COMPLYAUTO PRIVACY

Marchese Ford of Mechanicville
Information Security Program Status

2023 ANNUAL REPORT

Prepared by: John Byrne on March 17, 2023
Dates Covered: March 17, 2022 to March 18, 2023

Created pursuant to the Gramm-Leach Bliley Act's Federal Safeguards Rule. 16 CFR § 314.4(i).

Background

On October 27, 2021, the Federal Trade Commission (FTC) finalized revisions to the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule ("Revised Rule") for the first time since the original rule was issued in 2002. The FTC specifically names "automobile dealerships" as non-banking financial institutions that fall under the purview of these new revisions. The Revised Rule is extensive and imposes a series of new technical and administrative requirements on dealers to protect customer information. This includes, but is not limited to, internal penetration testing, vulnerability assessments, use of multi-factor authentication, data encryption, security awareness training, and the performance of written risk assessments. Dealers must comply with the new Revised Rule beginning December 9, 2022, or otherwise risk penalties of up to $46,517 per violation.

Purpose of this Report

The new regulations require the submission of an annual report to the dealer's Board of Directors, equivalent governing body, or other senior officers. The purpose of the report is to ensure that senior management is engaged with and informed about the state of the dealer's information security program and overall compliance status with the regulations. According to the FTC, this will help dealers to ensure their information security programs are being maintained appropriately and given the necessary resources.

Legal Disclaimer and Disclosure

The information contained in the following report is confidential and only intended for the recipient(s). If you are not the intended recipient, you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. Given the sensitivity of this report it is recommended that distribution of this confidential report (or portions thereof) be on a "need to know" basis only and retained only for the length of time necessary to serve the legitimate business purposes for which the recipient intended.

ComplyAuto, its subsidiaries, the directors, employees, and agents cannot be held liable for the use of and reliance of the opinions and findings of this report.

This report is not intended as a source of legal advice nor as a substitute for legal advice. Readers that require legal advice should contact competent counsel.

About the Preparation of this Report

This report was prepared with the help of ComplyAuto. ComplyAuto is a software company specializing in automating privacy and cybersecurity compliance specifically for dealerships. ComplyAuto offers a full suite of solutions to help dealers achieve compliance with state and federal privacy and cybersecurity regulations, like the Revised Rule. The information provided throughout this report is based on the dealer's use of the software and entries of individual dealership users. Therefore, the accuracy of the information provided in this report cannot be guaranteed by ComplyAuto. To learn more about ComplyAuto, please visit www.complyauto.com.

Table of Contents

1. Overall Status of Compliance

This section of the report is intended to provide a high-level summary of our dealership's overall compliance with the requirement of the Revised Rule. For each item, additional information can be found in the corresponding section of this report, as well as within the ComplyAuto dashboard.

Regulation	Status	Citation
Appointment of Qualified Individual	COMPLETE	16 CFR § 314.4(a)
Annual Internal Risk Assessment (Physical)	COMPLETE	16 CFR §314.4(b)
Annual Internal Risk Assessment (Technical)	COMPLETE	16 CFR §314.4(b)
Device Inventory	COMPLETE	16 CFR §314.4(c)(2)
Data & Systems Inventory	COMPLETE	16 CFR §314.4(c)(2)
Encryption at Rest & In-Transit	IN PROGRESS	16 CFR § 314.4(c)(3)
Multi-factor Authentication	IN PROGRESS	16 CFR § 314.4(c)(5)
Annual Penetration Test	COMPLETE	16 CFR §314.4(d)(2)
Biannual Vulnerability Scan	COMPLETE	16 CFR §314.4(d)(2)
Service Provider Contracts & Risk Assessments	IN PROGRESS	16 CFR §314.4(f)(2)-(3)
Written Information Security Program	COMPLETE	16 CFR §314.4(g)
Written Incident Response Plan	COMPLETE	16 CFR §314.4(h)
Written Data Retention Plan	COMPLETE	16 CFR §314.4(c)(6)(i)-(ii)
Written IT Change Management Procedures	COMPLETE	16 CFR §314.4(c)(7)
Employee Security Awareness Training	COMPLETE	16 CFR §314.4(e)
Intrusion & Attack Detection	COMPLETE	16 CFR §314.4(d)(1)
Unauthorized activity monitoring	COMPLETE	16 CFR §314.4(c)(8)
Phishing & Social Engineering Simulations	COMPLETE	16 CFR §314.4(d)(2)(i)

2. Appointing a Qualified Individual to Oversee Compliance

COMPLIANCE STATUS

COMPLETE

BACKGROUND

Under the Revised Rule, dealers must appoint a single "Qualified Individual" to oversee our Information Security Program (“ISP”). This individual is also known as the "Program Coordinator." According to the FTC, dealers may designate any qualified individual who is appropriate for their business based on the business size and complexity. The purpose behind requiring designation of a single coordinator is to improve accountability, avoid gaps in responsibility in managing data security, and improve communication. Note that while the Program Coordinator must have ultimate responsibility for overseeing and managing the ISP, dealers may still assign particular duties, decisions, and responsibilities to other staff members and outside vendors and service providers.

DETAILS / RESULTS

Our current Qualified Individual is:

John Byrne
Controller
jbyrne@marcheseford.com

3. Annual Internal Risk Assessments

COMPLIANCE STATUS

COMPLETE

BACKGROUND

The Revised Rule requires that dealers perform written risk assessments that serve four general purposes: (1) identify potential physical, technical, and administrative security vulnerabilities and threats that may exist at their dealership, (2) include specific criteria that outlines methods on how the organization will mitigate those risks once they are identified, (3) are performed periodically to reexamine potential risks, and (4) reassess the sufficiency and efficacy of any safeguards already in place to control those risks.

DETAILS / RESULTS

Physical & Administrative Risk Assessments

A physical & administrative risk assessment has been completed in the past 12 months for:
1 / 1 locations

Our most recent assessment for physical & administrative information safeguards was performed on:
September 22, 2022

Risks and/or violations were found for the following safeguards:

Technical Risk Assessments

A technical risk assessment has been completed in the past 12 months for:
1 / 1 locations

Our most recent assessment for technical information safeguards was performed on:
October 4, 2022

Risks and/or violations were found for the following safeguards:

1. Install EDR Software and Continuously Monitor Logs on All Endpoints
   total issues: 1, issues mitigated: 1

2. Enable MFA for Employee Workstations and Internal Servers Containing NPI
   total issues: 1, issues mitigated: 1

3. Enable MFA for All Third-Party Cloud-Based Applications Containing NPI
   total issues: 1, issues mitigated: 1

4. Ensure Digital Copiers Have Encryption, Overwriting, Auto-Wiping Enabled
   total issues: 1, issues mitigated: 1

4. Completing a Device, Data and Systems Inventory

COMPLIANCE STATUS

COMPLETE

BACKGROUND

Under the Revised Rule, dealers are required to perform a device, data and systems inventory. This requirement was designed to ensure that businesses inventory the data in their possession and inventory the systems on which that data is collected, stored, or transmitted. According to the FTC, this inventory forms the basis of an Information Security Program because a system cannot be protected if the business does not understand its structure or know what data is stored in which systems. A data and systems inventory is the process of identifying and tracking how customer information is collected and flows through the dealership (data mapping), as well as documenting where it is stored, who it is shared with, and for which business purposes it is collected. Identifying all devices connected to the network is a critical part of this step so that no devices or systems accessing customer information get overlooked. Given that dealers store most of their customer information in third-party vendor systems, a complete inventory of all vendors and service providers that have access to customer information must be completed.

DETAILS / RESULTS

Device Inventory

Our device inventory was last updated on:
March 9, 2023

We are currently tracking 56 devices.

Data & Systems Inventory

We are currently tracking 9 vendors that store, access, or receive customer information covered under the Revised Rule.

Our data and system inventory was last updated on:
January 19, 2023

5. Encryption of Data at Rest & In Transit

COMPLIANCE STATUS

IN PROGRESS

BACKGROUND

Encryption is the process of transforming usable data into an unreadable form. The Revised Rule requires that customer information be encrypted while in transit (e.g., while being sent over email or uploaded to a DMS) and at rest (e.g., while being stored on a computer's hard drive). For email, dealers should ensure the use of a centrally managed corporate email system that has transport layer security (TLS) enabled. For devices running on a Windows operating system, dealers should strongly consider enabling BitLocker, which is Microsoft's free built-in mechanism for device encryption.

DETAILS / RESULTS

Our dealership does allow or endorse the use of personal or unmanaged email addresses for work-related purposes.

We currently use Gmail as our centrally managed email client.

We have enabled TLS on our email client/server.

We are using the following tool to ensure that all workstation hard drives (e.g., Windows and Mac computer drives) that are likely to have customer information are encrypted:
ComplyAuto (powered By Coro)

We currently have 17 devices running software to detect unencrypted drives and remotely encrypt them.

6. Multi-factor Authentication

COMPLIANCE STATUS

IN PROGRESS

BACKGROUND

Multi-factor authentication ("MFA") is an authentication system that requires at least two distinct authentication factors for successfully logging into a system. The three authentication factors are:

1. Knowledge factors, such as a password;
2. Possession factors, such as an SMS/text, app-based push notification, or email token; and
3. Inherence factors, such as biometric characteristics, like a fingerprint.

Under the Revised Rule, dealers must require MFA for any system containing customer information. MFA can significantly help reduce your dealership's chances of a cybersecurity incident. There are three primary scenarios under which dealers will need to implement MFA:

1. Employee workstations upon logging into a Windows and MacOS machine.
2. Third-party applications like the DMS, CRM, etc.*
3. Email clients like Office 365 and Google Workspace.

*Since dealers are often at the behest of their individual vendors supporting MFA, this item is addressed via vendor contracts and risk assessments.

DETAILS / RESULTS

Our dealership does not require MFA upon logging into our corporate email client.

Our dealership does require MFA upon Windows/MacOS login.

We are using the following tool for device-level MFA (e.g., Windows and MacOS logon MFA):
ComplyAuto (powered by Duo)

We currently have 15 users enrolled in MFA.

We currently have 11 devices registered for MFA.

7. Conducting Annual Penetration & Vulnerability Tests

COMPLIANCE STATUS

COMPLETE

BACKGROUND

The Revised Rule requires that dealers perform internal penetration tests at least annually. Penetration testing is a type of IT security test in which evaluators mimic real-world attacks to attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual hackers. The goal of this exercise is to expose vulnerabilities so that the organization can work to reinforce their data security protocols.

The Revised Rule also requires that dealers perform vulnerability assessments. A vulnerability assessment is any systemic scan of a dealership's entire IT environment in which all installed software is identified and checked for any publicly known security vulnerabilities. Under the Revised Rule, vulnerability assessments must be performed once at least every six months.

DETAILS / RESULTS

Penetration Testing

We are using the following company for penetration testing:
ComplyAuto

Penetration tests performed within the full reporting window:
Most Recent Scan: November 16, 2022
Total Scans Run: 1

The following vulnerabilities and/or exploits were identified across 1 different network(s):

- Critical: 0 identified
- High-risk: 0 identified
- Medium-risk: 0 identified

Vulnerability Assessments

We are using the following company for vulnerability assessments:
ComplyAuto

Vulnerability scans performed within the past 6 months of the reporting window:
Most Recent Scan: November 16, 2022
Total Scans Run: 1

The following vulnerabilities and/or exploits were identified across 1 different network(s):

- Critical: 0 identified
- High-risk: 8 identified
- Medium-risk: 0 identified

Details of each issue identified in the scans, along with recommended mitigation steps, can be found within the ComplyAuto dashboard.

8. Assessing Adequacy of Service Provider Safeguards

COMPLIANCE STATUS

IN PROGRESS

BACKGROUND

For service providers that have access to NPI, dealers are required by the Revised Rule to do the following:

1. Take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the NPI at issue;
2. Require the service providers, by contract, to implement and maintain such safeguards; and
3. Periodically assess the service providers based on the risk they present and the continued adequacy of their safeguards.

DETAILS / RESULTS

Vendor Data Processing Agreements

5 Completed
3 Sent
0 Refused
0 Unsent

Vendor Risk Assessments

3 Completed
1 Sent
0 Refused
3 Unsent

9. Implementing Written Information Security Policies

COMPLIANCE STATUS

COMPLETE

BACKGROUND

The Revised Rule requires that dealers implement a series of written policies and procedures that includes a (1) Information Security Program, (2) Incident Response Plan, (3) Data Retention & Disposal Policy, and (4) Information Technology Change Management Procedures. The required written Information Security Program must be created and updated based on the results of the annual internal risk assessments outlined above.

DETAILS / RESULTS

The following policies were created and last updated as follows:

Information Security Program

Create Date: April 12, 2022
Last Updated: April 12, 2022

Incident Response Plan

Create Date: April 12, 2022
Last Updated: April 12, 2022

Data Retention Plan

Create Date: April 12, 2022
Last Updated: April 12, 2022

IT Change Management Procedures

Create Date: April 12, 2022
Last Updated: April 12, 2022

Each of the above policies are available in the ComplyAuto dashboard to review and download.

10. Implementing a Security Awareness Training Program

COMPLIANCE STATUS

COMPLETE

BACKGROUND

The Revised Rule now requires that dealers provide security awareness training to all employees as well as verifying that the information security personnel maintain current knowledge of changing information security threats and countermeasures.

DETAILS / RESULTS

Number of employees enrolled in required security awareness course in the last 12 months:
18

Employees who have completed the required security awareness training course:
14

The last time an employee was enrolled in a security awareness course was on:
November 7, 2022

11. Intrusion & Attack Detection

COMPLIANCE STATUS

COMPLETE

BACKGROUND

The Revised Rule requires a system for detecting intrusions and attacks on the dealer's network. While no specific technology or product is mentioned in the Revised Rule, many cybersecurity insurance carriers (and even some manufacturers) require something known in the industry as endpoint detection and response (EDR) software. EDR is security software that is installed on workstations and servers, commonly referred to as "endpoints." EDR collects technical data from these endpoints and then analyzes for suspicious patterns and threats. If a threat is identified, it is blocked and an alert is generated. Many EDR solutions include a traditional antivirus functionality and the ability for responders to remotely access compromised systems for remediation. In order to be effective, EDR logs must be continuously monitored and managed around the clock by experienced cybersecurity personnel. Fortunately, many EDR providers offer solutions supported by a 24/7 team to manage and respond to identified incidents. Note that EDR is not necessarily the same as an anti-virus or even "next-gen anti-virus" software, although there may be overlap. EDR is normally more advanced than your typical anti-virus and anti-malware system.

DETAILS / RESULTS

Our dealership is currently using the following EDR software:
ComplyAuto (powered by Coro)

We currently have 17 devices running software to detect intrusions and attacks.

12. Unauthorized Activity Monitoring

COMPLIANCE STATUS

COMPLETE

BACKGROUND

Under the Revised Rule, dealers are required to have a system capable of detecting unauthorized access, sharing, use of, and tampering with customer information by their own users and employees. While no particular technology is mentioned in the regulations, this is typically accomplished by something known as a data leak or loss prevention (DLP) tool. DLP tools utilize technology that scan devices and emails to ensure that users do not send sensitive information outside the corporate network or engage in other suspicious activities related to sensitive information.

DETAILS / RESULTS

Our dealership is currently using the following DLP tool or equivalent technology:
ComplyAuto (powered by Coro)

We currently have 16 users enrolled in software that provides active data governance monitoring.

We currently have 17 devices running software to discover locally stored data that may violate data governance rules.

13. Phishing & Social Engineering Simulations

COMPLIANCE STATUS

COMPLETE

BACKGROUND

The FTC has clarified that testing employees' susceptibility to social engineering and phishing scams is an important part of the new requirements. Multiple studies have found that over 90% of ransomware and cybersecurity incidents involve clicking on a link in a phishing email. Phishing simulations test employees' security awareness and susceptibility to social engineering tactics. This involves sending out emails designed to look like real-life phishing emails, and then tracking which employees are willing to click on links within those emails or enter credentials on a fake website landing page. "Phished" employees are then automatically enrolled in security awareness training. Internal phishing tests can be very effective at conditioning employees to scrutinize emails sent from people outside of your organization.

DETAILS / RESULTS

Our dealership is currently using the following tool for phishing simulations:
ComplyAuto

Since conducting these campaigns, our employees' susceptibility to phishing emails has been reduced by 100%.

In our most recent campaign, our employee click rate was 3.6%. Since the inception of this tool, our average is 5.3% compared to the national average of 2.3% collected by ComplyAuto across over 5,000 dealers across the country.

In the past 12 months, 8 employees have completed the required remedial training upon failing a phishing test.

Please refer to the ComplyAuto Dashboard for more information.

14. Questions

Questions regarding this report should be directed to:

John Byrne
Controller
jbyrne@marcheseford.com