

A solution for complying with the revised FTC Safeguards Rule



Presented on May 10th, 2022

by Chris Cleveland

CEO & Co-Founder, ComplyAuto; Compliance Director, Galpin Motors

www.complyauto.com



Chris Cleveland

CEO & Co-Founder, ComplyAuto
Compliance Director, Galpin Motors



John McCallan

Owner, Operator & Attorney, Raceway Ford
Partner, Kearny Mesa Ford & Kia of Sunroad Auto



Shane McCallan

Co-Founder, ComplyAuto
General Counsel, Raceway Ford (*former*)
Vice President, Auto Advisory Services (*former*)

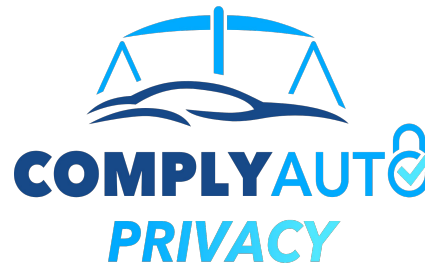


Hao Nguyen

General Counsel, ComplyAuto
Staff Counsel, CNCDA (*former*)
Sr. Manager of Legal Affairs, KPA (*former*)



AFFINITY
PROVIDER



About ComplyAuto

"By Dealers. For Dealers."

- 60+ years of combined dealership compliance experience
- ComplyAuto Privacy was created organically to solve problems faced by the owners at their own dealerships.
- In just the past year, ~2,000 dealers used the ComplyAuto software to achieve compliance with state and federal privacy and cybersecurity laws.

The Revised FTC Safeguards Rule

- 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 rule was issued in 2002.
- The Revised Rule is effective **January 10, 2022**, but most provisions are delayed until **December 9, 2022**.
- The Revised Rules are detailed in a 145-page publication.
- In its announcement, 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 (summary on next slide).
- Dealers must act immediately to meet compliance with the new rules or otherwise risk penalties of up to \$46,517 per violation.
- NADA estimated that the new rules would cost a single dealer \$276,925/yr
- GLBA/CIS compliance also helps dealers significantly reduce their cybersecurity insurance premiums (and prevent denial in coverage/renewal)
- NADA released their newest compliance manual last month, which was co-authored by ComplyAuto/Chris Cleveland



New FTC Safeguards Rule Requirements

- Required documentation of IT change management procedures
- Required annual penetration testing
- Required biannual vulnerability scanning
- Required employee training on information security
- Required contracts for vendors containing NPI
- Required risk assessments of vendors containing NPI
- Required written incident response plan
- Required annual written report to the Board of Directors
- Appointment of “qualified individual”
- Requirement to undertake written risk assessments and update policies after each assessment
- Implementation of “access controls”
- Undertake a required data and systems inventory
- Data encryption requirement
- Multi-factor authentication for systems containing NPI
- Systems monitoring and logging
- Development of secure data disposal procedures
- Phishing simulations & security awareness



APPLICABLE LAW OR REGULATION

16 CFR §314.4(c)(6)-(7), §314.4(c)(6)(h)(1)

Dealers must have a written Information Security Program and Incident Response Plan that is made available to employees.



FOUR WRITTEN POLICY REQUIREMENTS

The revised rule requires the following written policies:

1. Information Security Program
 - Existing programs must be updated in accordance with the new regulations.
2. Incident Response Plan
 - The regulations specify exactly what must be included in this plan.
3. Data Retention Plan
 - Must dispose of NPI after there's no longer a legal/business need
4. IT Change Management Procedures
 - Process to follow when major changes are made to IT infrastructure to ensure no security gaps

- Dashboard 🏠
- Requests 📧
- Locations 📍
- Vendors 🚚
- Request Portal 📋
- Notices ▾
 - Signage
 - Web Banner
 - Email, Text, and Voice
 - Privacy Policy Builder
- Users 👤
- Learning Center 📖
- Employee Training 🎓
- Federal Safeguards ▾
 - Risk Assessments
 - ISP Policy Builder
- Data Map 📊
- Phishing 🐟

New ISP Policy - ABC Motors, Inc.

General Info — Program Coordinator — **3 Frameworks** — 4 Policies

Security Frameworks for Electronic & Technical Safeguards

Please select the security frameworks that your organization currently employs.
Note: These will be included in your ISP Policy.

REQUIRED

☒ Physical & Administrative Safeguards Based on FTC Guidelines & Enforcement Actions

Show Safeguards ▾

More Info

REQUIRED

☒ Technical Safeguards Based on FTC Guidelines & Enforcement Actions

Show Safeguards ▾

More Info

OPTIONAL

☒ CIS Critical Security Controls - Version 8

Hide Safeguards ^

More Info

SAFEGUARDS

☒ Establish and Maintain Detailed Enterprise Asset Inventory

☐ Address Unauthorized Assets

☐ Establish and Maintain a Software Inventory

☒ Ensure Authorized Software is Currently Supported

☐ Address Unauthorized Software

☐ Establish and Maintain a Data Management Process

- Dashboard
- Requests
- Locations
- Vendors
- Request Portal
- Notices
- Signage
- Web Banner
- Email, Text, and Voice
- Privacy Policy Builder
- Users
- Learning Center
- Employee Training
- Federal Safeguards
- Risk Assessments
- ISP Policy Builder
- Data Map
- Phishing

New ISP Policy - ABC Motors, Inc.

✓ General Info — ✓ Program Coordinator — ✓ Frameworks — 4 Policies

Incident Response Plan

Would you like to include an incident response plan in this ISP policy? Select "No" only if your company maintains their own incident response plan outside of this ISP.

☒ Yes ☐ No

Data Retention Plan

Would you like to include a data retention plan in this ISP policy? Select "No" only if your company maintains their own data retention response plan outside of this ISP.

☒ Yes ☐ No

IT Change Management Policy

Would you like to include an IT change management policy in this ISP policy? Select "No" only if your company maintains their own IT change management policy outside of this ISP.

☒ Yes ☐ No

Cancel

< Back

Finish

DESIGNATE A SINGLE PERSON TO OVERSEE YOUR ISP

Under the Revised Rule, you must appoint a single "Qualified Individual" to oversee your Information Security Program ("ISP").

- It is generally recommended that this be a Chief Information Security Officer (CISO), IT Director, or person in a similar role. However, no prerequisite level of education, experience, or certification is defined by the Revised Rule.
- The purpose behind requiring designation of a single coordinator is to improve accountability, avoid gaps in responsibility in managing data security, and improve communication. According to the FTC, splitting authority over an information security program between two or more people leads to failures of communications and oversight.
- Note that while this person must have ultimate responsibility for overseeing and managing the ISP, dealers may still assign particular duties, decisions, and responsibilities to other staff members.



APPLICABLE LAW OR REGULATION

16 CFR § 314.4(a)

Under the Revised Rule, dealers must appoint a single "Qualified Individual" to oversee their Information Security Program ("ISP")

✖ Old Rule	✔ New Rule
Could be anyone at the dealership	Must be "qualified" in area of information security
Could be multiple individuals	Must be a single person
Known as the "Program Coordinator"	Referred to as the "Single Qualified Individual"



Dashboard Requests Locations Vendors Request Portal Notices 

Signage

Web Banner

Email, Text, and Voice

Privacy Policy Builder

Users Learning Center Employee Training Federal Safeguards 

Risk Assessments

ISP Policy Builder

Data Map Phishing 

New ISP Policy - ABC Motors, Inc.

1 General Info 2 Program Coordinator 3 Frameworks 4 Policies

Program Coordinator

Under the revised Safeguards Rule, you must appoint a single "Qualified Individual" to oversee your Information Security Program. This individual is also known as the "Program Coordinator". It is generally recommended that this be a CISO, IT Director, or person in a similar role. However, no particular level of education, experience, or certification is defined by the Rule. According to the FTC, dealers may designate any qualified individual who is appropriate for their business as based on their 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 information security program, dealers may still assign particular duties, decision making, and responsibilities to other staff members. Moreover, the Rule does not require that this be the Program Coordinator's sole job – he or she may have other duties.

Employee Name *

Chris Cleveland

Employee Title *

CISO

Employee Email *

chris@complyauto.com

[Cancel](#)[< Back](#)[Next >](#)

IMPLEMENT MFA FOR SYSTEMS WITH NPI



APPLICABLE LAW OR REGULATION

16 CFR § 314.4(c)(5)

Under the Revised Rule, dealers must require MFA for any system containing NPI.

Multi-factor authentication (“MFA”) is an authentication system that requires at least two distinct authentication factors for successfully logging into a system. For example, **Password + Text Code**

MFA isn’t just the law -- it can significantly help reduce your dealership’s chances of a cybersecurity incident. According to a study by Microsoft, MFA blocks over 99.9 percent of account compromise attacks. There are three primary scenarios under which dealers will need to consider enabling MFA:

- **Third-party Applications.** Start by enabling MFA for all of your online or cloud-based applications and software that store or access customer NPI (e.g., your CRM, DMS, and credit-related systems). Popular dealer systems like DealerTrack and RouteOne already have a way to enable MFA for all users.
- **On-premises MFA.** If dealers are storing NPI on their own internal devices, networks, or servers (including an on-premises DMS), they should strongly consider enabling MFA on logins to the employees’ workstations/operating systems.
- **Cloud Computing and Email Clients.** Most major email clients, like Microsoft 365 and Google (Gmail) natively support MFA. Make sure you enable MFA for all users accessing email, as NPI is commonly transmitted and stored via email. If your dealership is using Google Workspace or Microsoft Azure Active Directory, you should also enable MFA.



Logging in to your account using **Multi-Factor Authentication**

You will be prompted to login using Multi-Factor Authentication for the first time post enrollment and any time you login using an new unrecognized browser.

1. After logging into Dealertrack.com, you will be brought to the Verification view. Select one method you would like to use to verify. You will only need to use one method at the time of verification. 
2. Upon your selection, you will receive a verification code.
3. Enter your one time verification code in the 'Enter Code' field and click 'Verify'. 
4. **Important!**: Be sure to check the "Trust this browser" checkbox to not be prompted to verify the next time you log in. 

Multi-Factor Authentication (MFA) - Verification

Please select which Multi-Factor Authentication (MFA) option you would like to log in with for your current session.

Enrolled options






 Email 	 SMS 
---	---

Multi-Factor Authentication (MFA) - Verification

Please select which Multi-Factor Authentication (MFA) option you would like to log in with for your current session.

 Please check your email inbox for your verification code.

Enrolled options

 Email k...l@gmail.com  Enter Code <input type="text"/>  	 SMS 
---	---

ENCRYPTING DATA AT REST & IN TRANSIT



APPLICABLE LAW OR REGULATION

16 CFR § 314.4(c)(3)

The Revised Rule requires that customer information be encrypted while in transit and at rest.

Put simply, 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).

- **Dealer-owned Systems and Devices.** If any of the dealership's devices, such as desktops, laptops, tablets, or mobile devices store customer information, consider enabling the encryption of the hard drives on those devices.
- **Email Clients.** At a minimum, dealers should ensure the email client (e.g. Office 365, Google) is configured to send emails using TLS. Never allow employees to use their own personal email account for work, as it is difficult to control the security and encryption settings of those accounts.
- **Dealer-maintained Websites.** Most major website providers (e.g., Dealer.com, DealerInspire, Jazel, Sincro, etc.) have SSL certificates by default. However, if a dealership maintains any of its own websites, such as a group site landing page, ensure it has an SSL certificate (i.e., using an https:// instead of an http:// url). Not only is this a good security practice, but it also helps the site rank higher on search engines!



⌘ TECHNOLOGY TIP

Encryption for Windows Devices. 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. For a collection of helpful articles on deploying BitLocker at your organization, see the following link:
<https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview>

REQUIRED SERVICE PROVIDER CONTRACTS



APPLICABLE LAW OR REGULATION

16 CFR §314.4(f)(2)

Dealers must require that vendors with access to NPI sign a contract where they promise to implement reasonable safeguards.

Who needs to sign a GLBA Service Provider Addendum?

Any vendor who collects or processes NPI.

What if they refuse to sign?

While there is obviously no way to force vendors to sign the addendum, there are some actions you can take:

- Remind the service provider that they may be independently required to comply with the Revised Rule, so completing these items is mutually beneficial. Indeed, in a 2019 complaint against (and subsequent consent order with) a dealership DMS, the FTC took the position that businesses whose services facilitate financial operations on behalf of dealers are themselves considered financial institutions subject to the privacy and data security requirements under the GLBA Safeguards Rule.
- Determine if there's an existing contract with language that already satisfies the requirements of the Revised Rule. Ask your legal counsel to review your existing contract with the vendor as there may already be provisions that require the service provider to maintain appropriate safeguards. If the service provider refused to sign on this basis, ask them to produce a copy of the contract and cite to the applicable provision(s).



VENDOR RISK ASSESSMENTS

Dealers must now assess the adequacy of their vendors' safeguards as well. Therefore, dealers should consider the following:

1. Before signing with a new service provider, require them to complete a risk assessment questionnaire that assesses their overall risk and ability to maintain appropriate physical, administrative, and technical safeguards; and
2. Require that existing service providers periodically complete a new risk assessment questionnaire as new risks or safeguards are identified.



APPLICABLE LAW OR REGULATION

16 CFR §314.4(f)(3)

Dealers are required to periodically assess their service providers based on the risk they present and the continued adequacy of their safeguards.



Compliance Motors

DEMO

Name	Designations	Type	DPA's	Risk Assessment	Risk Score	Sources
Concentra	Processor Third Party	Background Check Companies	REQUIRED	OPTIONAL		N/A
Consumer Connection	Processor Third Party	Direct Mailers	REQUIRED	REQUIRED		17
Conversica	Processor Third Party	Text Messaging Tools	REQUIRED	REQUIRED		14
CoroData	Processor Third Party	Records Management Companies	REQUIRED	REQUIRED		N/A
Credit Bureau Connection (CBC)	Processor Third Party	Credit Reporting & Compliance Systems	REQUIRED	COMPLETED		N/A
CreditCall		Payment Processors & Gateways	REQUIRED	IN PROGRESS		N/A
CrossCheck	Third Party	Check Guarantee Companies	REQUIRED	REQUIRED		N/A
Darwin	Processor Third Party	Electronic F&I Menu Systems	REQUIRED	REQUIRED		N/A
Davenport, Gerstner, and McClure		Employment Law Firms	N/A	OPTIONAL		N/A

Send Contract to Vendor for Signing

Vendor Name
Credit Bureau Connection (CBC)

Contract Type
GLBA Service Provider Agreement [Download template](#)

Dealer Contact
Chris Cleveland (chris@complyauto.com)

Vendor's Email Address *

Suggested Vendor Emails

Darin Larsen (COO)	Completed 100% of recent eSigns.	Use
dlarsen@creditbureauconnection.com		

Your Legal Entity Name *

Your Organization or Group Name *

Compliance Motors

You only need to change this if the vendor would recognize your organization under a different name.

Additional Email Addresses to CC

Type or paste email addresses and press Enter or Space...

Prefer to send the email to the vendor yourself? Click the button "Copy Link to Clipboard" and you'll be provided a unique link to send to the vendor.

[Copy Link to Clipboard](#) [Close](#) [Send](#)

Consumer Connection **EMAIL REQUIRED**

Conversica

CoroData

Credit Bureau Connection (CBC)

CreditCall

CrossCheck

Darwin

Davenport, Gerstner, and McClure

Davenport, Gerstner, and McClure

Processor Third Party

Employment Law Firms

REQUIRED

OPTIONAL

Showing 51 to 60 of 138 entries

< 1 ... 5 6 7 ... 14 >



APPLICABLE LAW OR REGULATION

16 CFR §314.4(b)

Dealers must have a written risk assessments for physical and technical safeguards that documents evaluation methods mitigation efforts.



DOCUMENTED INTERNAL RISK ASSESSMENTS

Risk assessments should test for and incorporate, at a minimum, the following:

1. Safeguards required under the revised rule
 - <https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information>
2. Safeguards based on FTC enforcement actions
 - <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>
3. Safeguards based on practices recommended by the FTC
 - https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

<https://www.cis.org>



COMPLYAUTO
PRIVACY

Dashboard 🏠

Requests 📧

Locations 📍

Vendors ▼ 📁

Surveys

Manage

Request Portal 📋

Notices ^ ☰

Users 👤

Learning Center 📖

Employee Training 🎓

Federal Safeguards ▼ 🛡️

Risk Assessments

ISP Policy Builder

Data Map 🗺️

Phishing ^ 📧

4. Limit Administrative Access to a Neutral Department or Person

Risk: MEDIUM ✖

5. Require Complex and Unique Passwords

Risk: HIGH ✖

6. Ensure User Credentials Are Not Stored in Vulnerable Formats

Risk: HIGH ✖

7. Enable MFA for All Systems Containing Nonpublic Personal Information

Risk: HIGH ✔

Do you require the use of multi-factor authentication (MFA) on your most sensitive databases, such as your DMS, CRM, credit and finance systems, and HR software?

✖ Reset 💾 Save

Practical Tip Associated Risk Evaluation Method

Third-party Applications. Start by enabling MFA for all of your online or cloud-based applications and software that store or access customer NPI (e.g., your CRM, DMS, and credit-related systems). If you're finding that many of your third-party applications and software companies do not support MFA, then try to enable IP whitelisting if that's available instead, which will help mitigate the risk of unauthorized access. You should also put pressure on each third-party vendor to begin supporting MFA due to the new regulations. Popular dealer systems like DealerTrack and RouteOne already have a way to enable MFA for all users.

On-premises MFA. There are several popular software companies that offer solutions for on-premises multi-factor authentication, such as Okta and Duo Security. If dealers are storing NPI on their own internal devices, networks, or servers (including an on-premises DMS), they should strongly consider enabling MFA on logins to the employees' workstations/operating systems.

Cloud Computing and Email Clients. Most major email clients, like Microsoft 365 and Google (Gmail) natively support MFA. Make sure you enable MFA for all users accessing email, as NPI is commonly transmitted and stored via email. If your dealership is using Google Workspace or Microsoft Azure Active Directory, you should also enable MFA.

☒ Yes ☐ No

Describe the technology or solution used

Using CISO Duo MFA via SMS tokens for all Windows devices. MFA also enabled for Google Workspace and all other cloud-based applications containing NPI, where supported. Systems not supporting MFA have IP safelisted enabled instead.

8. Disable User Accounts After Multiple Unsuccessful Login Attempts

Risk: MEDIUM ✖

9. Encrypt Data at Rest and in Transit

Risk: HIGH ✖

- Dashboard
- Requests
- Locations
- Vendors
 - Manage
- Request Portal
- Notices
- Users
- Learning Center
- Employee Training
- Federal Safeguards
 - Risk Assessments
 - ISP Policy Builder
- Data Map
- Phishing

29. Establish and Maintain a Vulnerability Management Process

Risk: MEDIUM



30. Establish and Maintain a Remediation Process

Risk: MEDIUM



31. Perform Automated Operating System Patch Management

Risk: HIGH



32. Perform Automated Application Patch Management

Risk: MEDIUM



33. Establish and Maintain an Audit Log Management Process

Risk: LOW



34. Collect Audit Logs

Risk: LOW



35. Ensure Adequate Audit Log Storage

Risk: LOW



36. Ensure Use of Only Fully Supported Browsers and Email Clients

Risk: HIGH



37. Use DNS Filtering Services

Risk: MEDIUM



Safeguard 9.2 - Do you use DNS filtering services on all enterprise assets to block access to known malicious domains?

Practical Tip

Associated Risk

Evaluation Method

Multiple organizations exist that provide DNS filtering. Some even provide this service free of charge such as Quad9. With a simple configuration change, enterprise systems will use the filtering service with little to no impact on an organization's Internet browsing all the while blocking bad traffic. Accordingly, the following resources can be of assistance:

- OpenDNS: Steps for setting up OpenDNS on Windows 10 (<https://support.opendns.com/hc/en-us/articles/228007207-Windows-10-Configuration>).
- Quad9: Steps for setting up Quad9 on Windows 10 (<https://www.quad9.net/microsoft>).

☒ Yes ☐ No

38. Deploy and Maintain Anti-Malware Software

Risk: HIGH





APPLICABLE LAW OR REGULATION

16 CFR §314.4(e)

Employees must be trained on security awareness and your information security program policies, procedures, and safeguards.

NEW EMPLOYEE TRAINING REQUIREMENTS



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.



Privacy, Phishing, and Information Security Awareness

2 modules

Start course →

Overview

Both federal and state laws require dealers to implement a variety of safeguards to protect the security and confidentiality of customer information. Dealers are obligated to not only protect sensitive customer information, but to also notify customers and regulatory agencies in the event of a security breach and establish both physical and electronic safeguards. Given the nature of dealers' business practices, most, if not all, employees have access to sensitive customer information.

This training will cover policies and procedures necessary to safeguarding customer information. Doing so ensures dealers are protecting their customer base and providing outstanding

Course content

- ☒ Privacy and Information Security 0%
- ☒ Phishing & Security Awareness 0%

Employees (Training)

[Refresh](#)
[Manage Employees](#)
[SCORM Package](#)
[Preview Training](#)
[Active \(15\)](#)
[Archived \(9\)](#)

<input type="checkbox"/>	Name	Completed Trainings	Pending Trainings	Training Summary			
<input type="checkbox"/>	Aly Rappoldt aly@complyauto.com	NONE	Dealership Security Awareness	NOT VIEWED Feb 7, 2022			
<input type="checkbox"/>	Carolynn Chavez carolynn@complyauto.com	NONE	Dealership Security Awareness	NOT VIEWED Feb 4, 2022			
<input type="checkbox"/>	Casey Graff casey+training@complyauto.com	California Consumer Privacy Act	Phishing & Dealership Security Awareness Dealership Security Awareness	INCOMPLETE Jan 28, 2022			
<input type="checkbox"/>	Casey Graff caseyagraff@gmail.com	California Consumer Privacy Act Privacy & Information Security Phishing & Dealership Security Awareness Identity Theft Prevention (Red Flags)	Dealership Security Awareness	INCOMPLETE Feb 4, 2022			
<input type="checkbox"/>	Casey Graff casey@complyauto.com	Identity Theft Prevention (Red Flags)	Dealership Security Awareness	INCOMPLETE Feb 4, 2022			
<input type="checkbox"/>	Chris Cleveland chris@complyauto.com	NONE	Dealership Security Awareness	NOT VIEWED Feb 4, 2022			
<input type="checkbox"/>	David Estrada david.estrada@complyauto.com	NONE	Dealership Security Awareness	NOT VIEWED Feb 4, 2022			
<input type="checkbox"/>	David Podolsky david@complyauto.com	NONE	Dealership Security Awareness	NOT VIEWED Feb 4, 2022			
<input type="checkbox"/>	Hao Nguyen hao@complyauto.com	NONE	Dealership Security Awareness	NOT VIEWED Feb 4, 2022			
				NOT VIEWED			

REQUIRED ANNUAL PENETRATION TESTING

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. A comprehensive internal penetration test will usually include, at a minimum, the following:

1. **Phishing and social engineering simulations.**
2. **Ransomware emulations.**
3. **Password cracking.**
4. **Credentials sniffing.**
5. **Web application attack simulations.**
6. **Active Directory attack simulations.**



APPLICABLE LAW OR REGULATION

16 CFR §314.4(d)(1)(i)

Dealers must perform penetration tests of their IT infrastructure and information systems at least annually.



🔗 TECHNOLOGY TIP

Phishing Simulations. A study by Verizon showed that 90% of ransomware and cybersecurity incidents involve clicking on a link in a phishing email. Consider using a phishing simulation software to test employees' security awareness and susceptibility to social engineering tactics. This normally 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 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.

Penetration Testing. Many IT consulting firms and managed security service providers (MSSPs) offer internal penetration tests. Software is also available to help automate penetration testing without the need for evaluators to come on premises.





APPLICABLE LAW OR REGULATION

16 CFR §314.4(d)(1)(ii)

Dealers must perform vulnerability assessments at least biannually.

REQUIRED BIANNUAL VULNERABILITY ASSESSMENTS

A vulnerability assessment is a scan of the 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.

⌘ TECHNOLOGY TIP

Open-Source Vulnerability Scanners. The FTC has mentioned OpenVAS, a free open source vulnerability scanner, as a tool that can be used to help satisfy the requirement for biannual vulnerability assessments. OpenVAS is a very popular tool for internal and external vulnerability scans. Visit <https://www.openvas.org/> for more details. While not mentioned by the FTC, nMap is another popular open-source vulnerability scanner. Visit <https://nmap.org/> for more details. However, dealers are advised to consult with experienced IT personnel before attempting to install and run these open source tools themselves.



Herman Motors

Pen Test Overview

25 Total Vulnerabilities Detected

1Critical

4High

0Medium

20Low

Click to expand for vulnerability details

Vulnerabilities

Severity	Name	Count	Found On	Remediation
8.0	Using easy-to-guess password(s)	1	root	It is recommended to set a stronger password policy for every use or service that requires authentication. The following is a list of minimal requirements for password complexity: A. The password should contain at least 8 characters B. The password should contain at least one upper case character, one lower case letter and one number. C. It is strongly advised not to use commonly used password, such as Aa123456 or P@ssw0rd.
5.5	Captured credentials by forced authentication of a rogue server	4	FTPSERVER, MSSQLSERVER, workgroup	It is recommended to disable the LLNMR Protocol in the group policy settings. By going to 'Computer Configuration/Policies/Administrative Templates/Network/DNS Client/Turn off Multicast Name Resolution'. The same can happen with NetBIOS or Multicast-DNS hence consider disabling them as well.
2.3	Discovered closed ports on the host	19	192.168.1.1, 192.168.1.10, 192.168.1.106, 192.168.1.12, 192.168.1.123, 192.168.1.18, 192.168.1.244, 192.168.1.29,...	If closed ports are reachable through the firewall, they can be abused. It is recommended to block closed ports via firewalling to prevent malicious software from establishing a C2 channel through a closed port.
0.0	Host supports SMBv1 protocol	1	192.168.1.45	Disable support for SMBv1 on all Windows hosts in the network.

Herman Motors

Pen Test Overview

25 Total Vulnerabilities Detected

1Critical

4High

0Medium

20Low

Click to expand for vulnerability details

17 Total Achievements

Every achievement represents a discrete successful action performed by the penetration test.

1Critical

11High

0Medium

5Low

Click to expand for achievement details

23 Discovered Hosts

0Critical

0High

0Medium

23Low

0Win Workstation

19Linux


0Win Server

0Network Devices

0Generic Windows

4Other

Click to see host details



COMPLYAUTO

PRIVACY

Dashboard

Requests

Locations

Vendors

Surveys

Manage

Request Portal

Notices

Users

Learning Center

Employee Training

Federal Safeguards

Risk Assessments

ISP Policy Builder

Data Map

Phishing

Template Library

Employee Mailing Lists



Campaign Benchmarking

Open Rate

Click Rate

Penetration Rate

1.22%

5.37%

4.31%

Your Latest Test

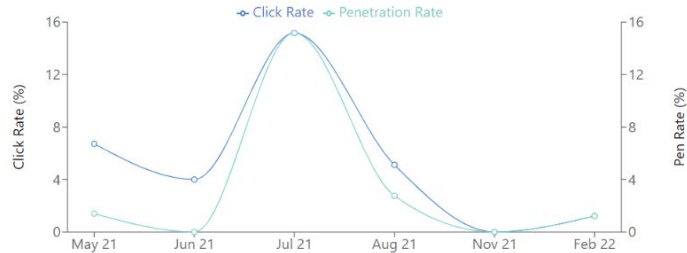
Your Average

Other Dealers' Average

Testing Effectiveness

Performance Over Time

Reduction Rate



Repeat Offenders

Employee Name	# of Times Phished	Date Last Phished
Berenice Satterfield	5	2/24/2022
Willow Douglas	5	2/24/2022

Active Phishing Simulations

Test Name	Start Date	End Date
DoorDash - Free Cheesecake	2/13/2022	2/27/2022
United Airlines - Promotion	2/13/2022	2/27/2022
LinkedIn - Connection Request	2/13/2022	2/27/2022
UPS - Delivery Update	2/13/2022	2/27/2022

Recent Actions

Template	Employee	Action	Date
LinkedIn - Connection Request	Heber Barton	Replied	2/26/2022
DoorDash - Free Cheesecake	Neoma Thompson	Hacked	2/26/2022
LinkedIn - Connection Request	Miller Walter	Opened	2/26/2022
DoorDash - Free Cheesecake	Heber Barton	Opened	2/26/2022
LinkedIn - Connection Request	Kameron Lebsack	Hacked	2/25/2022

Showing 1 to 5 of 24 entries

< 1 2 3 4 5 >

Training Required

Search	Q
--------	---



Dashboard

Requests

Locations

Vendors

Surveys

Manage

Request Portal

Notices

Users

Learning Center

Employee Training

Federal Safeguards

Risk Assessments

ISP Policy Builder

Data Map

Phishing

Template Library

Employee Mailing Lists



Explore Available T

Name

CDK - DMS Security Alert

Email Template Preview



CDK Global

1950 Hassell Road, Hoffman
Estates, IL
847.397.1700

© 2021 CDK Global LLC / CDK Global is a trademark of CDK Global LLC.

Security Alert : {fname} {lname}'s Account for {company}

CDK has recently detected suspicious activity regarding your account. Please login immediately to reset your password.

Failure to do so may result in your account being compromised.

CDK prides itself on taking the necessary precautions to keep you and your dealership safe from cybersecurity threats.

{hook_link}

Close

Refresh

Landing Page

Date Added



7/16/2021

- Dashboard
- Requests
- Locations
- Vendors
 - Surveys
 - Manage
- Request Portal
- Notices
- Users
- Learning Center
- Employee Training
- Federal Safeguards
 - Risk Assessments
 - ISP Policy Builder
- Data Map
- Phishing
 - Template Library
 - Employee Mailing Lists

Explore Available T

Name

CDK - DMS Security Alert

Landing Page Preview



Username:

Password:

Sign In

☐ Remember Me

Close

Refresh

Landing Page

Date Added



7/16/2021

OTHER REQUIREMENTS

- **Performing both a data and systems inventory**
 - i. This requirement was designed to ensure that companies inventory the data in their possession and inventory the systems on which that data is collected, stored, or transmitted.
- **Annual written report to your Board of Directors or senior management.** Must include:
 - i. The overall status of the ISP and compliance with the Revised Rule; and
 - ii. Material matters related to the ISP, addressing issues such as risk assessments, 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.
- **Implementing secure access controls**
 - i. Includes technical controls, limitations on customer access to their own records, and physical controls

Dashboard



Requests



Locations



Vendors



Surveys

Manage

Request Portal



Notices



Users



Learning Center



Employee Training



Federal Safeguards



Risk Assessments

ISP Policy Builder

Data Map



Phishing



Template Library

Employee Mailing Lists

Interactive Data Map

Filter by

SubFilter by

Location

Personal Information

None (Show All)

All Locations

PERSONAL INFORMATION	VENDOR TYPES	SYSTEMS	DEPARTMENTS	INTERACTIONS
Audio/Video/Visual	401k Providers & Administrators	10th Degree	Digital and Telemarketing	Current or past employee
Biometric	Appraisal Tools	11 sight	Human Resources	Email communications
Commercial	Auctions & Wholesalers	700Credit	Parts & Service	Internet leads or online activity
Customer Records	Background Check Companies	Accurate Background	Rentals	Job applicant
Education	Call Tracking & Phone Solutions	Ace Small Claims Service	Sales and F&I	Over-the-counter parts transactions
Geolocation	Chat Modules	Acensus		Phone calls, voicemails, and text messages
Identifiers	Check Guarantee Companies	ActiveEngage		Service customer
Inferences	COBRA Administrators	Acura		Service loaner activity
Internet Activity	Consumer Defense Attorneys	Administrative Solutions		Test drive records
Professional/Employment	Credit Reporting & Compliance Systems	Advantage Group		Vehicle cash transaction
Protected Classes	Credit Reporting Agencies (CRAs)	Alliance Credit Union		Vehicle lease or finance transaction
	Customer Relations Management (CRM)	American Fidelity		Vehicle rental
	Data Analytics Tools	American Funds 401		Vehicle subscription deliveries
	Dealer Management System (DMS)	American Honda Protection Products Corporation		
	Debt Collection Agencies & Repossession Companies	Ameritrust		
	Deskling Tools	AMI Success		
	Digital Retailers & eCommerce Platforms	AON		
	Direct Mailers	Applicant Tracking		
	DMV Title & Registration Software	Arent Fox		
	Electronic Estimate & Invoice Tools	Associated Pension Consultants		
	Electronic F&I Menu Systems	Auctions in Motion		
	Email Blasts	Audi Financial Services		
	Employment Law Firms	AutoAlert		
	Environmental Health & Safety Consultants	AutoLoop		
	F&I Product Providers & Administrators	Automate		
	Financial Institutions	Automotive Product Consultants		
	Government Entities	Automotive Systems Analysis		

Interested in the solution?

Let ComplyAuto help ease the burden and cost of compliance.

SCHEDULE A DEMO

<https://complyauto.com/schedule-demo/>

TRANSPARENT PRODUCT PRICING

Single rooftop dealers: <https://complyauto.com/pricing-single/>

Dealer groups: <https://complyauto.com/pricing-groups/>

CONTACT US

chris@complyauto.com
CEO & Co-Founder
(385) 277-5882



<https://www.complyauto.com>



Facts

- The NADA estimated that the new rules would cost even small dealers \$276,925 per year.
- Penalties for non-compliance are \$46,517 per violation.
- ComplyAuto represents 1,900+ dealers nationwide with a 100% client retention rate.
- ComplyAuto is a purpose-built solution by and for dealers.