.com/incident-response/incident-response-plan/

(86 FedReg 70297 (Ftnt 294))

1. The name and contact information of the reporting financial institution, i.e., dealership;
2. A description of the types of information involved in the security event;
3. If it is possible to determine, the date or date range of the security event; and,
4. A general description of the security event.

IX. Written Regular/Annual Report

(§ 314.4(i))

• Qualified Individual regularly reports in writing, and at least annually, to the board of directors, dealer, or senior officer responsible for the security program.

• Report includes:

1. Overall status, including compliance, of the information security program.
2. Address material matters of the information security program such as:
    - o Risk assessment
    - o Risk Management & control decisions
    - o Service Provider arrangements
    - o Testing results
    - o Security events or violations & responses
    - o Recommendations for changes to the program

■ Exceptions

(16 CFR § 314.6)

• A financial institution with fewer than **5,000 consumers** (the number of individuals that a financial institution maintains customer information) are exempt from:

1. The required written risk assessment (§314.4(b)(1));
2. The required continuous monitoring or annual penetration testing and biannual vulnerability assessment (§314.4(d)(2));
3. A required written incident response plan (§314.4(h)); and,
4. A required annual or regular written report by the Qualified Individual (§ 314.4(i))

DEFINITIONS

(16 CFR § 314.2)

The FTC gives specific definitions for terms used throughout the Safeguards Rule.

(a) **Authorized User**

Any employee, contractor, agent, customer, or other person that is authorized to access any of the dealership's information systems or data.

(b) **Consumer**

An individual who obtains or has obtained a financial product or service from the dealership that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

EX: Individual applies for credit for personal, family, or household purposes is a consumer regardless of whether credit is extended.

(c) **Customer**

A consumer who has a customer relationship with the dealership.

(d) **Customer information**

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 the dealership or the dealership's affiliates.

(e)(1) **Customer relationship**

A *continuing relationship* between a consumer and the dealership under which the dealership provides one or more financial products or services to the consumer that are used primarily for personal, family, or household purposes.

(2) **EX**: A consumer has a *continuing relationship* with the dealership if the consumer: (1) obtains a loan from the dealership; (2) purchases an insurance product from the dealership; (3) enters into a lease on a non-operating basis with the dealership (i.e., the lease agreement does not include maintenance or repair services).

(f) **Encryption**

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.

(g)(2) **Financial service**

Includes the dealership's evaluation or brokerage of information that the dealership collects in connection with a request or an application from a consumer for a financial product or service.

(h)(1) **Financial institution**

EX: (ii) An **automobile dealership** that, as a usual part of its business, leases automobiles on a non-operating basis (i.e., the lease agreement does not include maintenance or repair services)for longer than 90 days.[3]

(vi) If regularly wiring money to and from consumers, then the dealership is a financial institution.[4]

(i) **Information security program**

The administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use transmit, dispose of, or otherwise handle customer information.

(j) **Information system**

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 control systems, telephone switching and private branch exchange systems, and environmental control systems that contain customer information or that is connected to a system that contains customer information.

(k) **Multi-factor authentication**

Authentication through verification of at last 2 of the following types of authentication factors:

1. Knowledge factors

EX: User name & password

2. Possession factors

EX: One-time password sent to a smartphone

3. Inheritance factors

EX: Biometric characteristics such as a fingerprint or a retina scan

(l) **Nonpublic personal information** (NPPI)

1. Personally identifiable financial information; and,
2. 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.

---

[3]12 CFR 225.28(b)(3); referenced in section 4(k)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

[4]*See* Bank Holding Company Act 12 U.S.C. 1843(k)(4)(A).

EX: List of individuals' names & addresses derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers.

(m) **Penetration testing**

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 the dealership's information systems.

(n) **Personally identifiable financial information**

Any information:

(i) A consumer provides to the dealership to obtain a financial product or service from the dealership;

(ii) About a consumer resulting from any transaction involving a financial product or service between the dealership and a consumer; or,

(iii) The dealership obtains about a consumer in connection with providing a financial product or service to that consumer.

EX: • Information a consumer provides to the dealership on an application to obtain a loan (retail installment transaction), credit card, or other financial product or service;

• Account balance information; payment history; credit or debit purchase information.

• Person who is or has been a customer or obtained a financial product or service from the dealership.

• Disclosing information about a dealership's consumer indicating the individual is or has been the dealership's consumer.

• Consumer provided information to the dealership or that is obtained in connection with collecting on or servicing a credit account.

• Information collected by the dealership through an internet "cookie."

• Information from a credit report.

(o)(1) **Publicly available information**

Any information that the dealership has a reasonable basis to believe is lawfully available to the general public from:

(i) Federal, State or local government records;

(ii) Media that is widely distributed;

(iii) Disclosures to the general public as required by Federal, State, or local law.

(2) The dealership has a **reasonable basis** to believe that information is lawfully available to the general public. Must take steps to determine:

(i) The information is the type that is available to the general public; and,

(ii) Whether an individual can direct that the information not be made available to the general public and that the dealership's consumer has not done so.

EX: • Publicly available information in government records (real estate records and security interest filings).

• Media that is widely distributed includes information from a TV or radio program, newspaper or an unrestricted website available to the public.

(p) **Security event**

An event resulting in unauthorized access to or disruption or misuse of an information system, information stored on an information system, or customer information held in physical (EX: paper) form.

(q) **Service Provider**

Any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provisions or services directly to a financial institution (i.e., dealership) subject to this Rule.