Revised FTC Safeguards Rule & Privacy Compliance
ADVANCED SESSION

Sherryl Nens, VP of Sales, ComplyAuto

Our Story

BY DEALERS. FOR DEALERS.

ComplyAuto was born out of the frustrations of having to spend substantial time and resources in complying with complex privacy and cybersecurity regulations.

Using the experience in managing their own dealership operations, the founders built a purpose-built solution that saved them hundreds of hours and hundreds of thousands of dollars annually. This allowed them to focus their limited resources on what they do best – selling and servicing vehicles.

We now bring that solution to you.

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 Group

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, ComplyAuto Privacy
Dealer Relations Manager, Ford Motor Co. *(former)*

+7,500
Active Dealers

+35
State Dealer Association Endorsements

99.9%
Dealer Retention

Three Pillars of InfoSec Compliance

REVISED FTC SAFEGUARDS RULE

145-page set of regulations effective ~~December 9, 2022~~ June 9, 2023.

In 2022, the FTC Safeguards Rule was revised for the first time in 20 years to include a comprehensive set of new privacy & cybersecurity regulations estimated by the NADA to cost dealers ~$277,000 annually.

- Policy builders & risk assessments with automatic updates
- Vendor contract & risk management automation
- Penetration & vulnerability tests
- 24/7/365 monitoring (EDR + MTR)
- Device encryption
- Multi-factor authentication
- Systems monitoring & logging for employee data misuse
- Employee training & phishing simulations
- Device & systems inventory tools

CONSUMER PRIVACY RIGHTS

Enforced by state Attorneys General & the FTC (and plaintiff lawyers).

Third-party tracking cookies, online privacy disclosures, and data sharing practices have all become common targets for litigation by state agencies, the FTC, and private plaintiff attorneys.

- Cookie consent management
- Online privacy policy builder with real-time updates
- Online consumer privacy request (DSAR) portal
- Compliance with laws in California, Colorado, Connecticut, Virginia, and Utah

STATE DATA BREACH LAWS

All 50 states now have data breach laws & some have specific cybersecurity laws.

Every state now has its own data breach reporting obligations and some have specific cybersecurity and privacy regulations that grant safe harbor for meeting certain cybersecurity standards.

- 50-state legal incident response plan builder
- Advanced risk assessment tools to meet CIS standards
- Online employee training modules that meet applicable state standards

New FTC Safeguards Rule Requirements

NADA LEGAL SUMMARY

FTC Enforcement:
$50,120 per violation

Est. Cost Per Dealer:
$293,975 upfront
$276,925 per year

*Independent study performed by the NADA

NADA NATIONAL AUTOMOBILE DEALERS ASSOCIATION

Qualified Employee	Written Risk Assessment	Access Controls	Data and Systems Inventory
Data Encryption	Intrusion Detection/ Vulnerability Testing	Multi-Factor Authentication	Systems Monitoring and Logging
Secure Data Disposal Procedures	Change Management Procedures	Unauthorized Activity Monitoring	
Overseeing/Monitoring Service Providers	Written Incident Response Plan	Annual Reporting to Board	

Note: While the FTC did extend the deadline by 6 months, the extension did not apply to these provisions:

- Implementing a written Information Security Program (ISP);
- Getting your vendors who collect customer information ("Service Providers") to sign a contract promising to implement reasonable safeguards; and
- Implement a system capable of detecting attacks and intrusions on your network

COMPLYAUTO PRIVACY

Part 1: Federal Safeguards Essentials

RULE #1 - Four Written Policies

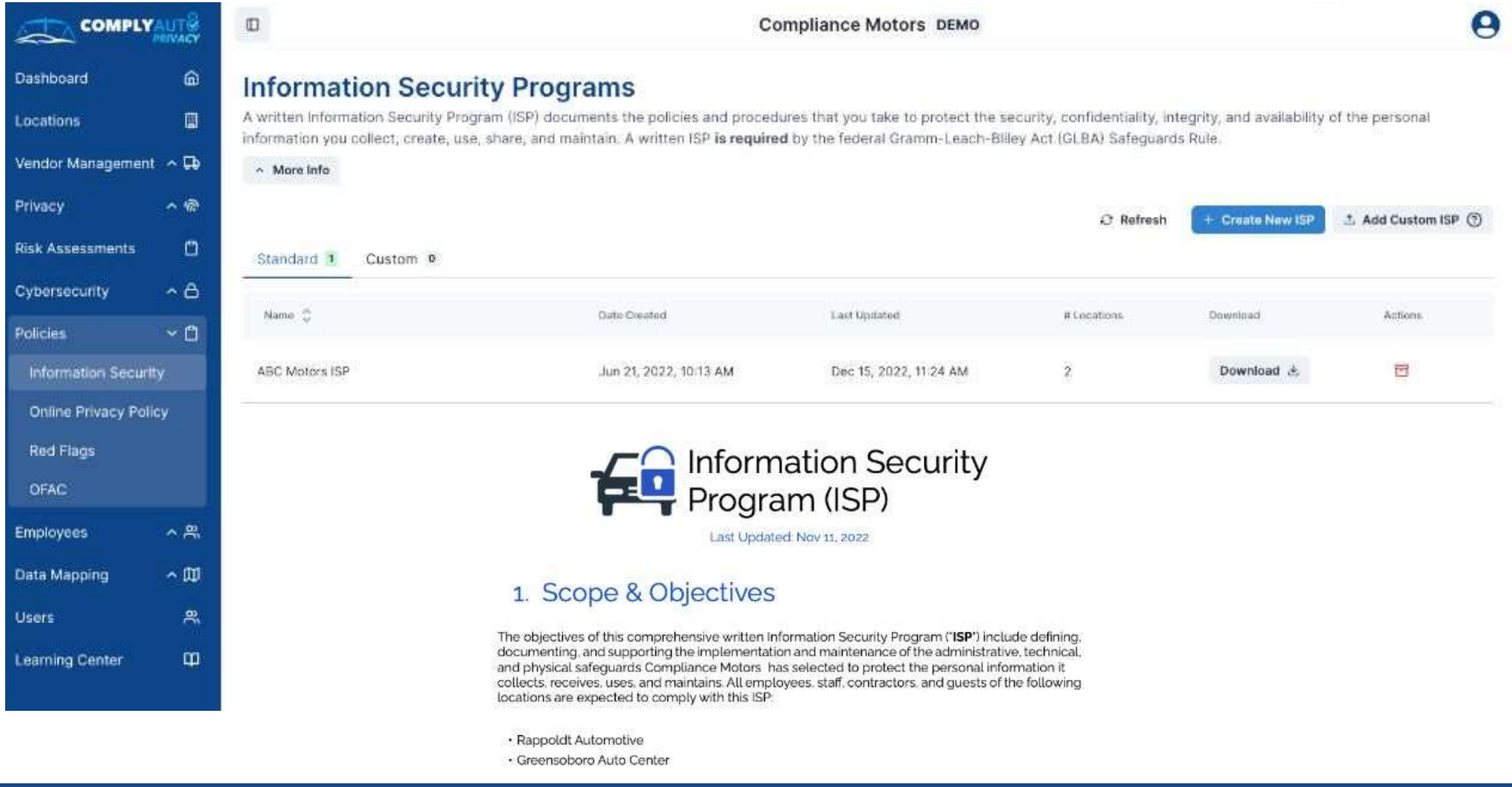
Dealers must have a written Information Security Program, Incident Response Plan, Data Retention Plan, and IT Change Management Procedures that are made available to employees. 16 CFR §314.4(c)(6)-(7), §314.4(c)(6)(h)(1).

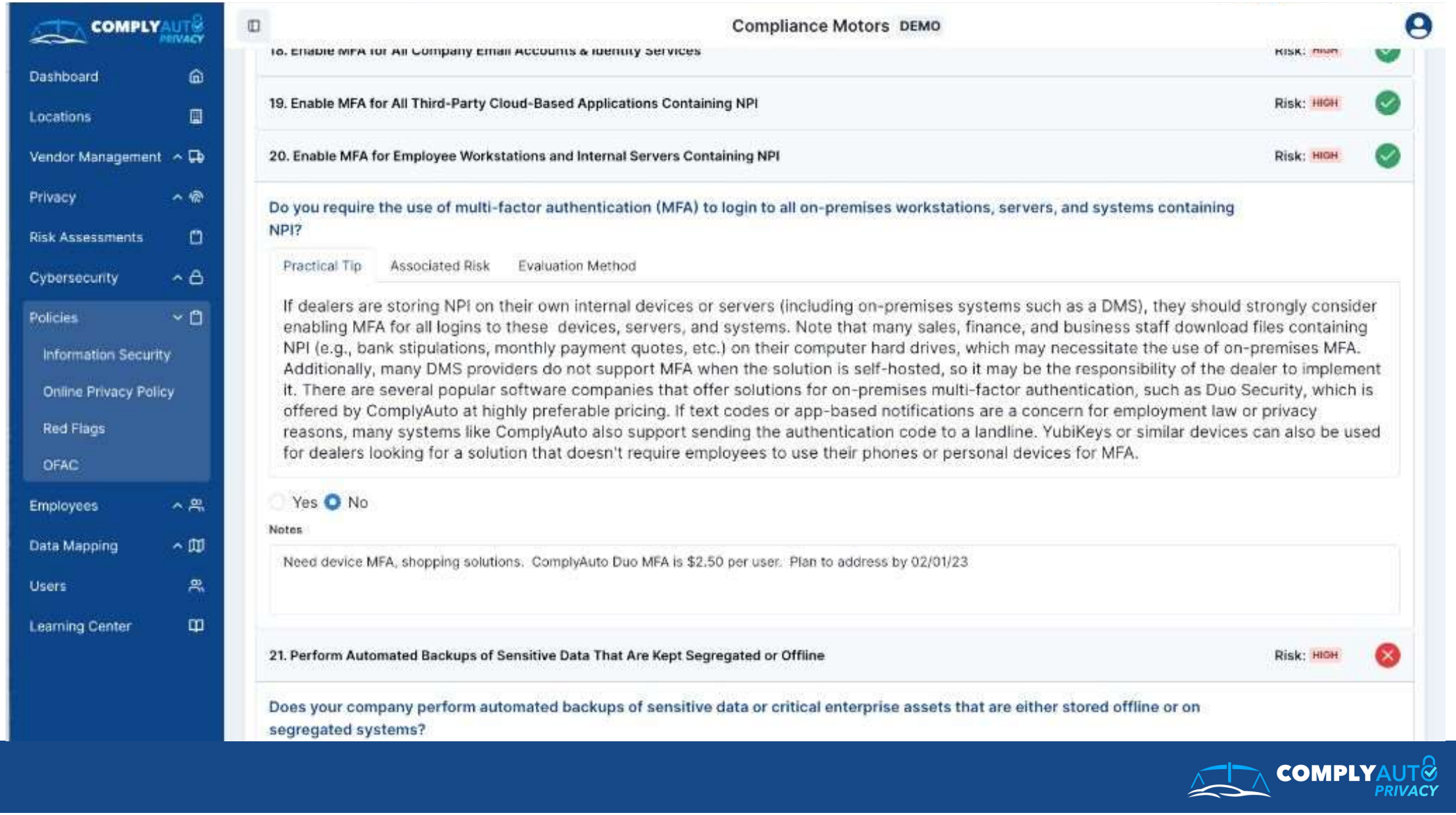
PRACTICAL TIPS
Your old policies in the binder from 2002 won't suffice.
Incorporate requirements from state laws.
Don't use cookie cutter templates

RULE #2 - Annual Written Risk Assessment

At least annually, dealers must complete a formal written risk assessments where they (1) identify any information security risks, (2) document mitigation efforts, and (3) update the four policies based on the results. 16 CFR §314.4(b).

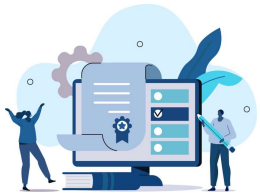
PRACTICAL TIPS
Don't just look at the regulations themselves -- incorporate risks based on FTC guidance, law suits, and consent orders.
Incorporate items that come up on your cybersecurity insurance renewal application.


COMPLYAUTO PRIVACY
Compliance Motors DEMO
Dashboard
Locations
Vendor Management
Privacy
Risk Assessments
Cybersecurity
Policies
Information Security
Online Privacy Policy
Red Flags
OFAC
Employees
Data Mapping
Users
Learning Center
Information Security Programs
A written Information Security Program (ISP) documents the policies and procedures that you take to protect the security, confidentiality, integrity, and availability of the personal information you collect, create, use, share, and maintain. A written ISP is required by the federal Gramm-Leach-Bliley Act (GLBA) Safeguards Rule.
More Info
Refresh
Create New ISP
Add Custom ISP
Standard 1
Custom 0
Name
Date Created
Last Updated
Locations
Download
Actions
ABC Motors ISP
Jun 21, 2022, 10:13 AM
Dec 15, 2022, 11:24 AM
2
Download
Information Security Program (ISP)
Last Updated: Nov 11, 2022
1. Scope & Objectives
The objectives of this comprehensive written Information Security Program ("ISP") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards Compliance Motors has selected to protect the personal information it collects, receives, uses, and maintains. All employees, staff, contractors, and guests of the following locations are expected to comply with this ISP:
• Rappoldt Automotive
• Greensoboro Auto Center


COMPLYAUTO PRIVACY
Compliance Motors DEMO
Dashboard
Locations
Vendor Management
Privacy
Risk Assessments
Cybersecurity
Policies
Information Security
Online Privacy Policy
Red Flags
OFAC
Employees
Data Mapping
Users
Learning Center
18. Enable MFA for All Company Email Accounts & Identity Services
Risk: HIGH
19. Enable MFA for All Third-Party Cloud-Based Applications Containing NPI
Risk: HIGH
20. Enable MFA for Employee Workstations and Internal Servers Containing NPI
Risk: HIGH
Do you require the use of multi-factor authentication (MFA) to login to all on-premises workstations, servers, and systems containing NPI?
Practical Tip
Associated Risk
Evaluation Method
If dealers are storing NPI on their own internal devices or servers (including on-premises systems such as a DMS), they should strongly consider enabling MFA for all logins to these devices, servers, and systems. Note that many sales, finance, and business staff download files containing NPI (e.g., bank stipulations, monthly payment quotes, etc.) on their computer hard drives, which may necessitate the use of on-premises MFA. Additionally, many DMS providers do not support MFA when the solution is self-hosted, so it may be the responsibility of the dealer to implement it. There are several popular software companies that offer solutions for on-premises multi-factor authentication, such as Duo Security, which is offered by ComplyAuto at highly preferable pricing. If text codes or app-based notifications are a concern for employment law or privacy reasons, many systems like ComplyAuto also support sending the authentication code to a landline. YubiKeys or similar devices can also be used for dealers looking for a solution that doesn't require employees to use their phones or personal devices for MFA.
Yes
No
Notes
Need device MFA, shopping solutions. ComplyAuto Duo MFA is $2.50 per user. Plan to address by 02/01/23
21. Perform Automated Backups of Sensitive Data That Are Kept Segregated or Offline
Risk: HIGH
Does your company perform automated backups of sensitive data or critical enterprise assets that are either stored offline or on segregated systems?

RULE #3 - Annual Employee Security Awareness Training

All employees must be trained on security awareness as well as your specific information security program policies, procedures, and safeguards. 16 CFR §314.4(e)

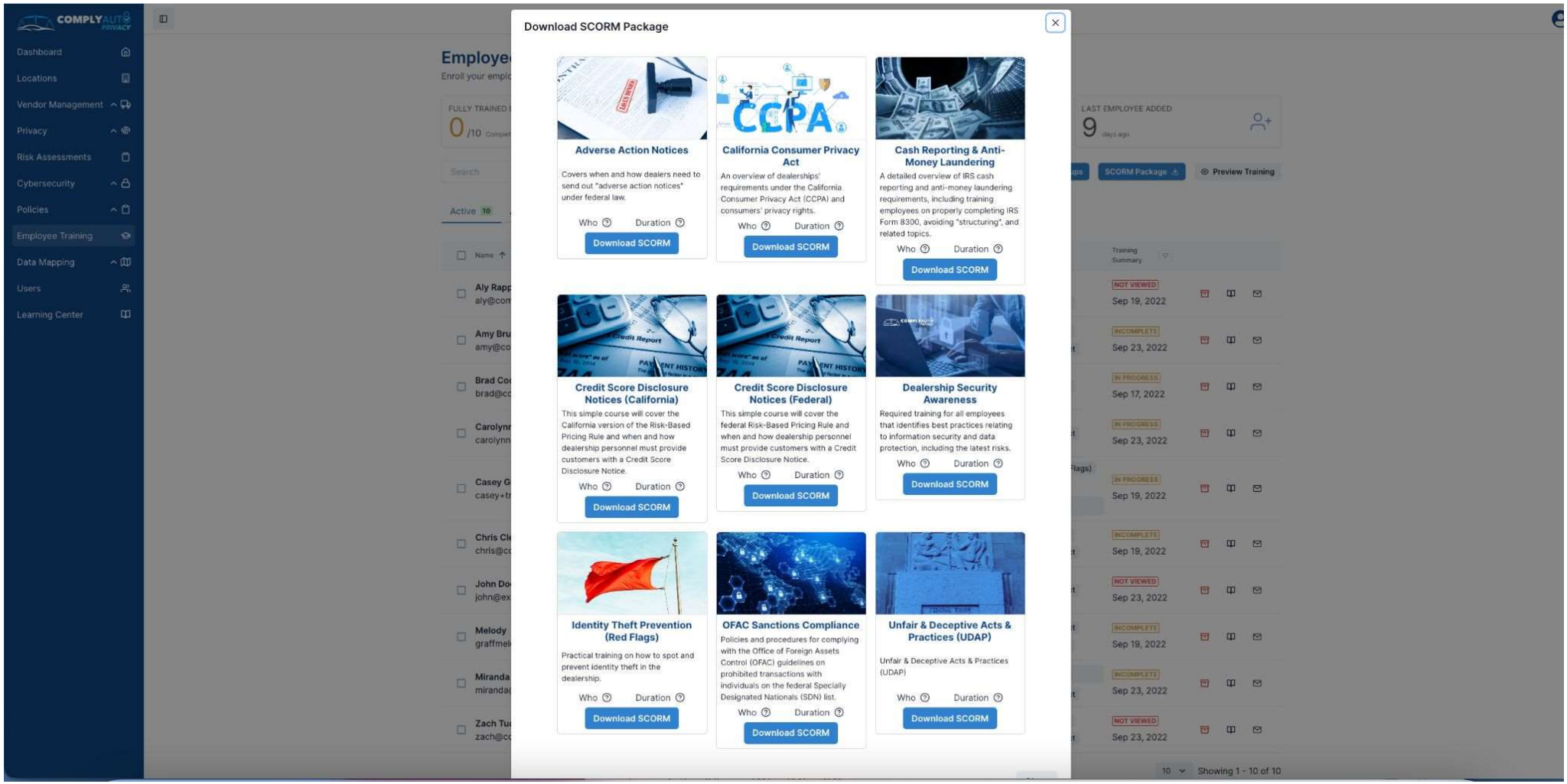


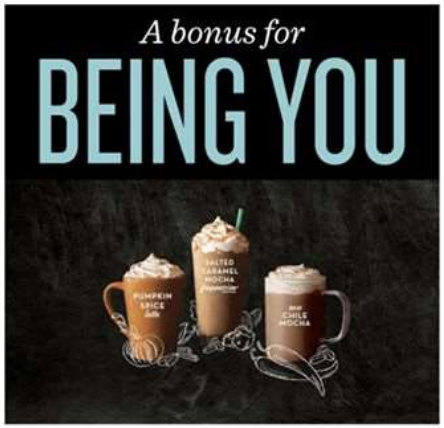
PRACTICAL TIPS
Train everyone! The law doesn't provide for any exceptions and information security is everyone's responsibility.
Best practice is to incorporate the topics required under nationally accepted cybersecurity frameworks (secure disposal, password composition, MFA, clean-desk policies, etc.)
Use dealer-specific training.

RULE #4 - Phishing & Social Engineering Simulations

The FTC has clarified testing your employees' susceptibility to social engineering and phishing scams is an important part of the new penetration testing requirements. 16 CFR §314.4(d)(2)(i).

PRACTICAL TIPS
Phish everyone without exceptions! It's highly effective and it only takes one employee to cause a data breach.
Within 90 days, susceptibility to phishing typically decreases by >90%.
Common phish: Email client PW reset (Google, Office 365), Dealer Principal gift cards, **free pumpkin spice latte?**


Download SCORM Package
Adverse Action Notices
Covers when and how dealers need to send out "adverse action notices" under federal law.
Who
Duration
Download SCORM
California Consumer Privacy Act
An overview of dealerships' requirements under the California Consumer Privacy Act (CCPA) and consumers' privacy rights.
Who
Duration
Download SCORM
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
Download SCORM
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
Download SCORM
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
Download SCORM
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
Download SCORM
Identity Theft Prevention (Red Flags)
Practical training on how to spot and prevent identity theft in the dealership.
Who
Duration
Download SCORM
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
Download SCORM
Unfair & Deceptive Acts & Practices (UDAP)
Unfair & Deceptive Acts & Practices (UDAP)
Who
Duration
Download SCORM



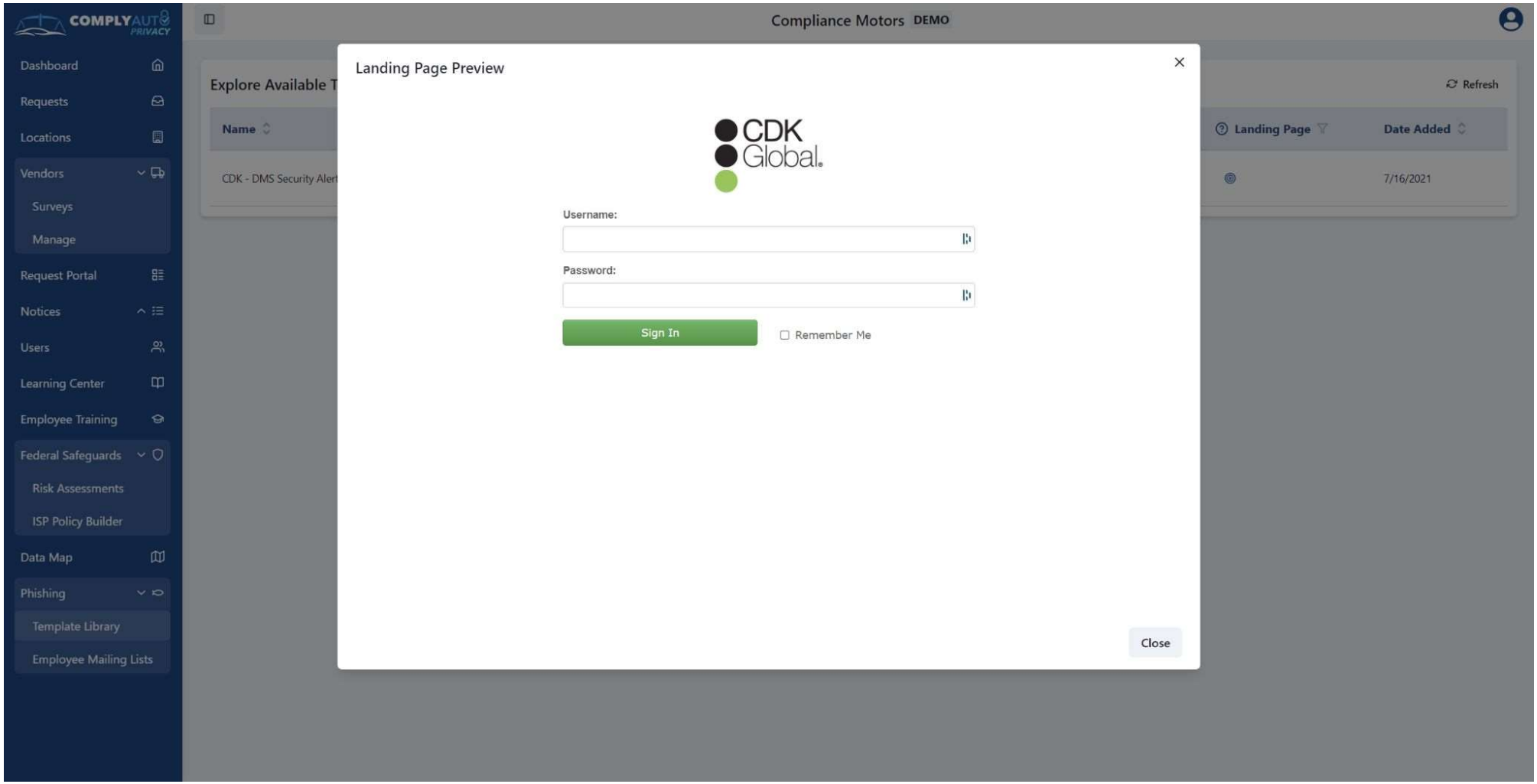
First Fall Favorite on Us!

Fall flavors are in full swing with the return of Pumpkin Spice Latte and Salted Caramel Mocha, and the arrival of our new Chile Mocha. Each can be enjoyed hot or blended to satisfy your seasonal craving. And your first one's free!

Choose your drink below to get a voucher and get it FREE in the store!

Pumpkin Spice Latte | Salted Caramel Mocha | Chile Mocha

Reply | Forward


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

RULE #5 - GLBA Service Provider Contracts

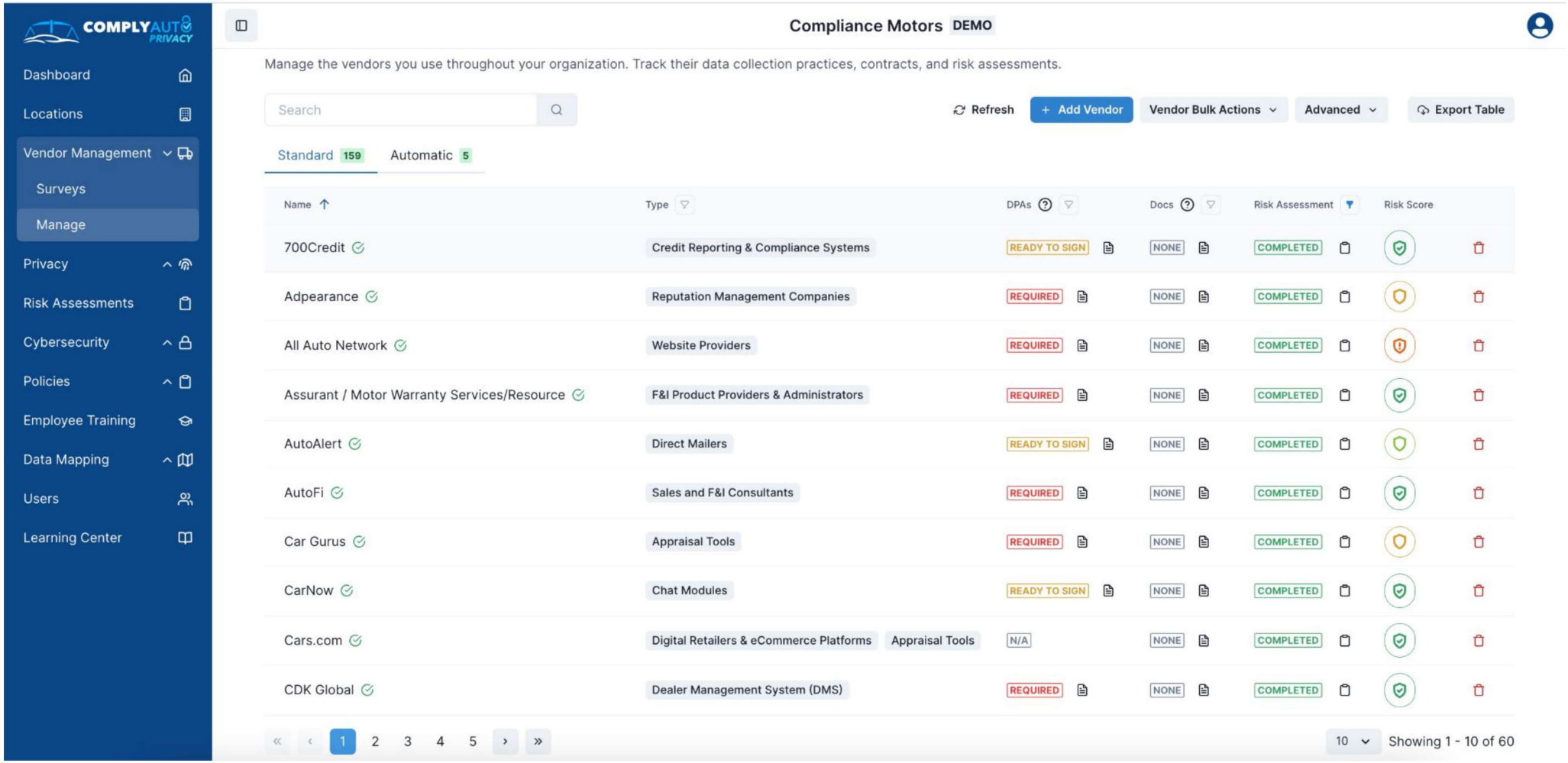
Dealers are responsible for having service providers who access NPI (customer info related to a finance or lease transaction) sign a specific contract where they promise to implement reasonable safeguards. 16 CFR §314.4(f)(2)

PRACTICAL TIPS
OEMs don't think they're covered as "service providers". NADA disagrees. Potential gray area, but not much dealers can do about it.
Don't worry about your banks/lenders - they're "financial institutions", not "service providers".
Only applies to vendors collecting customer NPI -- HR vendors not covered under GLBA - may be required at state level.

RULE #6 - Annual Service Provider Risk Assessments

Dealers are required to periodically assess or "check in" with their service providers to ensure the continued adequacy of their safeguards, which is accomplished through a security questionnaire. 16 CFR §314.4(f)(3).

PRACTICAL TIPS
No, you don't have to physically inspect or perform a penetration test of your vendors.
FTC's position is that you should not continue doing business with vendors who have failed to complete the contract & risk assessment.
Use a system like ComplyAuto to make this easy. Hundreds of pre-completed contract and risk assessments for popular vendors and built-in eSign functionality and automatic tracking


COMPLYAUTO PRIVACY
Dashboard
Locations
Vendor Management
Surveys
Manage
Privacy
Risk Assessments
Cybersecurity
Policies
Employee Training
Data Mapping
Users
Learning Center
Compliance Motors DEMO
Manage the vendors you use throughout your organization. Track their data collection practices, contracts, and risk assessments.
Search
Refresh
+ Add Vendor
Vendor Bulk Actions
Advanced
Export Table
Standard 159
Automatic 5
Name
Type
DPAs
Docs
Risk Assessment
Risk Score
700Credit
Credit Reporting & Compliance Systems
READY TO SIGN
NONE
COMPLETED
Adpearance
Reputation Management Companies
REQUIRED
NONE
COMPLETED
All Auto Network
Website Providers
REQUIRED
NONE
COMPLETED
Assurant / Motor Warranty Services/Resource
F&I Product Providers & Administrators
REQUIRED
NONE
COMPLETED
AutoAlert
Direct Mailers
READY TO SIGN
NONE
COMPLETED
AutoFi
Sales and F&I Consultants
REQUIRED
NONE
COMPLETED
Car Gurus
Appraisal Tools
REQUIRED
NONE
COMPLETED
CarNow
Chat Modules
READY TO SIGN
NONE
COMPLETED
Cars.com
Digital Retailers & eCommerce Platforms
Appraisal Tools
N/A
NONE
COMPLETED
CDK Global
Dealer Management System (DMS)
REQUIRED
NONE
COMPLETED
1 2 3 4 5
10
Showing 1 - 10 of 60

RULE #7 - Annual Penetration & Biannual Vulnerability Scans

Dealers must perform annual internal penetration testing (simulated hacking) of their networks and biannual vulnerability assessments for known exploits. 16 CFR §314.4(d)(2)

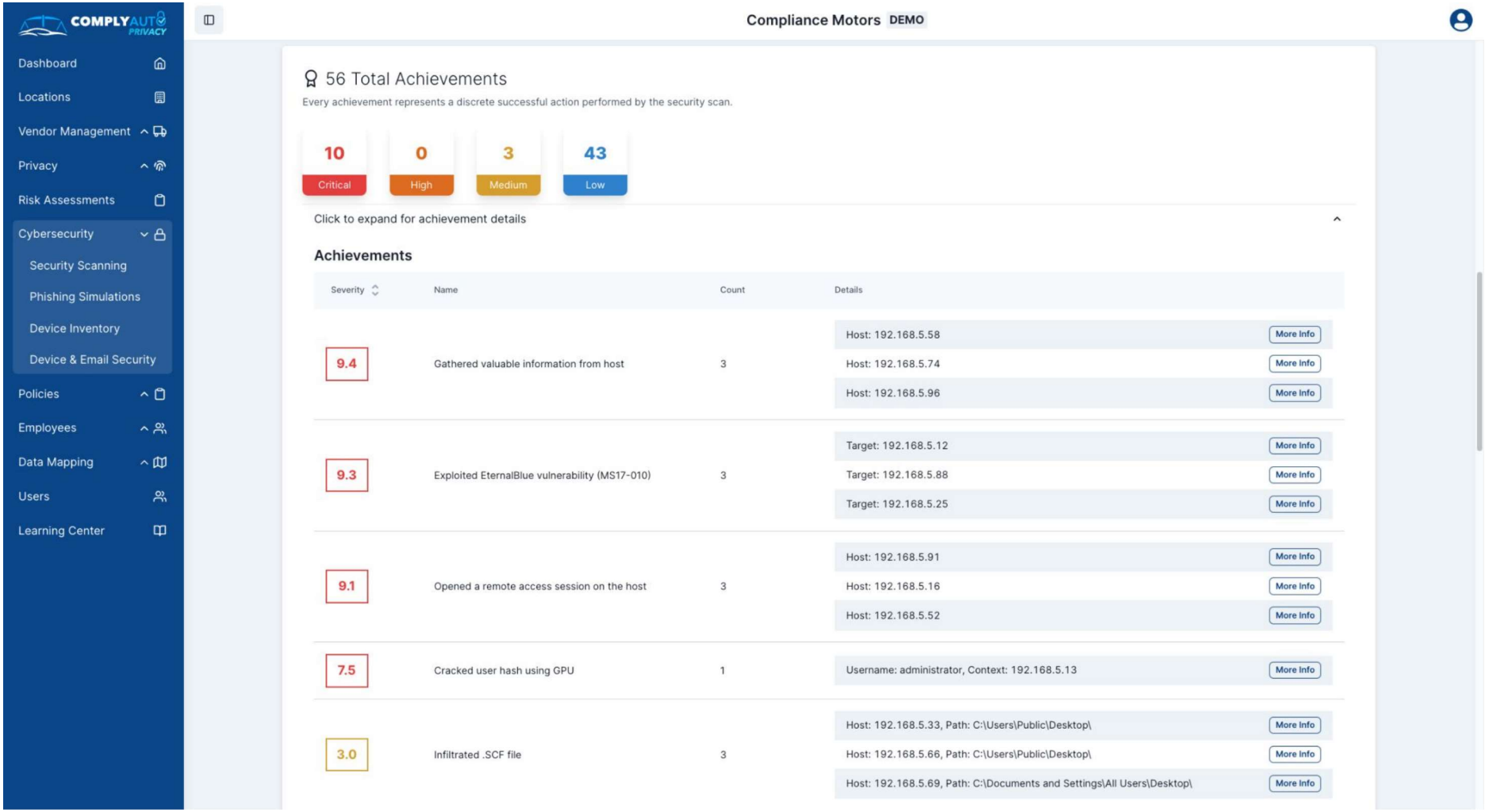
PRACTICAL TIPS
No, the law doesn't require human testers. It can be automated.
ComplyAuto services include a full internal penetration test (performed biannually) that satisfies regulatory requirements and does everything from password cracking, remote code execution, credentials sniffing, ransomware emulations, malware injections, active directory attacks, and much more.
The penetration test performed by your PCI Compliance company or insurance company is usually just an external test (testing your firewall), which isn't as valuable and won't satisfy the Safeguards Rule.

WHAT ABOUT THE "CONTINUOUS MONITORING" EXCEPTION?

Myth-Buster

Q: I don't need to do pen tests and vulnerability scans if I have EDR because that constitutes "continuous monitoring" under the regulations.

A: **False**. "Continuous monitoring" is a term defined in the regulations to include monitoring for (1) security threats, (2) misconfigured system settings, and (3) other vulnerabilities. **EDR only does the first item**. Tools that do true continuous monitoring for all three items are usually cost-prohibitive for most dealers.


COMPLYAUTO PRIVACY
Compliance Motors DEMO
Dashboard
Locations
Vendor Management
Privacy
Risk Assessments
Cybersecurity
Security Scanning
Phishing Simulations
Device Inventory
Device & Email Security
Policies
Employees
Data Mapping
Users
Learning Center
56 Total Achievements
Every achievement represents a discrete successful action performed by the security scan.
10 Critical
0 High
3 Medium
43 Low
Click to expand for achievement details
Achievements
Severity
Name
Count
Details
9.4
Gathered valuable information from host
3
Host: 192.168.5.58 More Info
Host: 192.168.5.74 More Info
Host: 192.168.5.96 More Info
9.3
Exploited EternalBlue vulnerability (MS17-010)
3
Target: 192.168.5.12 More Info
Target: 192.168.5.88 More Info
Target: 192.168.5.25 More Info
9.1
Opened a remote access session on the host
3
Host: 192.168.5.91 More Info
Host: 192.168.5.16 More Info
Host: 192.168.5.52 More Info
7.5
Cracked user hash using GPU
1
Username: administrator, Context: 192.168.5.13 More Info
3.0
Infiltrated .SCF file
3
Host: 192.168.5.33, Path: C:\Users\Public\Desktop\ More Info
Host: 192.168.5.66, Path: C:\Users\Public\Desktop\ More Info
Host: 192.168.5.69, Path: C:\Documents and Settings\All Users\Desktop\ More Info

RULE #8 - Device, Data & Systems Inventory

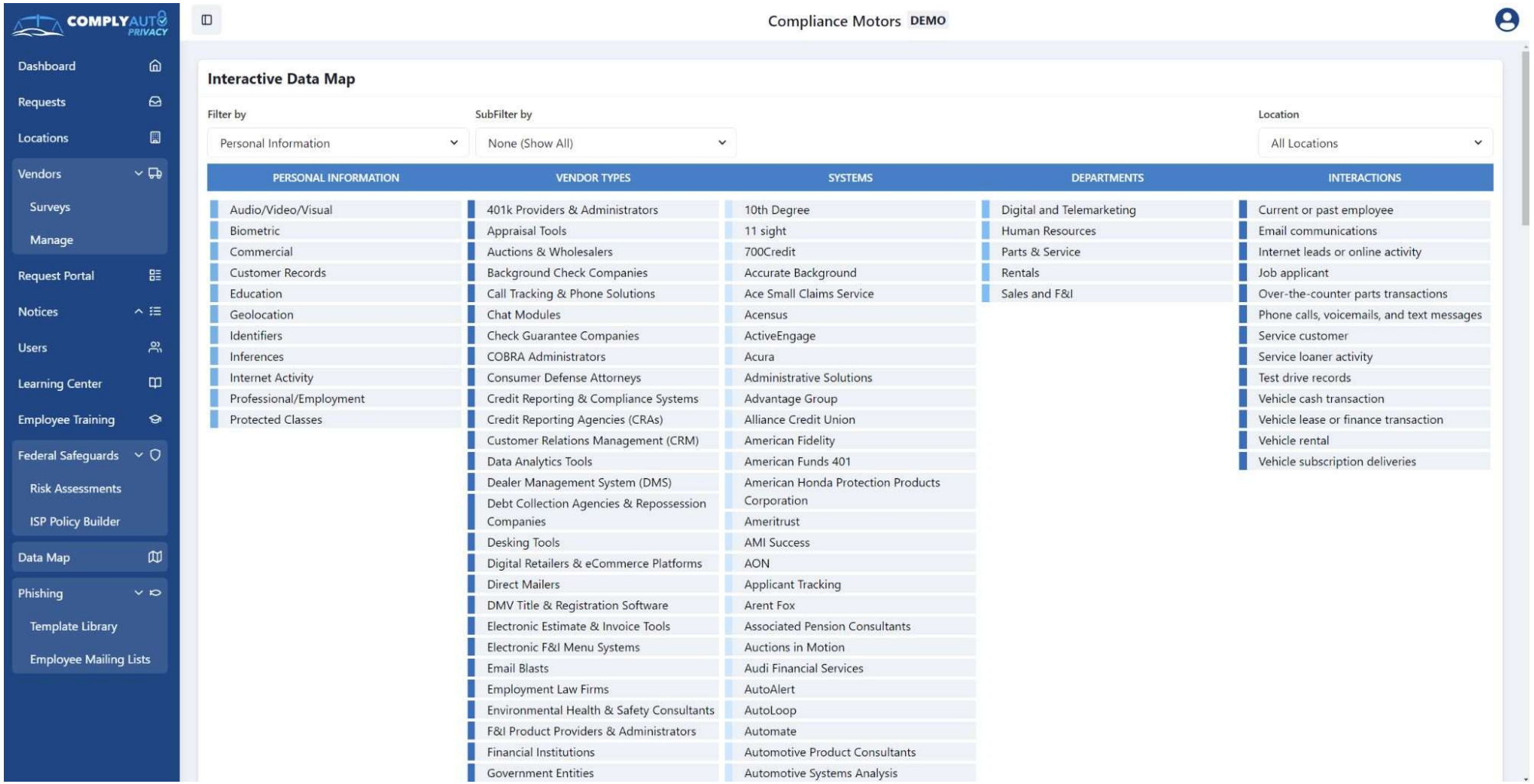
Dealers are required to perform data and systems inventory where they must identity the data in their possession and track the vendors and systems on which the data is collected, stored, or transmitted. 16 CFR §314.4(c)(2).

COMPLYAUTO SOLUTION
Must track and inventory all the devices connected to your network or issued to employees.
Must track and inventory every vendor and the categories of personal information being collected from them.
According to the FTC, you can't protect data if you don't track where it is or know the scope of what's being collected in the first place.

RULE #9 - Annual Report to Board of Directors

Dealer must submit a written report to their Board of Directors or other senior executives summarizing all their efforts to comply with the Safeguards Rule. 16 CFR §314.4(i).

COMPLYAUTO SOLUTION
If no board (LLC or not a corporation) then dealer principal and other officers.
Idea from the FTC is to create accountability and prevent executive management from feigning ignorance.
Good resource tool to use as proof of cybersecurity compliance for your cybersecurity insurance renewal.


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
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

COMPLYAUTO PRIVACY

Compliance Motors
Information Security Program Status

2023 ANNUAL REPORT

Prepared by: Casey Graff on January 4, 2023

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

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	COMPLETE	16 CFR § 314.4(c)(3)
Multi-factor Authentication	COMPLETE	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	COMPLETE	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)

COMPLYAUTO PRIVACY

Part 2: Technical Rule Requirements for Email & Device Protection

RULE #10 - Intrusion & Attack Detection

The Safeguards Rule, as well as most OEMs and cybersecurity insurance carriers, require a system for detecting intrusions and attacks on your network. 16 CFR §314.4(d)(1)

PRACTICAL TIPS
The FTC doesn't refer to any particular technology, but for practical reasons, this means endpoint detection and response (EDR).
You may already have this at your dealership through your IT company or DMS (Sophos, Nuspire, SentinelOne, Huntress, etc.)

RULE #11 - User & Employee Monitoring & Logging

Dealers are required to have a system capable of detecting unauthorized access, sharing, use of, and tampering with customer information 16 CFR §314.4(c)(8).

PRACTICAL TIPS
The FTC doesn't refer to any particular technology, but we usually refer to this as Data Loss/Leak Prevention (DLP) in the cybersecurity industry.
Most dealers are not currently using a DLP tool that detects for data governance violations (NPI, PCI, PII sharing, emailing downloading, deleting).

Device & Email Security

It is essential for both GLBA compliance and cybersecurity liability insurance that you take appropriate security measure to protect your organization's data and operations. Endpoint security, including endpoint detection and response (EDR) and next-gen anti-virus (NGAV), device encryption, email monitoring (phishing or ransomware), and data governance (NPI scanning) are all critical aspects of ensuring your data and your customers' data are protected.

Access Management Dashboard

Users

View Users

37

Protected Users

- Access Restrictions Violations
- Mass Data Deletion
- Mass Data Download
- Suspicious exposure of source code
- Suspicious exposure of certificate
- Suspicious exposure of critical data
- Suspected Bot Attacks

Emails

92,176

Emails Processed

(last 90 days)

21

Malicious

Blocked & Discarded

- Suspicious Email Content
- Malware in Email Attachments

Top Sources of Suspicious Emails

Devices

View Devices

21

Devices

- Firewall Disabled
- Malware on Endpoint
- UAC Notification Missing
- Device Password Missing
- Unencrypted Endpoint Drive
- Non-genuine Windows copy

Data Governance

96,697

Data objects processed

(last 90 days)

Email

- Payment Card Info (PCI)
- Personally Identifiable Info (PII)
- Non-public Information (NPI)

RULE #12 - Device Encryption

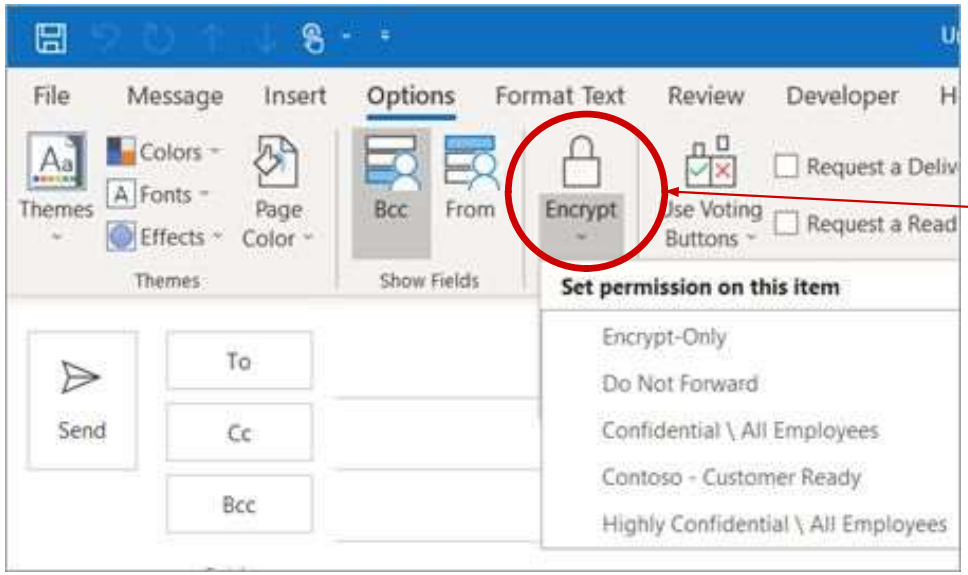
If any of the dealership's devices, such as desktops, laptops, tablets, or mobile devices contain customer information, the hard drives of those devices must be encrypted. 16 CFR § 314.4(c)(3).

PRACTICAL TIPS
Enable Bitlocker (Microsoft's free built-in encryption tool) on all computers (at a minimum those used to access finance/lease info), but make sure to manage the keys (looooong passwords) securely.
"My computers don't have any customer information on them". Are you sure about that? Think email downloads, DMS reports/exports, file scanning/copiers.
Email encryption: enable TLS for all emails. No, you don't need to use the Outlook/Office encryption button on every email. TIME TO UPGRADE TO COMMERCIAL EMAIL ACCOUNTS!

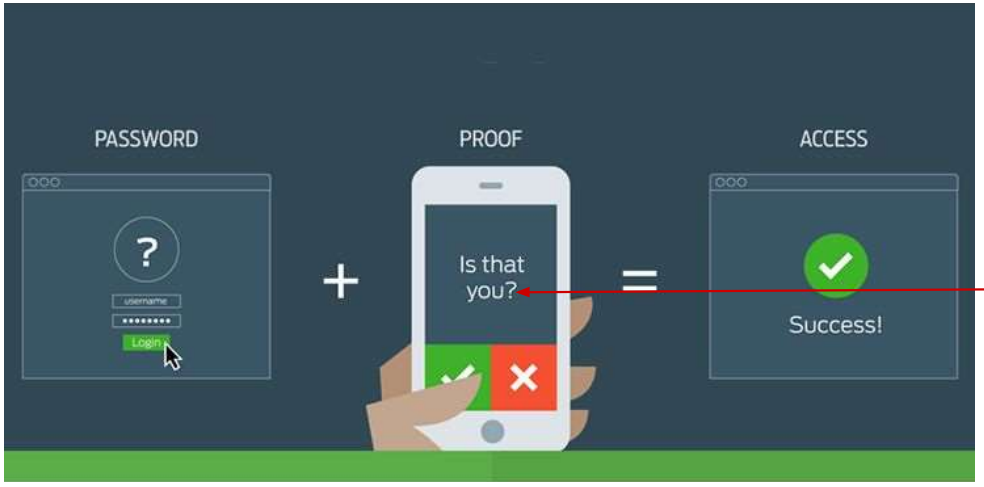
RULE #13 - Multi-factor Authentication

Dealers must implement MFA on any system used to access customer information, including device-level MFA such as upon a Windows or MacOS login. 16 CFR § 314.4(c)(5).

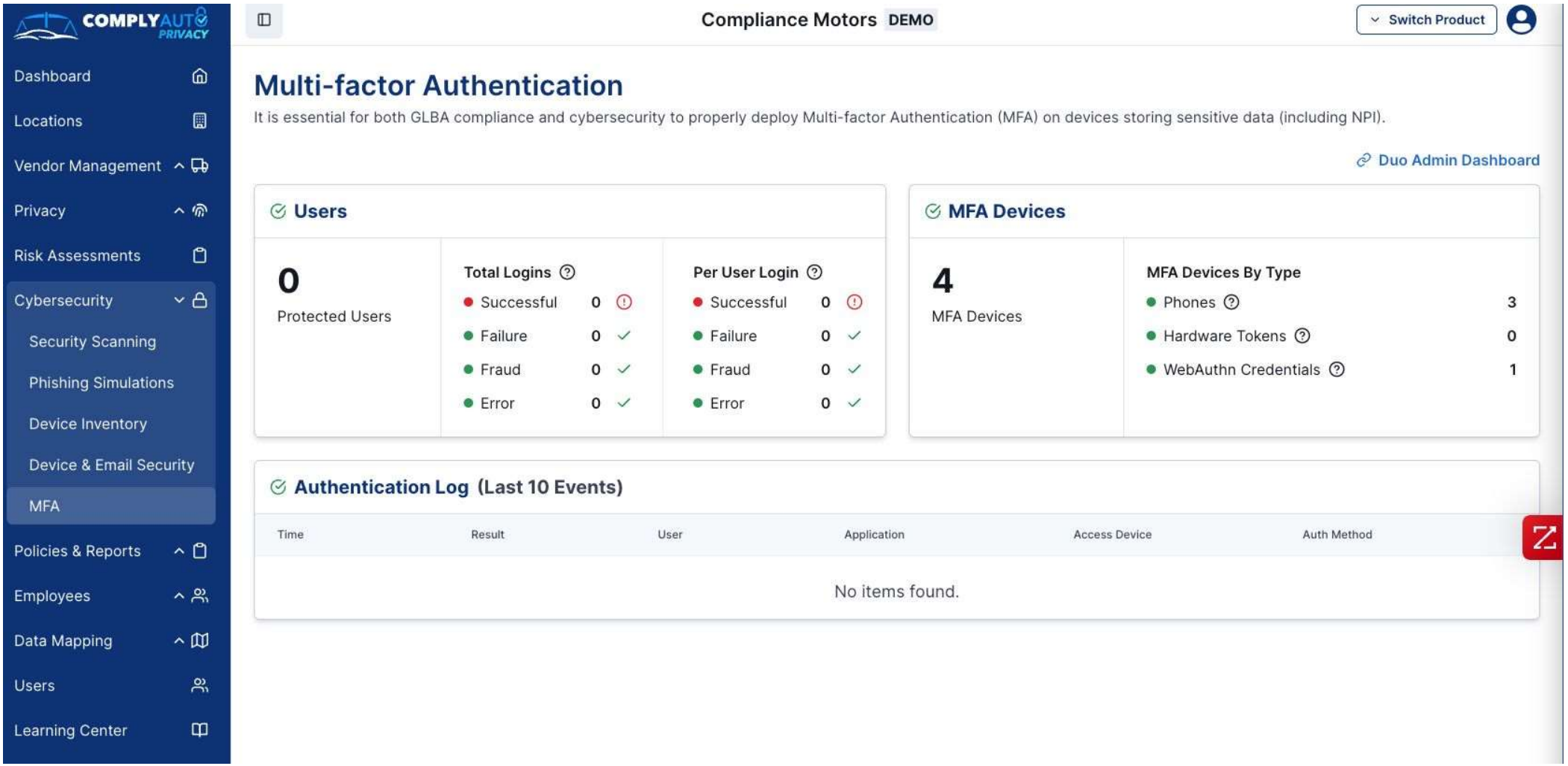
COMPLYAUTO SOLUTION
Email MFA, Application MFA, and device (Windows logon) MFA are necessary.
Windows Hello isn't really MFA (pin, facial recognition, finger print)
Need a tool like Duo, Okta, Google Credential Provider for Windows (GCPW) for device-level MFA.



Not necessary for most emails, but useful when sending sensitive info to outside third parties.



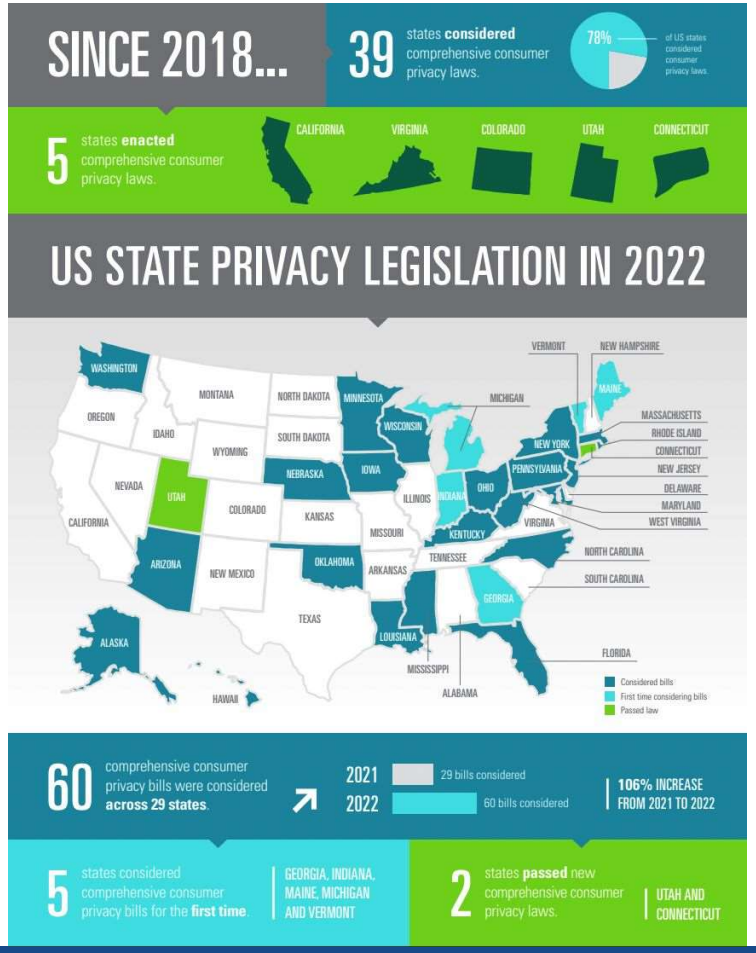
Duo MFA One-Tap Authentication with Duo Push.
Duo can also accommodate more traditional second-factor authentication controls like SMS text code.


COMPLYAUTO PRIVACY
Compliance Motors DEMO
Switch Product
Dashboard
Locations
Vendor Management
Privacy
Risk Assessments
Cybersecurity
Security Scanning
Phishing Simulations
Device Inventory
Device & Email Security
MFA
Policies & Reports
Employees
Data Mapping
Users
Learning Center
Multi-factor Authentication
It is essential for both GLBA compliance and cybersecurity to properly deploy Multi-factor Authentication (MFA) on devices storing sensitive data (including NPI).
Duo Admin Dashboard
Users
0
Protected Users
Total Logins
Successful 0
Failure 0
Fraud 0
Error 0
Per User Login
Successful 0
Failure 0
Fraud 0
Error 0
MFA Devices
4
MFA Devices
MFA Devices By Type
Phones 3
Hardware Tokens 0
WebAuthn Credentials 1
Authentication Log (Last 10 Events)
Time
Result
User
Application
Access Device
Auth Method
No items found.

COMPLYAUTO PRIVACY

Part 3: State Specific Consumer Privacy Laws

Consumer Privacy Rights Compliance



Should you be concerned about cookie consent and privacy rights issues if your state doesn't have a comprehensive privacy law?

YES, the FTC wants a piece of the state privacy law action!

- The FTC is enforcing issues related to cookie tracking under its broad Section 5 **Unfair & Deceptive Acts & Practices** (UDAP) authority.
  - Two 7 figure lawsuits from the FTC this year
  - You're a target if you're not getting explicit consent to load tracking cookies for retargeting (e.g., Facebook Pixel, Google Ads)
- Class actions lawsuits have been filed in both regulated and unregulated states for deploying tracking cookies without consent and/or proper disclosures the **Federal Wiretap Act**, (2) general **UDAP** claims, (3) the federal **Consumer Fraud & Abuse Act**, and (4) the federal **Stored Communications Act**.
- So far in 2023, **8 states have proposed Consumer Privacy Rights Legislation.**
- Five States enacted comprehensive privacy laws - CA, VA, CO, UT and CT with **fines ranging from $5,000-$20,000**

source: US State Privacy Legislation IAAP's Resource Center

ComplyAuto Exclusive - rounding out your compliance & risk mitigation strategy with a comprehensive set of consumer privacy tools installed for you in the background.

Issues related to third-party tracking cookies, online privacy disclosures, and data collection practices are receiving increased scrutiny from the FTC, plaintiff lawyers, and state Attorneys Generals or class action lawsuits. Additionally, several states (CA, CO, CT, VA, UT) now have specific requirements targeting these issues.

Cookie Consent Management

- Website cookie banner templates for all 50 states.
- Completely customizable based on dealer's risk appetite with automatic blocking and Global Privacy Control (GPC) detection.
- Responds to GPC and do-not-track signals.

The FTC enforces issues related to cookie tracking under its broad Section 5 **Unfair & Deceptive Acts & Practices** (UDAP) authority.

A plethora of class actions lawsuits have been filed in both regulated and unregulated states for deploying tracking cookies without consent and/or proper disclosures. Sources for authority have been (1) the **Federal Wiretap Act**, (2) general **UDAP** claims, (3) the federal **Consumer Fraud & Abuse Act**, and (4) the federal **Stored Communications Act**.

Online Privacy Policy Builder

- Ensure your online privacy policy complies with state and federal laws.
- Automatic real-time updates that syncs with the vendor management system and other ComplyAuto tools.
- No cookie-cutter templates. Ensure accurate disclosures about your unique data collection and sharing practices.

Multiple state and federal laws govern online privacy disclosures.

Dealers can be held liable for failing to accurately notify its customers of its practices for collecting or sharing personal information.

Unfortunately, the cookie-cutter default disclosures provided by website providers are not sufficient.

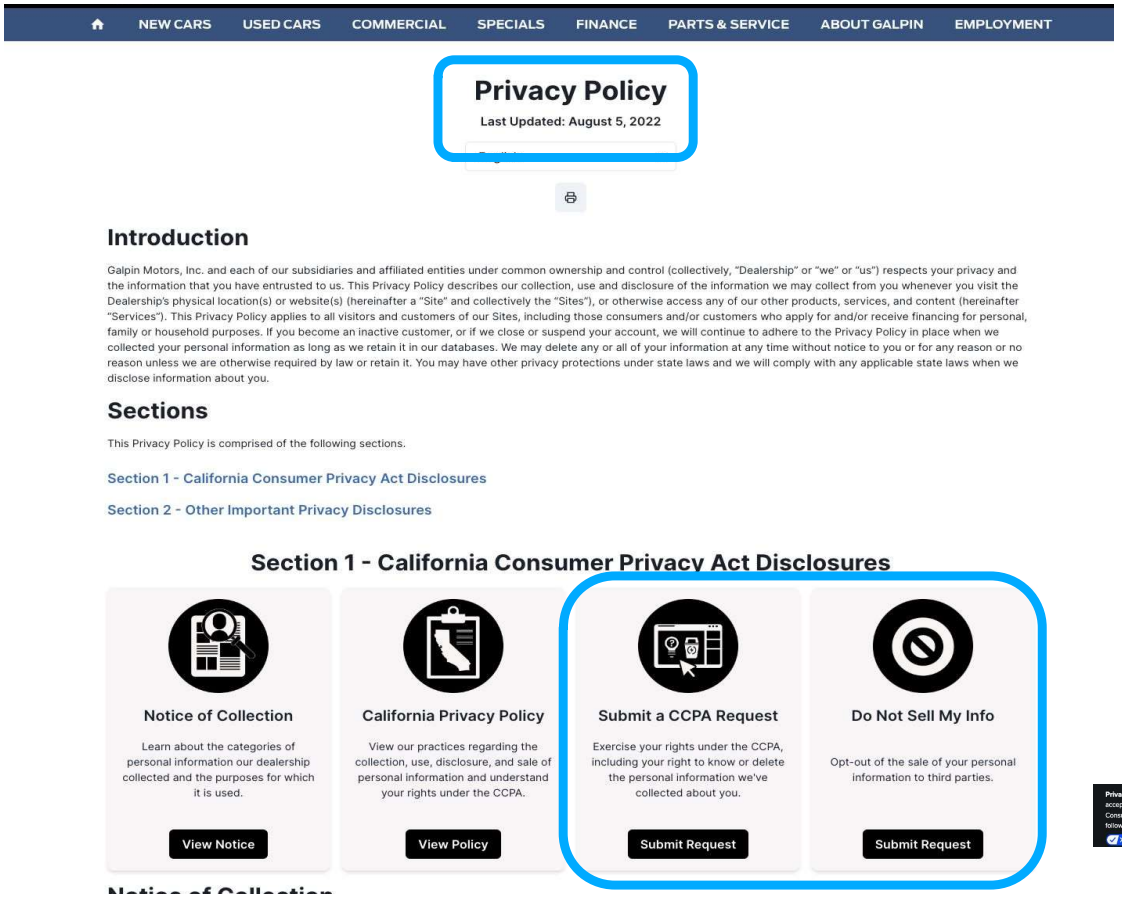
Consumer Privacy Portal (DSAR)

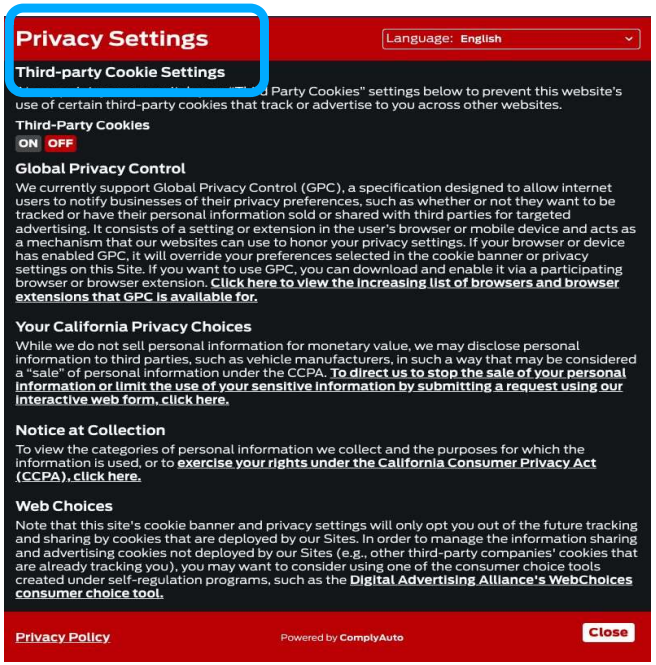
- Automate opt-out, deletion, and right to know / access requests.
- Give consumers transparency and control over their personal information.
- Ensure compliance for residents of regulated states (CA, CO, CT, VA, UT).

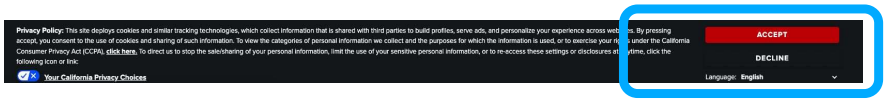
Several states granted new privacy rights to their residents, such as the ability to opt-out of data sharing and the right to know, delete, and access information collection about them.

There is a common misconception that only dealerships in those states need to comply, but dealerships have potential exposure, for example, if they are collecting information on these out-of-state residents (including cookies and similar information) who shop or browse online.

Consumer Privacy Tools and Disclosures







Consumer Privacy Rights Compliance

APPLICABLE LAW OR REGULATION

Many states, like Ohio, California, Utah, and Connecticut offer forms of limited liability or even safe harbor for adhering to frameworks like the CIS Controls.

Other State Specific Requirements:

- Consumer Privacy Rights employee training
- Third-Party Vendor Data Processing agreements and/or Vendor Risk Assessment
- B2B or Employee Privacy Rights
- Process Consumer Privacy Requests, notify third-party vendors

CIS SecureSuite® Membership

What to expect in the coming months
(if you're complying)

THINGS YOU'LL NOTICE

1. **Multi-factor authentication upon login to systems containing customer information**
2. **More complex passwords (8-14 character alphanumeric)**
3. **Automatic timeouts on computer of 15 minutes or less**
4. **Phishing susceptibility tests!**
5. **Controls on sharing sensitive customer information**
6. **Corporate email accounts**
7. **Security awareness training**
8. **Cookie banners (and unfortunately less retargeting)**

What to expect in the coming months

(if you're complying)

Do's & Don'ts

✔ **Do use a password manager tool**
✘ **Don't use weak or repeat passwords (or store them in plain text**

✔ **Do set up individual user profiles for workstations**
✘ **Don't used shared logins or passwords**

✔ **Do use corporate email accounts**
✘ **Don't use personal email addresses for work purposes**

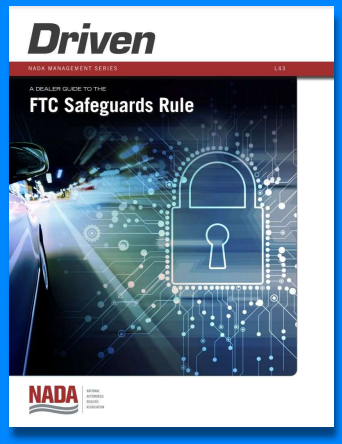
✔ **Do use a tool to send/receive encrypted customer info**
✘ **Don't send/receive such info via text or email**

✔ **Do upgrade all machines to Windows 10+ (or latest iOS)**
✘ **Don't allow connected Windows 7 machines**

✔ **Do check every email for suspicious content**
✘ **Don't click on phishing emails!**

ComplyAuto was chosen as an NADA Affinity Provider for compliance and helped draft the NADA FTC Safeguards Manual

TURN-KEY SOFTWARE SOLUTION



NADA AFFINITY PROVIDER + COMPLYAUTO PRIVACY

- Qualified Employee
- Written Risk Assessment
- Access Controls
- Data and Systems Inventory
- Data Encryption
- Intrusion Detection/ Vulnerability Testing
- Multi-Factor Authentication
- Systems Monitoring and Logging
- Secure Data Disposal Procedures
- Change Management Procedures
- Unauthorized Activity Monitoring
- Overseeing/Monitoring Service Providers
- Written Incident Response Plan
- Annual Reporting to Board

THE COMPLYAUTO DIFFERENCE

Month-to-month
We treat dealers the way we wanted to be treated as dealers, which means no long term contracts.

Unlimited Support
With ComplyAuto, you get a dedicated client success manager and unlimited technical support.

No Setup Fees
No additional implementation fees, service charges, or installation costs. Just a simple monthly subscription fee.

First Month Free
Complete a short setup survey within 2 weeks and get the first month of ComplyAuto completely free!

Annual Discount (10%)
Get an additional 10% off for annual billing. Even then, your contract term stays month-to-month.

Endorsed By More State Dealer Associations than Any Other Provider

There's a reason why the NADA and +35 state associations have endorsed ComplyAuto for compliance.

Let us show you why.

COMPLYAUTO PRIVACY

NADA AFFINITY PROVIDER

Join the nation's #1 Dealership Privacy & Cybersecurity Platform

GUARANTEE 100% COMPLIANCE

50-state legal compliance with the industry's only

COMPLIANCE GUARANTEE

Worry less and sell more. We are so confident that ComplyAuto is the best way to comply with privacy and cybersecurity laws that if you're using our platform and you receive a penalty or fine under a privacy or cybersecurity regulation from a governmental agency that is caused by using our platform, we will pay the fine or penalty up to $100,000. Learn more at https://complyauto.com/compliance-guarantee/

MileOne · Jenkins Auto Group · LeithCars.com · Sheehy · Premier Automotive · Calpine Motors · Serra Automotive · Penske · Norm Reeves Superstores · Jeff Wyler · Sunroad Auto · Koons · LAcarGUY · Hansel · DGDG · Paul Miller · Payne

COMPLYAUTO PRIVACY

Transparent Pricing

https://complyauto.com/pricing/

Questions?

Scan for contact info:

Thank you!

https://www.complyauto.com
info@complyauto.com
(661) 214-3028