Achieving Compliance with the FTC Safeguards Rule

Presented on August 24, 2022

by Hao Nguyen

General Counsel, ComplyAuto

www.complyauto.com

This presentation is intended to be used as a compliance aid for New Mexico dealers. Reasonable efforts have been made to ensure the accuracy of the following subject matter. No express or implied warranty is provided respecting the information contained in this presentation. **The following material should not be construed as (nor used as a substitute for) legal advice.** If legal advice is required, the services of a competent professional should be sought. Each dealer must rely on its own expertise and knowledge of law when using the material provided.

Legal Disclaimer

Chris Cleveland
Compliance Director, Galpin Motors
CEO & Co-Founder, ComplyAuto Privacy

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

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

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

Sherryl Brightwell Nens
Vice President of Sales
Dealer Relations Manager, Ford Motor Co. *(former)*

About ComplyAuto

- Over **3,500** dealers use the ComplyAuto software for compliance with state & federal privacy/cybersecurity requirements.
- Endorsed by the +35 state dealer associations.
- Partnered with the NADA and drafted portions of their new FTC Safeguards Manual.

NADA AFFINITY PROVIDER
CNCDA California New Car Dealers Association
FADA
njcar
kada Kentucky Automobile Dealers Association
OADA
GCADA Georgia Automobile Dealers Association
VADA Virginia Automobile Dealers Association
MTADA Montana Automobile Dealers Association
Kansas Automobile Dealers Association
AFAP
NYSADA New York State Automobile Dealers Association
New Car Dealers of Utah Since 1923
MADA
maada
ADCO Association of Dealership Compliance Officers
AADA Arizona Automobile Dealers Association
Iowa Automobile Dealers Association
Tennessee Automotive Association
ADAA Automobile Dealers Association of Alabama, Inc.
MADA Mississippi Automobile Dealers Association
ARDA Arkansas Automobile Dealers Association
Colorado Automobile Dealers Association
TADA Texas Automobile Dealers Association ENDORSED
CAR
Connecticut Automotive Retailers Association
Maryland Automobile Dealers Association
New Mexico Automotive Dealers Association
DAADA
IADA Idaho Automobile Dealers Association
WVADA West Virginia Automobile Dealers Association
WADA Wyoming Automobile Dealers Association
VADA Vermont
GADA Services, Inc.

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 if 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 help 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

APPLICABLE LAW OR REGULATION

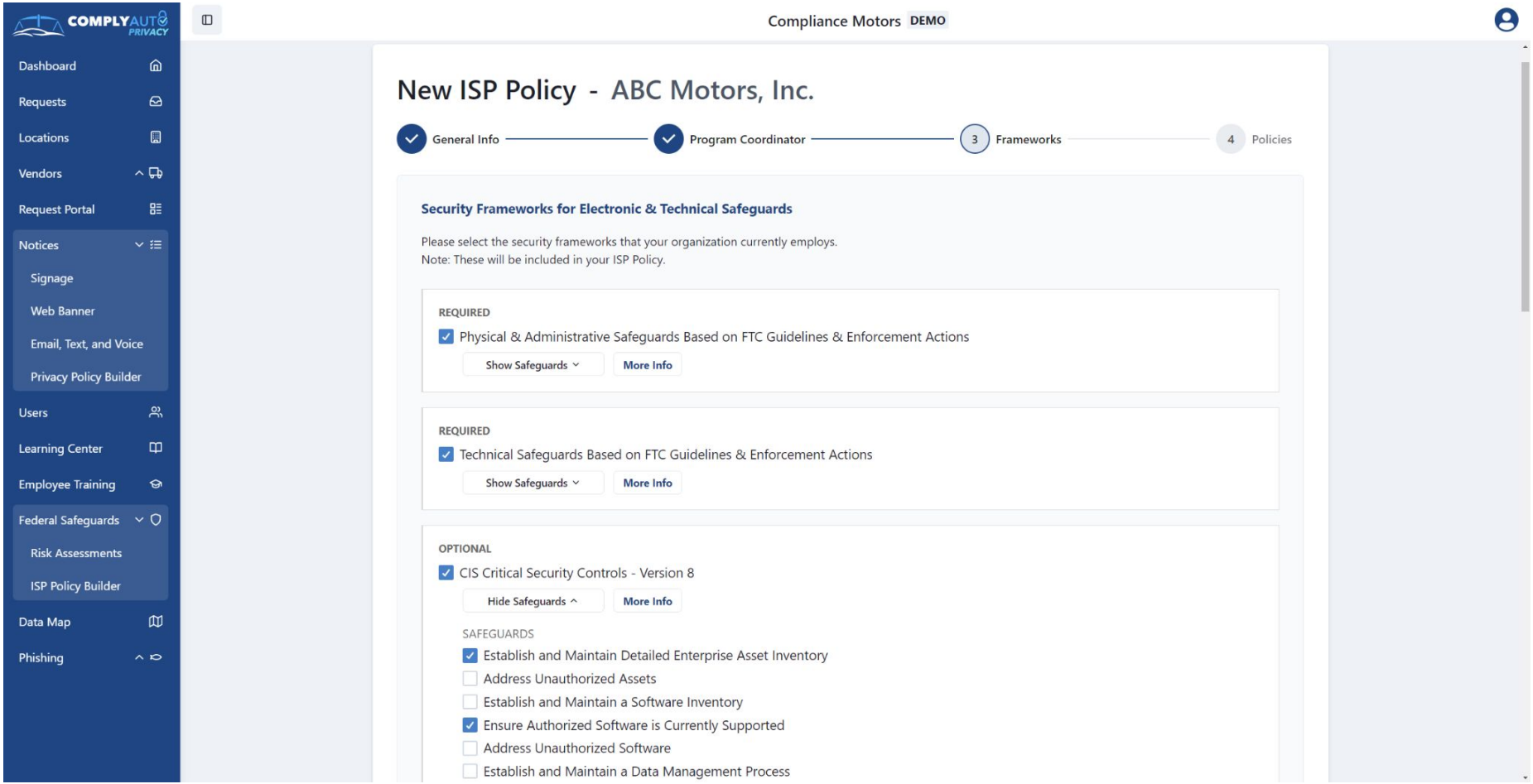
16 CFR §314.4(c)(6)-(7), §314.4(c)(6)(h)(1)

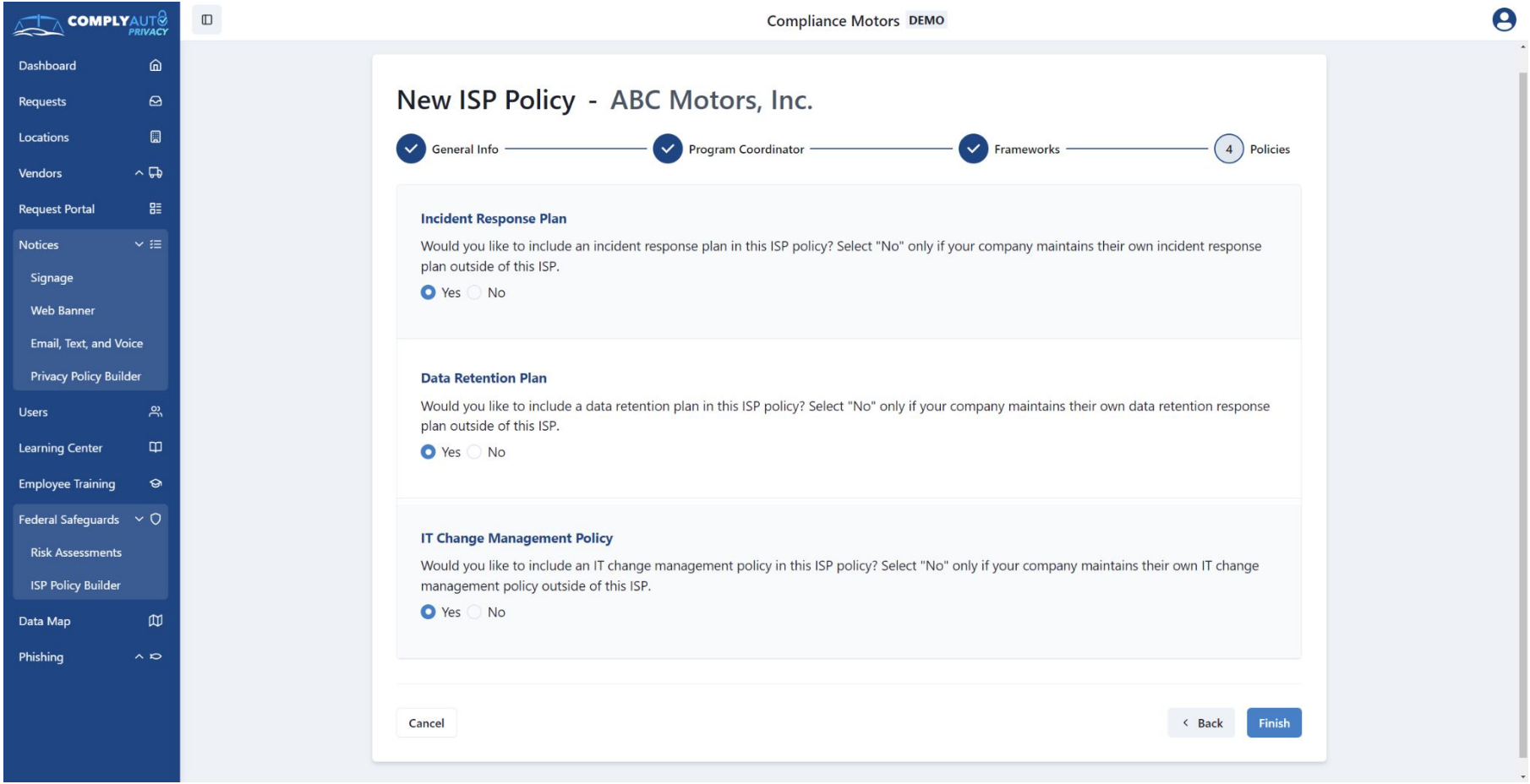
Dealers must have a written Information Security Program and Incident Response Plan that is made available to employees.

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
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


COMPLYAUTO PRIVACY
Compliance Motors DEMO
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


COMPLYAUTO PRIVACY
Compliance Motors DEMO
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 "QUALIFIED INDIVIDUAL" TO OVERSEE YOUR ISP

- It is generally recommended that this be a Chief Information Security Officer, IT Director, or person in a similar role.

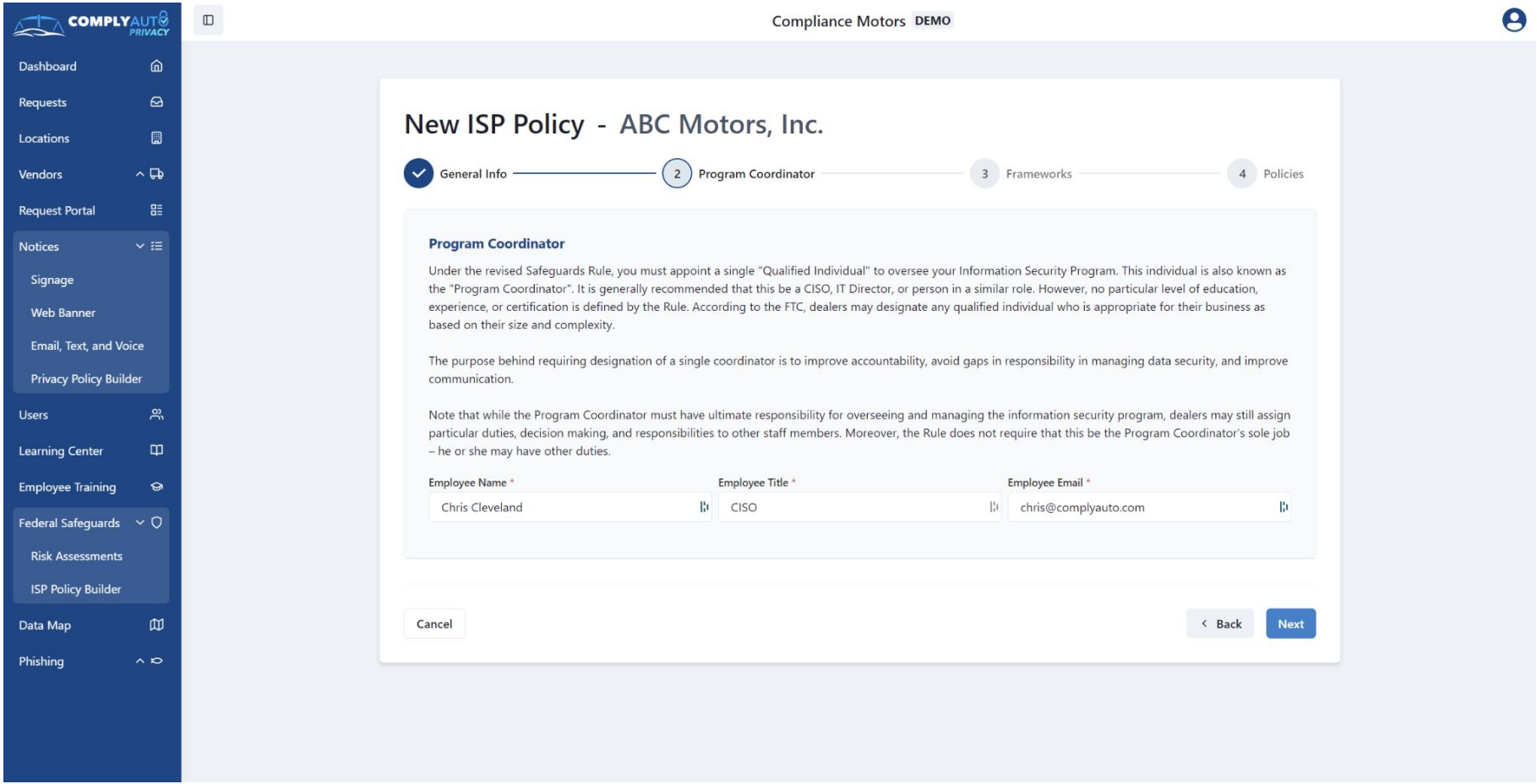
- Goal is to improve accountability, avoid gaps in responsibility in managing data security, and improve communication. Splitting authority over an information security program between two or more people may lead to failures of communications and oversight.

- "Qualified Individual" 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"


COMPLYAUTO PRIVACY
Compliance Motors DEMO
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
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

DOCUMENTED INTERNAL RISK ASSESSMENTS

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.

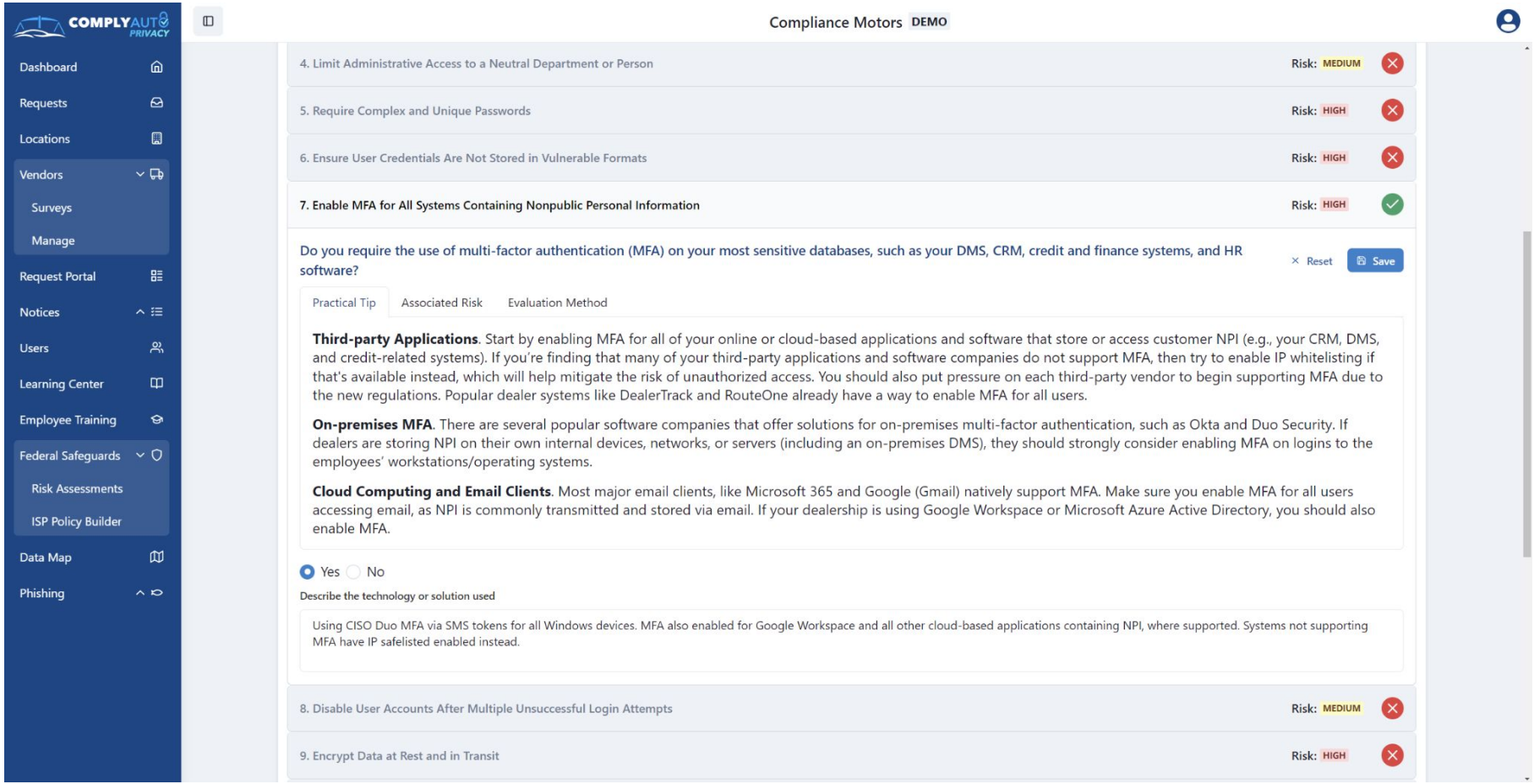
Risk assessments should test for, and incorporate the following:

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
Compliance Motors DEMO
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
Surveys
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

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.

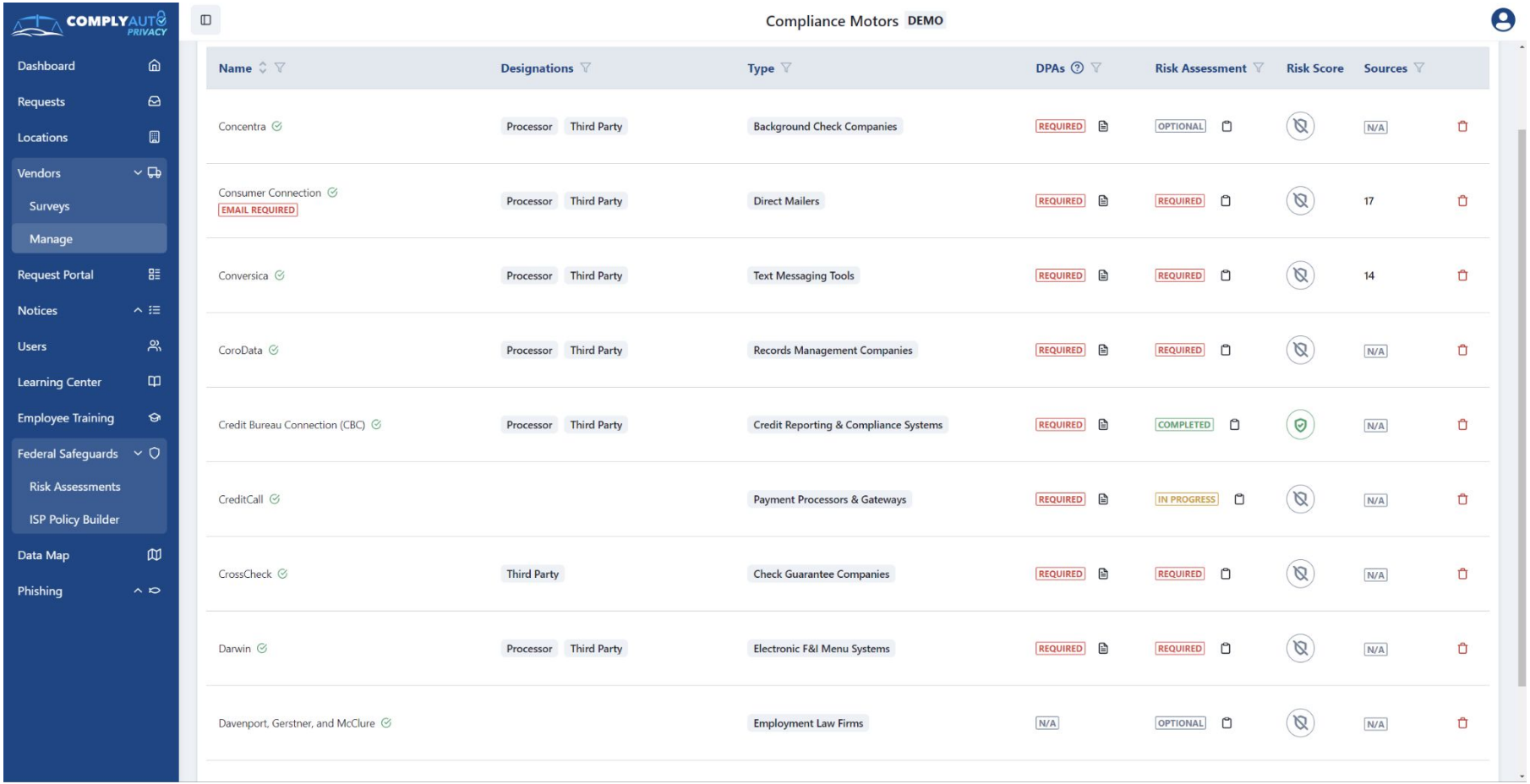
Who needs to sign a GLBA Service Provider Addendum?

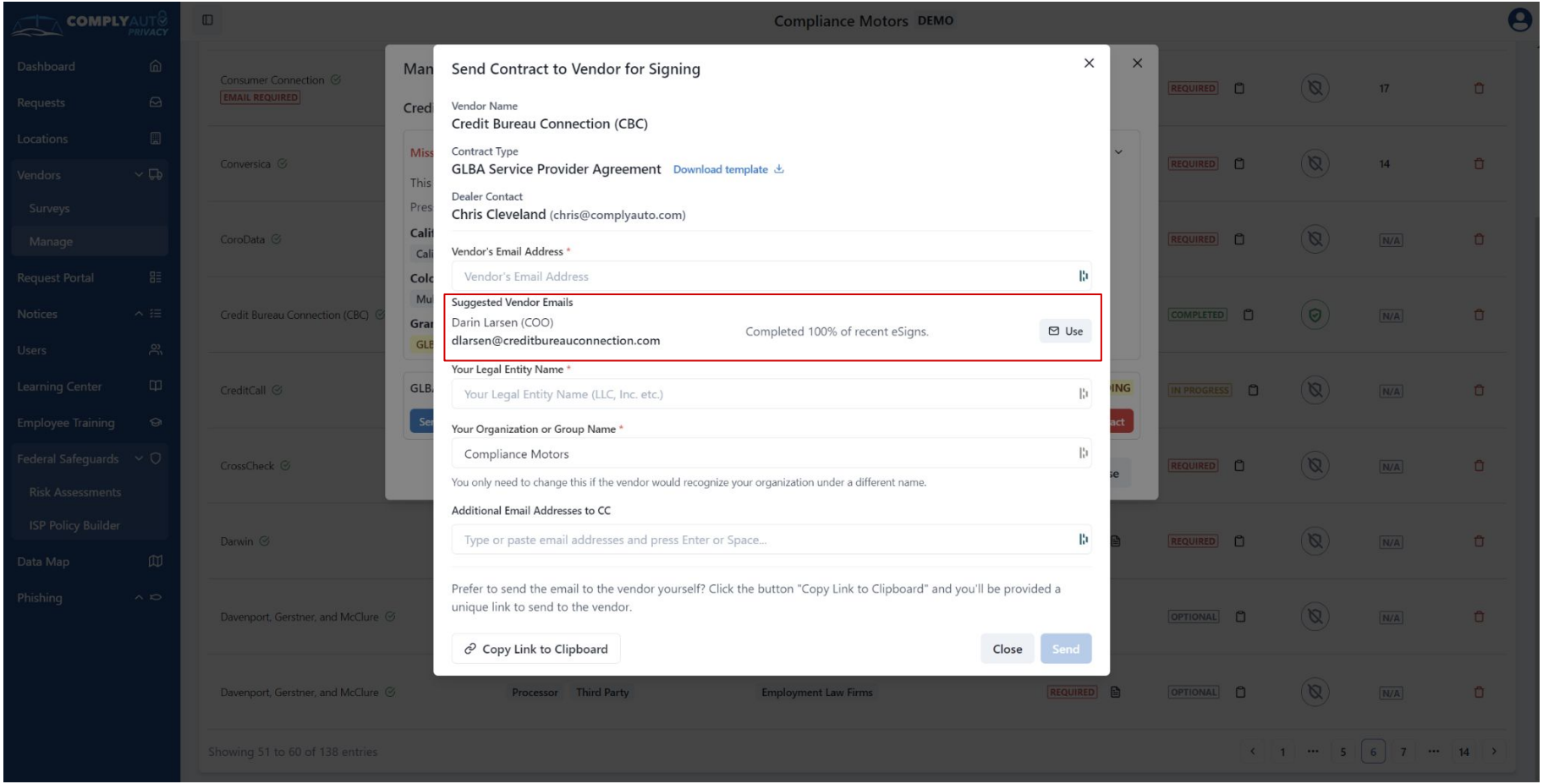
Any vendor who collects or processes NPI.

What if they refuse to sign?

- Remind the service provider that they may be independently required to comply with the Revised Rule

- Determine if there's an existing contract with language that already satisfies the requirements of the Revised Rule. 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).


COMPLYAUTO PRIVACY
Compliance Motors DEMO
Dashboard
Requests
Locations
Vendors
Surveys
Manage
Request Portal
Notices
Users
Learning Center
Employee Training
Federal Safeguards
Risk Assessments
ISP Policy Builder
Data Map
Phishing
Name
Designations
Type
DPAs
Risk Assessment
Risk Score
Sources
Concentra
Processor
Third Party
Background Check Companies
REQUIRED
OPTIONAL
N/A
Consumer Connection
EMAIL REQUIRED
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


Compliance Motors DEMO
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 *
Vendor's Email Address
Suggested Vendor Emails
Darin Larsen (COO)
dlarsen@creditbureauconnection.com
Completed 100% of recent eSigns.
Use
Your Legal Entity Name *
Your Legal Entity Name (LLC, Inc. etc.)
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

VENDOR RISK ASSESSMENTS

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.

Dealers must now periodically 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.

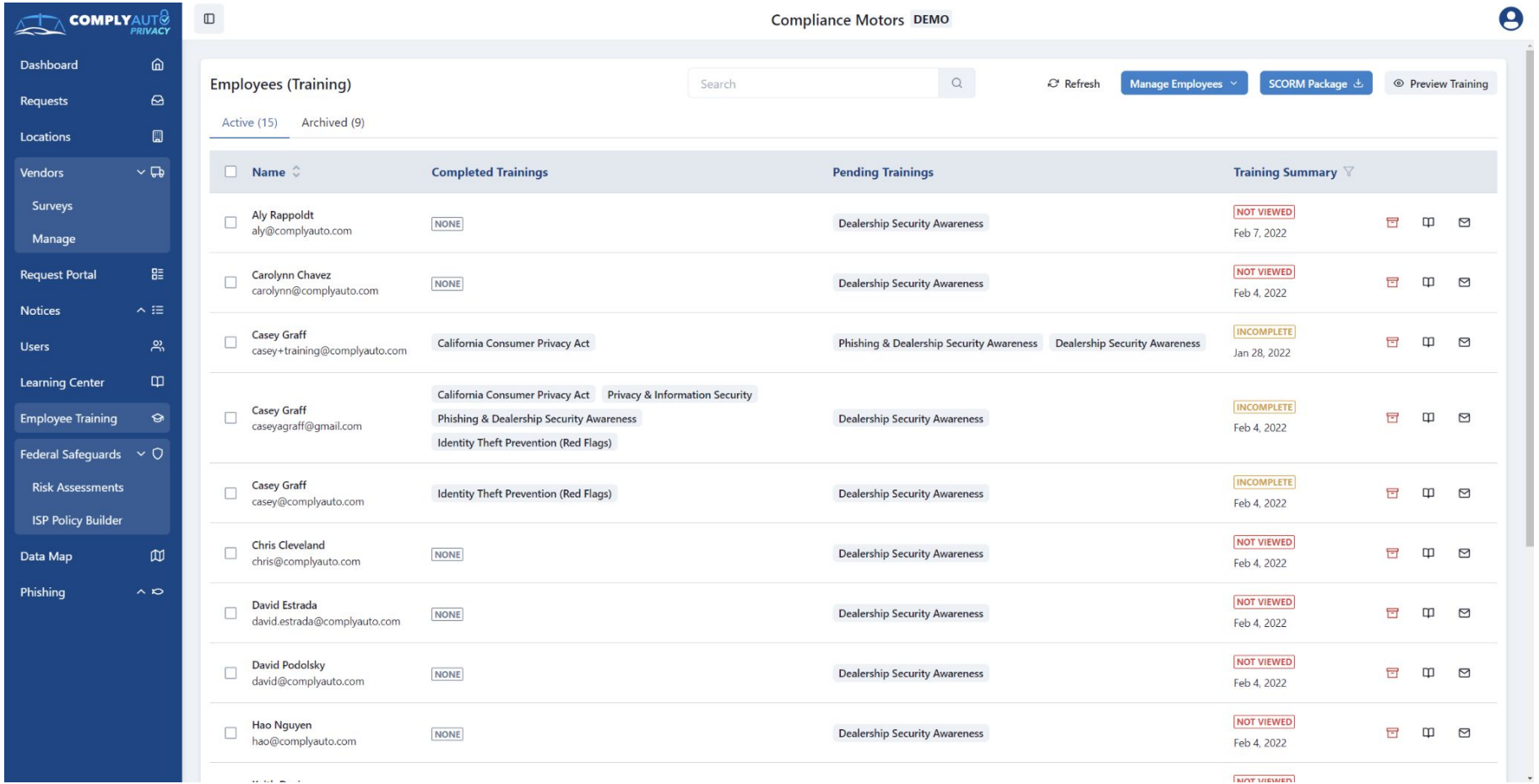
APPLICABLE LAW OR REGULATION

16 CFR §314.4(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.


COMPLYAUTO PRIVACY
Compliance Motors DEMO
Dashboard
Requests
Locations
Vendors
Surveys
Manage
Request Portal
Notices
Users
Learning Center
Employee Training
Federal Safeguards
Risk Assessments
ISP Policy Builder
Data Map
Phishing
Employees (Training)
Search
Refresh
Manage Employees
SCORM Package
Preview Training
Active (15)
Archived (9)
Name
Completed Trainings
Pending Trainings
Training Summary
Aly Rappoldt
aly@complyauto.com
NONE
Dealership Security Awareness
NOT VIEWED
Feb 7, 2022
Carolynn Chavez
carolynn@complyauto.com
NONE
Dealership Security Awareness
NOT VIEWED
Feb 4, 2022
Casey Graff
casey+training@complyauto.com
California Consumer Privacy Act
Phishing & Dealership Security Awareness
Dealership Security Awareness
INCOMPLETE
Jan 28, 2022
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
Casey Graff
casey@complyauto.com
Identity Theft Prevention (Red Flags)
Dealership Security Awareness
INCOMPLETE
Feb 4, 2022
Chris Cleveland
chris@complyauto.com
NONE
Dealership Security Awareness
NOT VIEWED
Feb 4, 2022
David Estrada
david.estrada@complyauto.com
NONE
Dealership Security Awareness
NOT VIEWED
Feb 4, 2022
David Podolsky
david@complyauto.com
NONE
Dealership Security Awareness
NOT VIEWED
Feb 4, 2022
Hao Nguyen
hao@complyauto.com
NONE
Dealership Security Awareness
NOT VIEWED
Feb 4, 2022

COMPLYAUTO PRIVACY

Compliance Motors DEMO

Dashboard
Locations
Vendor Management
Surveys
Manage
Privacy
Risk Assessments
Cybersecurity
Policies
Employee Training
Data Mapping
Users
Learning Center

Employe
Enroll your emplo

FULLY TRAINED
1 /8 Completed

LAST EMPLOYEE ADDED
24 days ago

Search

SCORM Package
Preview Training

Active 8

Name

Aly Rapp
aly@comp

Amy Bruz
amy@cor

Casey Gr
casey+tra

Chris Cle
chris@co

John Doe
john@exa

Melody
graffmelo

Miranda
miranda@

Zach Tuc
zach@co

Training Summary

NOT VIEWED Aug 18, 2022
COMPLETE Jun 28, 2022
INCOMPLETE Aug 18, 2022
INCOMPLETE Aug 18, 2022
NONE ASSIGNE
INCOMPLETE Aug 18, 2022
INCOMPLETE Aug 18, 2022
NO ATTEMPTS Aug 18, 2022

10 Showing 1 - 8 of 8

Select Training Module

Adverse Action Notices

Covers when and how dealers need to send out "adverse action notices" under federal law.

Who Duration

California Consumer Privacy Act

An overview of dealerships' requirements under the California Consumer Privacy Act (CCPA) and consumers' privacy rights.

Who Duration

Cash Reporting & Anti-Money Laundering

A detailed overview of IRS cash reporting and anti-money laundering requirements, including training employees on properly completing IRS Form 8300, avoiding "structuring", and related topics.

Who Duration

Credit Score Disclosure Notices (California)

This simple course will cover the California version of the Risk-Based Pricing Rule and when and how dealership personnel must provide customers with a Credit Score Disclosure Notice.

Who Duration

Credit Score Disclosure Notices (Federal)

This simple course will cover the federal Risk-Based Pricing Rule and when and how dealership personnel must provide customers with a Credit Score Disclosure Notice.

Who Duration

Dealership Security Awareness

Required training for all employees that identifies best practices relating to information security and data protection, including the latest risks.

Who Duration

Identity Theft Prevention (Red Flags)

Practical training on how to spot and prevent identity theft in the dealership.

Who Duration

OFAC Sanctions Compliance

Policies and procedures for complying with the Office of Foreign Assets Control (OFAC) guidelines on prohibited transactions with individuals on the federal Specially Designated Nationals (SDN) list.

Who Duration

Phishing Awareness

How to identify and avoid phishing and social engineering scams.

Who Duration

Unfair & Deceptive Acts & Practices (UDAP)

Unfair & Deceptive Acts & Practices (UDAP)

Who Duration

Close

REQUIRED ANNUAL PENETRATION TESTING

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.

Penetration testing mimics real-world attacks 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**.

⌘ **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. “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.

APPLICABLE LAW OR REGULATION

16 CFR §314.4(d)(1)(ii)

Dealers must perform vulnerability assessments at least biannually.

Note: EDR/MDR/XDR/SIEM does not satisfy true "continuous monitoring"

REQUIRED BIANNUAL VULNERABILITY ASSESSMENTS

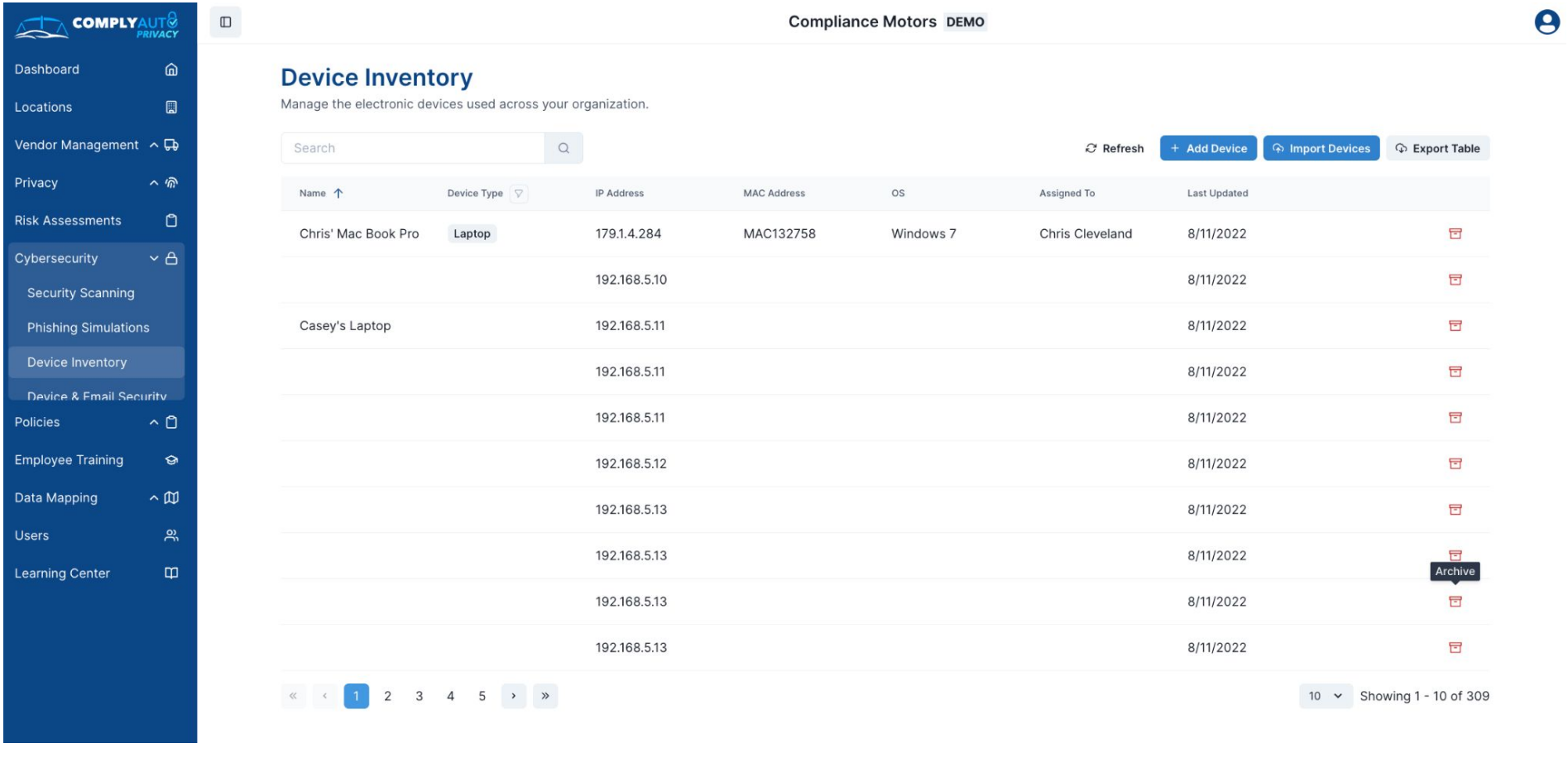
A vulnerability assessment is a scan of the entire IT environment in which all installed software is identified and checked for any publicly known security vulnerabilities.

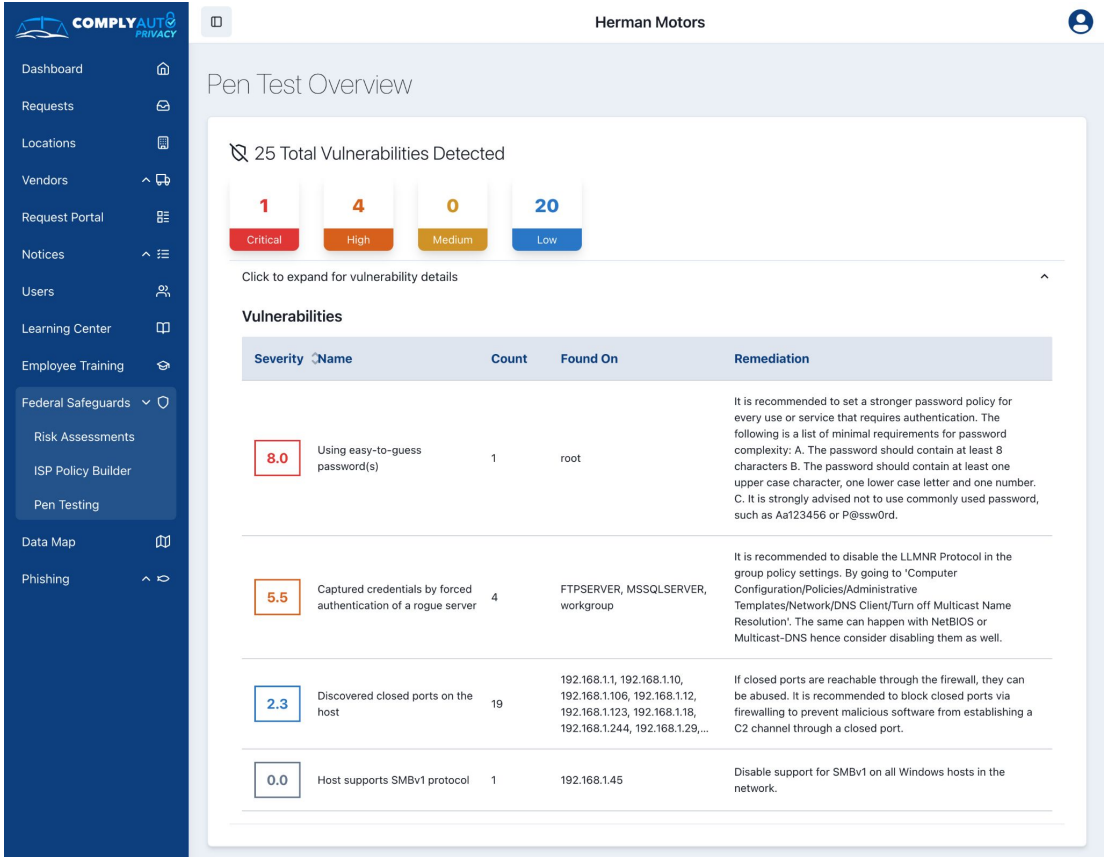
Under the Revised Rule, vulnerability assessments must be performed once at least every six months.

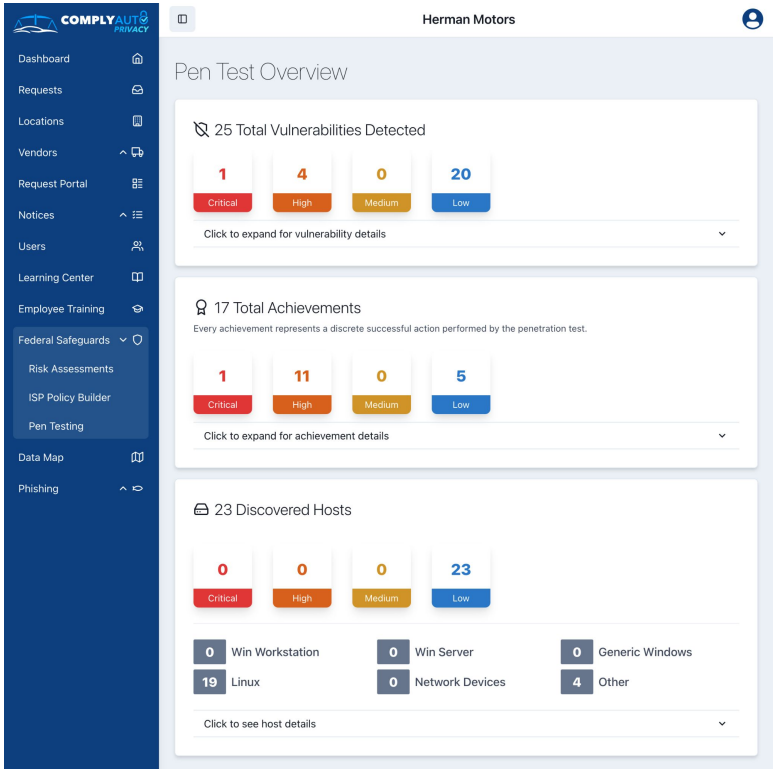
⌘ TECHNOLOGY TIP

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. Vist 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.

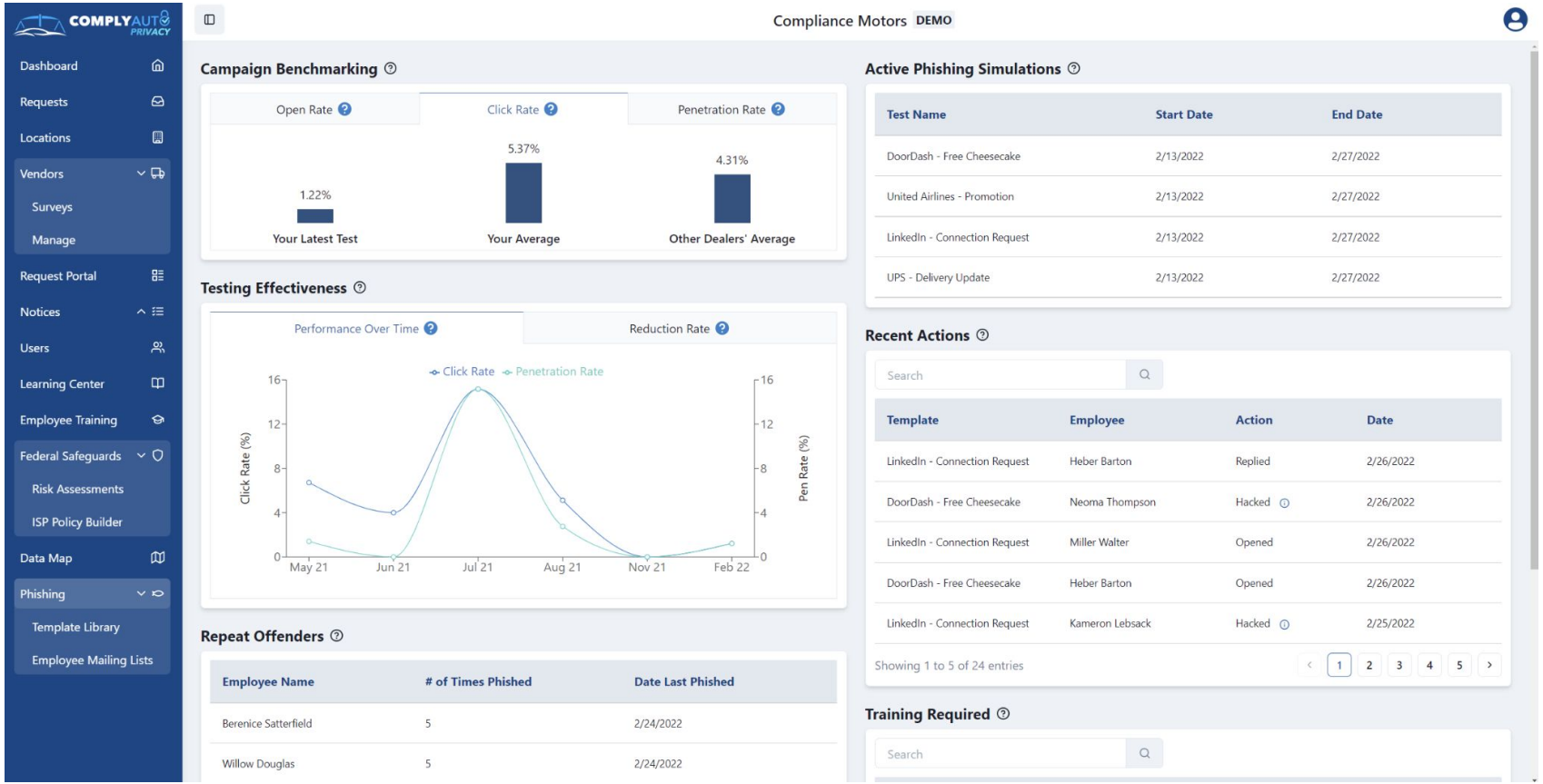
However, dealers are advised to consult with experienced IT personnel before attempting to install and run these open source tools themselves.

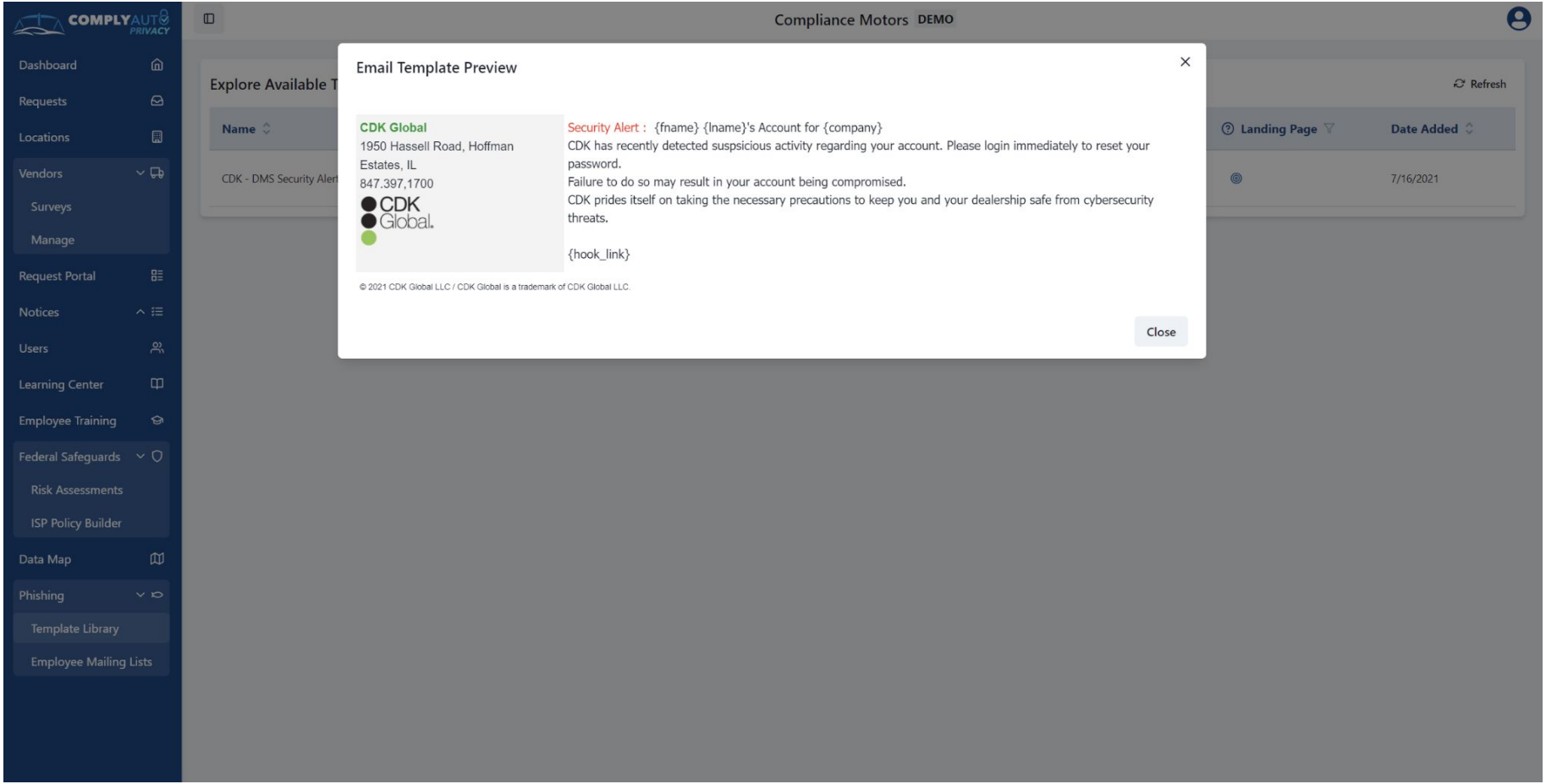

COMPLYAUTO PRIVACY
Compliance Motors DEMO
Dashboard
Locations
Vendor Management
Privacy
Risk Assessments
Cybersecurity
Security Scanning
Phishing Simulations
Device Inventory
Device & Email Security
Policies
Employee Training
Data Mapping
Users
Learning Center
Device Inventory
Manage the electronic devices used across your organization.
Search
Refresh
Add Device
Import Devices
Export Table
Name
Device Type
IP Address
MAC Address
OS
Assigned To
Last Updated
Chris' Mac Book Pro
Laptop
179.1.4.284
MAC132758
Windows 7
Chris Cleveland
8/11/2022
192.168.5.10
8/11/2022
Casey's Laptop
192.168.5.11
8/11/2022
192.168.5.11
8/11/2022
192.168.5.11
8/11/2022
192.168.5.12
8/11/2022
192.168.5.13
8/11/2022
192.168.5.13
8/11/2022
Archive
192.168.5.13
8/11/2022
192.168.5.13
8/11/2022
1
2
3
4
5
10
Showing 1 - 10 of 309

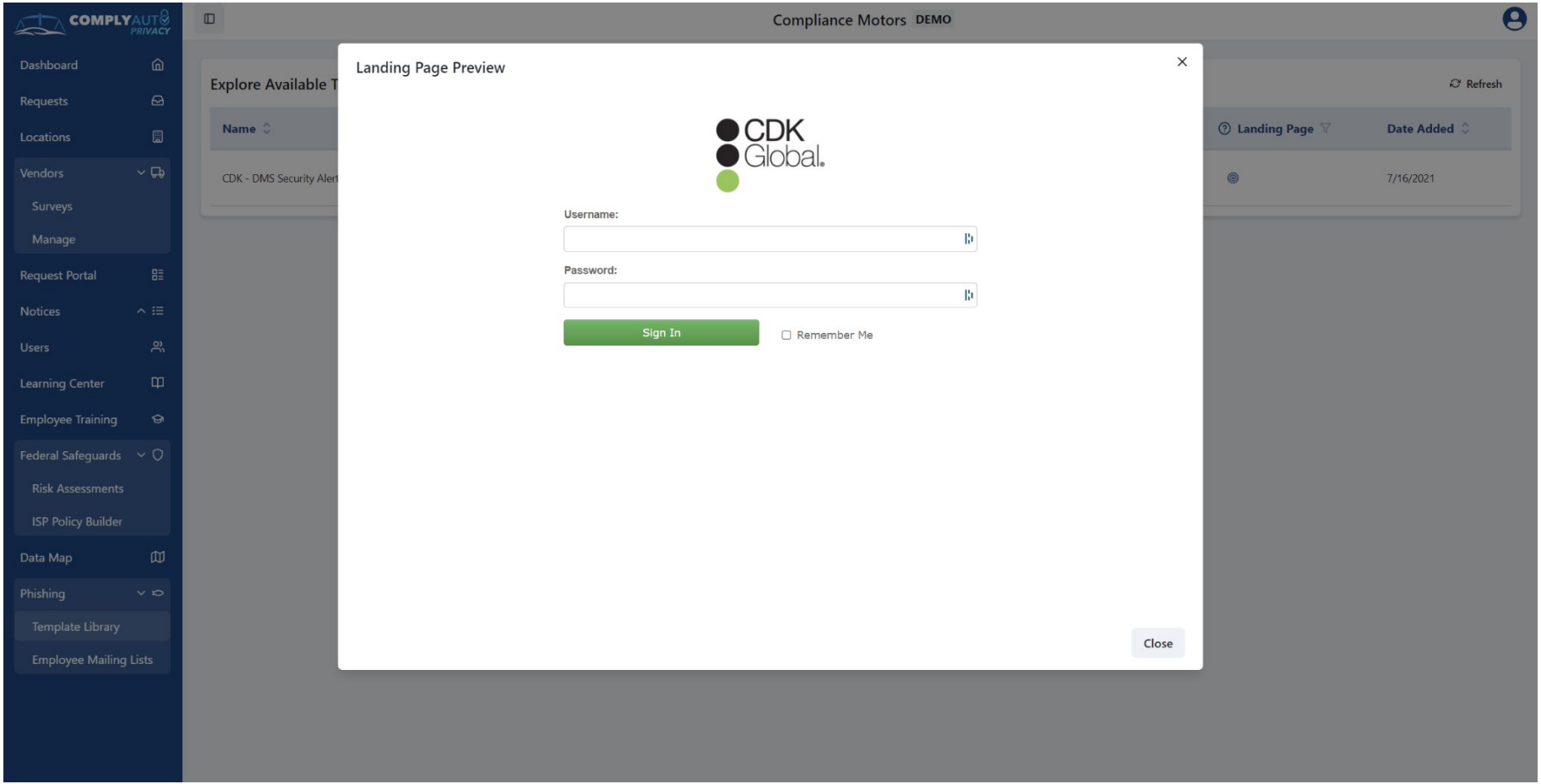

COMPLYAUTO PRIVACY
Herman Motors
Dashboard
Requests
Locations
Vendors
Request Portal
Notices
Users
Learning Center
Employee Training
Federal Safeguards
Risk Assessments
ISP Policy Builder
Pen Testing
Data Map
Phishing
Pen Test Overview
25 Total Vulnerabilities Detected
1 Critical
4 High
0 Medium
20 Low
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 LLMNR 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.


COMPLYAUTO PRIVACY
Herman Motors
Dashboard
Requests
Locations
Vendors
Request Portal
Notices
Users
Learning Center
Employee Training
Federal Safeguards
Risk Assessments
ISP Policy Builder
Pen Testing
Data Map
Phishing
Pen Test Overview
25 Total Vulnerabilities Detected
1 Critical
4 High
0 Medium
20 Low
Click to expand for vulnerability details
17 Total Achievements
Every achievement represents a discrete successful action performed by the penetration test.
1 Critical
11 High
0 Medium
5 Low
Click to expand for achievement details
23 Discovered Hosts
0 Critical
0 High
0 Medium
23 Low
0 Win Workstation
0 Win Server
0 Generic Windows
19 Linux
0 Network Devices
4 Other
Click to see host details

PHISHING SIMULATION SOFTWARE

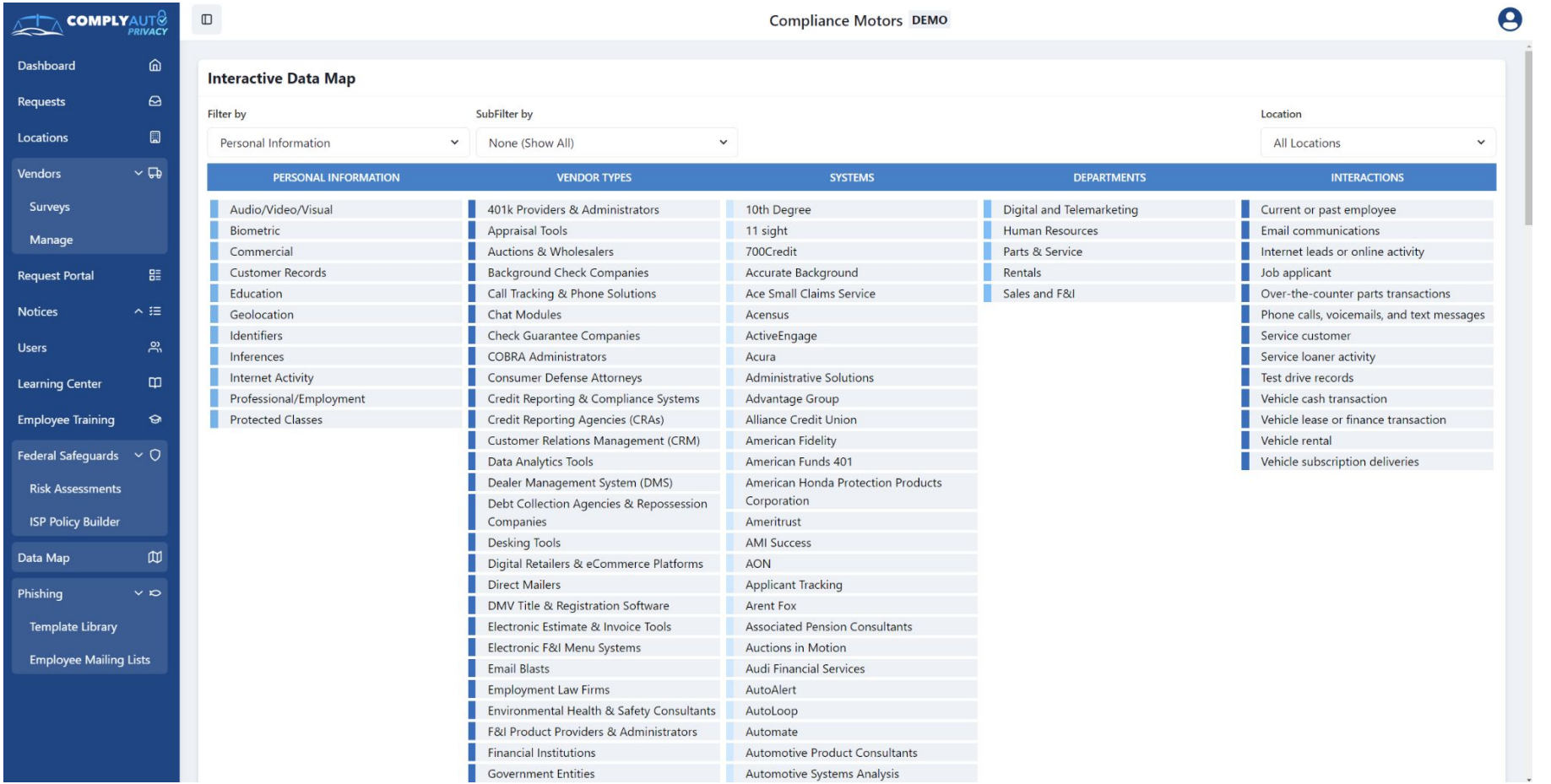



COMPLYAUTO PRIVACY
Compliance Motors DEMO
Dashboard
Requests
Locations
Vendors
Surveys
Manage
Request Portal
Notices
Users
Learning Center
Employee Training
Federal Safeguards
Risk Assessments
ISP Policy Builder
Data Map
Phishing
Template Library
Employee Mailing Lists
Explore Available T
Refresh
Name
Landing Page
Date Added
CDK - DMS Security Alert
7/16/2021
Email Template Preview
CDK Global
1950 Hassell Road, Hoffman Estates, IL
847.397.1700
CDK Global.
Security Alert : {fname} {lname}'s Account for {company}
CDK has recently detected suspsicious 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}
© 2021 CDK Global LLC / CDK Global is a trademark of CDK Global LLC.
Close


COMPLYAUTO PRIVACY
Compliance Motors DEMO
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
Refresh
Name
Landing Page
Date Added
CDK - DMS Security Alert
7/16/2021
Landing Page Preview
CDK Global.
Username:
Password:
Sign In
Remember Me
Close

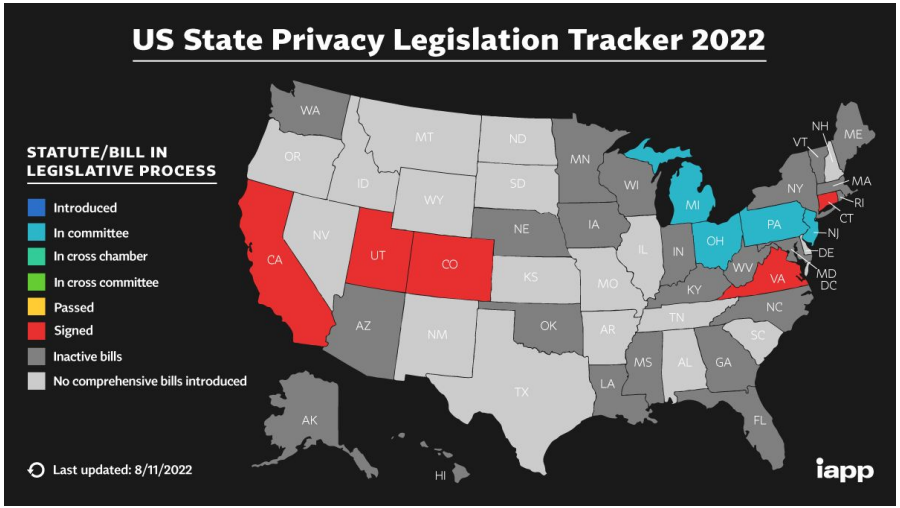
OTHER REQUIREMENTS

- **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


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
Compliance Motors DEMO
Interactive Data Map
Filter by
Personal Information
SubFilter by
None (Show All)
Location
All Locations
PERSONAL INFORMATION
Audio/Video/Visual
Biometric
Commercial
Customer Records
Education
Geolocation
Identifiers
Inferences
Internet Activity
Professional/Employment
Protected Classes
VENDOR TYPES
401k Providers & Administrators
Appraisal Tools
Auctions & Wholesalers
Background Check Companies
Call Tracking & Phone Solutions
Chat Modules
Check Guarantee Companies
COBRA Administrators
Consumer Defense Attorneys
Credit Reporting & Compliance Systems
Credit Reporting Agencies (CRAs)
Customer Relations Management (CRM)
Data Analytics Tools
Dealer Management System (DMS)
Debt Collection Agencies & Repossession Companies
Desking Tools
Digital Retailers & eCommerce Platforms
Direct Mailers
DMV Title & Registration Software
Electronic Estimate & Invoice Tools
Electronic F&I Menu Systems
Email Blasts
Employment Law Firms
Environmental Health & Safety Consultants
F&I Product Providers & Administrators
Financial Institutions
Government Entities
SYSTEMS
10th Degree
11 sight
700Credit
Accurate Background
Ace Small Claims Service
Acensus
ActiveEngage
Acura
Administrative Solutions
Advantage Group
Alliance Credit Union
American Fidelity
American Funds 401
American Honda Protection Products Corporation
Ameritrust
AMI Success
AON
Applicant Tracking
Arent Fox
Associated Pension Consultants
Auctions in Motion
Audi Financial Services
AutoAlert
AutoLoop
Automate
Automotive Product Consultants
Automotive Systems Analysis
DEPARTMENTS
Digital and Telemarketing
Human Resources
Parts & Service
Rentals
Sales and F&I
INTERACTIONS
Current or past employee
Email communications
Internet leads or online activity
Job applicant
Over-the-counter parts transactions
Phone calls, voicemails, and text messages
Service customer
Service loaner activity
Test drive records
Vehicle cash transaction
Vehicle lease or finance transaction
Vehicle rental
Vehicle subscription deliveries

CONSUMER PRIVACY RIGHTS

- Some state laws require the honoring of Global Privacy Controls (GPCs) and “Do Not Track Signals”.
- Some state laws regulate the deployment of third-party tracking cookies for retargeted advertising & provide consumers with other privacy rights, opt-out, deletion, access, and correction.
- Plaintiff attorneys often file lawsuits relating to third-party tracking cookies deployed without their consent.
- State Attorneys General have taken enforcement action across state line related to cookies and online tracking.



A common misconception that only dealerships in those states need to comply, but dealerships have potential exposure, if they are collecting information on CA, VA, CO, or UT residents who shop or browse online.

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

Hao@ComplyAuto.com
General Counsel
(661) 347-38309
https://www.complyauto.com

NADA AFFINITY PROVIDER

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.
- Average Pen Tests cost $15K - $30K per dealership
- ComplyAuto represents 3,500+ dealers nationwide with a 100% client retention rate.
- ComplyAuto is a purpose-built solution by and for dealers for 100% of your FTC Safeguards Compliance needs

COMPLYAUTO PRIVACY

NADA AFFINITY PROVIDER

By dealers, for dealers. A turnkey solution for privacy & cybersecurity compliance.

+3,500
Active Dealers

+35
Endorsements from State Dealer Associations

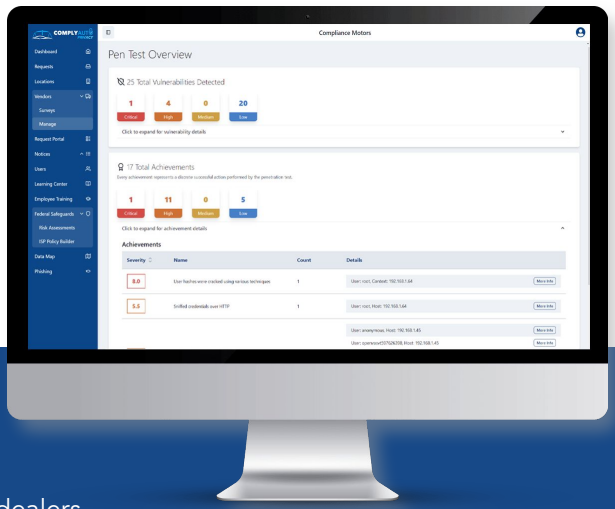
100%
Client Retention. Zero Cancellations.

FEDERAL SAFEGUARDS & CYBERSECURITY COMPLIANCE

Get compliant. Be secure. Save money.

Not only will ComplyAuto help you achieve 100% compliance with the revised FTC Safeguards Rule, but you'll become more secure in the process, which will help reduce your cybersecurity insurance premiums and help prevent data breaches.

- Penetration & Vulnerability Tests
- Vendor Management Platform
- Online Employee Training Courses
- Device & Systems Inventory
- Phishing Simulations
- Automated Policies & Risk Assessments



PRIVACY COMPLIANCE

A 50-state legal solution for local consumer privacy laws.

ComplyAuto is the only privacy rights management system built specifically for dealers. Processing consumer deletion, opt-out, right to know, and data portability requests has never been easier with our fully automated solution. ComplyAuto also installs the required website tools, like compliant cookie banners, privacy policies, and consumer request portals in a matter of days. We also support 100% compliance with state laws like the CTDPA (CT), UCPA (UT), CCPA and CPRA (CA), VDCPA (VA), and CPA (CO).

- Cookie Consent Management
- Global Privacy Controls
- Consumer Request (DSAR) Portal
- Automated Legal Responses
- Data Inventory & Mapping Tools
- Online Privacy Policy Builder

Month-to-Month

No one likes being locked into a contract, so we're purely month-to-month.

First Month Free

We want you compliant, so the first month is on us if you complete our implementation survey within 2 weeks.

No Implementation Fees

No hidden fees, services charges, or installation costs. Oh, and unlimited customer support & training!

Schedule a demo: https://complyauto.com/schedule-demo/ info@complyauto.com (661) 214-8671

COMPLYAUTO PRIVACY

POWERED BY CORO

CTMS Tech with Integrity

ComplyAuto | All-in-One Device & Email Security

The first all-in-one cloud, device, and email security platform built specifically for dealers.
Unparalleled defense. Unrivaled ease of use. Unmatched affordability.

Powerful AI-powered cyber defense for your users, devices, email, cloud apps, and data.

AUTOMATED
USER PROTECTION

Multi-factor authentication powered by Duo Security™

Automatically block inside threats, account hacking, and malicious activities.

Identify abnormal usage patterns and automatically block access to cloud applications

Detect abnormal admin activity and block the relevant accounts

Discover dormant accounts that become active and prevent malicious activities

DEALER-SPECIFIC
DATA GOVERNANCE

Automatically scan all devices and emails for regulatory data such as NPI/PII/PCI information

Identify mass data downloads or deletion & block those activities

Train employees responsible for data sharing or storage violations

Easy inspection of content, simple actions to resolve issues

INTEGRATED
EMAIL SECURITY

Automatically identify and block phishing attacks & impersonation scams

Scan every email for malware & ransomware

Detect employee GLBA, FTC Safeguards, and state data security violations (i.e., PCI, NPI, PII sharing)

Identify abnormal login patterns and block hacking attempts automatically

Integrated with Google Workspace & Microsoft Office 365

SIMPLIFIED
CLOUD SECURITY

Block suspicious login activity

Detect account compromises

Identify & automatically quarantine malicious files stored in the cloud

Integrated with Google Workspace & Microsoft Office 365.

Locate and block phishing attempts (i.e., share requests & access requests)

24/7 REAL-TIME
DEVICE MONITORING

Automated device-level encryption for Windows & macOS

Continuous threat monitoring (EDR + MDR/MTR) powered by Coro & Bitdefender™

Next-gen anti-virus

Email security with automatic phishing detection

Monitoring & logging of employee data/NPI violations

Detect devices with disabled firewalls, missing UAC, unencrypted drives, and other security hygiene issues.

24/7/365 Full-Coverage Security Monitoring

Powered by CoroSOC™ & CTMS

Reduce the noise. We automatically mitigate threats like malware & ransomware unless contacting you is absolutely necessary.

Upon detection of a potential threat, our team of security experts investigates the case, looks into historical data and current threat context, and decides upon appropriate follow-up actions. Issues and events are classified by severity. You are informed only when a severe threat that requires your attention is found. You receive incident updates and reports by email and/or phone.

Installation Included | **Zero Implementation Fees** | **Unlimited One-on-One Customer Support**

Complyauto.com | info@complyauto.com | (661) 214-8671