COMPLYAUTO

Compliance and Risk Mitigation

Federal and State Cybersecurity & Privacy Laws, Environmental Health and Safety

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)*

+9,000
Active Dealers

+36
State Dealer Association Endorsements

99.9%
Dealer Retention

COMPLYAUTO PRIVACY

Risk #1 Federal Safeguards Essentials

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.

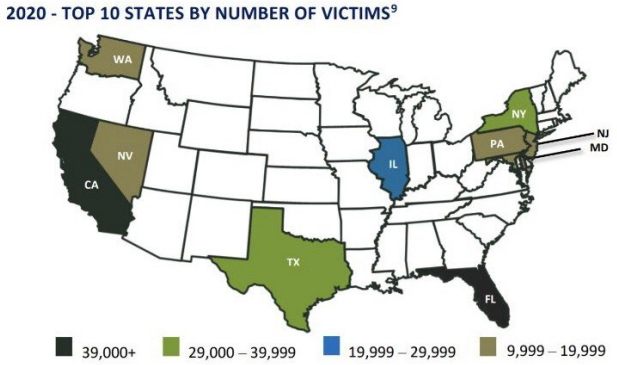
Every state now has its own data breach reporting obligations and some have specific cybersecurity and privacy regulations that grant safe harbor for meeting certain cybersecurity standards.

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

Data Breach Implications

- **Network/system downtimes**. Prepare to start handwriting contracts and calling bank analysts. Typical downtime is 3 days to 2 weeks.
- **Data loss.** DMS & CRM data (all your prospects and leads), custom sales reports, financial data, employee information, policies, proprietary data, legal files, etc.
- **Reputational damage**. Customer trust, public image resulting from security breach. 84% of consumers said they would not buy another car from a dealership after their data had been compromised
- **Financial loss**. Paying the ransom will usually cost you at least six figures. Does not include lost business, time, wages, files, equipment, and any third-party remediation services or security consulting.
- **Legal Liability**. Data breach reporting obligations, identity theft, negligence, government enforcement (FTC, State AG)

FBI: Businesses reported paying over $29.1 million in ransoms in 2020. **Phishing** was the number one cause of data breaches ransomware.



What does your policy cover?

- Cyber policies aren't cheap, but they will be well worth it if you find yourself being a victim of a data breach.
- Following a breach, industry standard is to pay for identity theft monitoring services for at least a year - will your carrier pay for that?
- Does it cover a ransomware payments if you choose or have to pay one? What about the other potential damages listed on this slide?
- A broker will help you navigate through these issues and considerations (and much more).

New FTC Safeguards Rule Requirements -
Effective June 9th, 2023.

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

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	

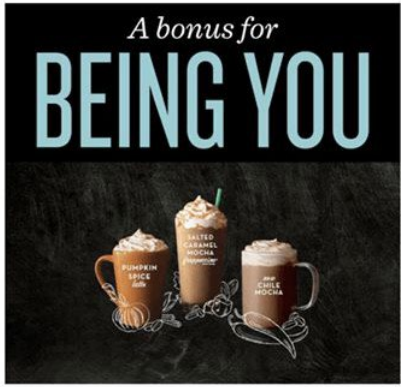
NADA NATIONAL AUTOMOBILE DEALERS ASSOCIATION

Are you compliant on the FTC Safeguards rule?

Areas dealers may not be covered?

- Updatable Written legal policies - Templates
- Phishing Simulations - 95% of all cyber attacks start with an employee
- Vendor Contracts & Vendor Risk Assessments
- Penetration Test or Vulnerability Assessment
- Systems Inventory and Data Mapping
- Written Annual Report to Board
- Cybersecurity Tools
- Intrusion Detections such as EDR, MDR
    - Email Scanning Protection
    - Data Loss Prevention - monitoring to ensure employees don't send NPI
    - Encryption - In transit and device
    - Multi Factor Authentication - email, vendors and device level


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



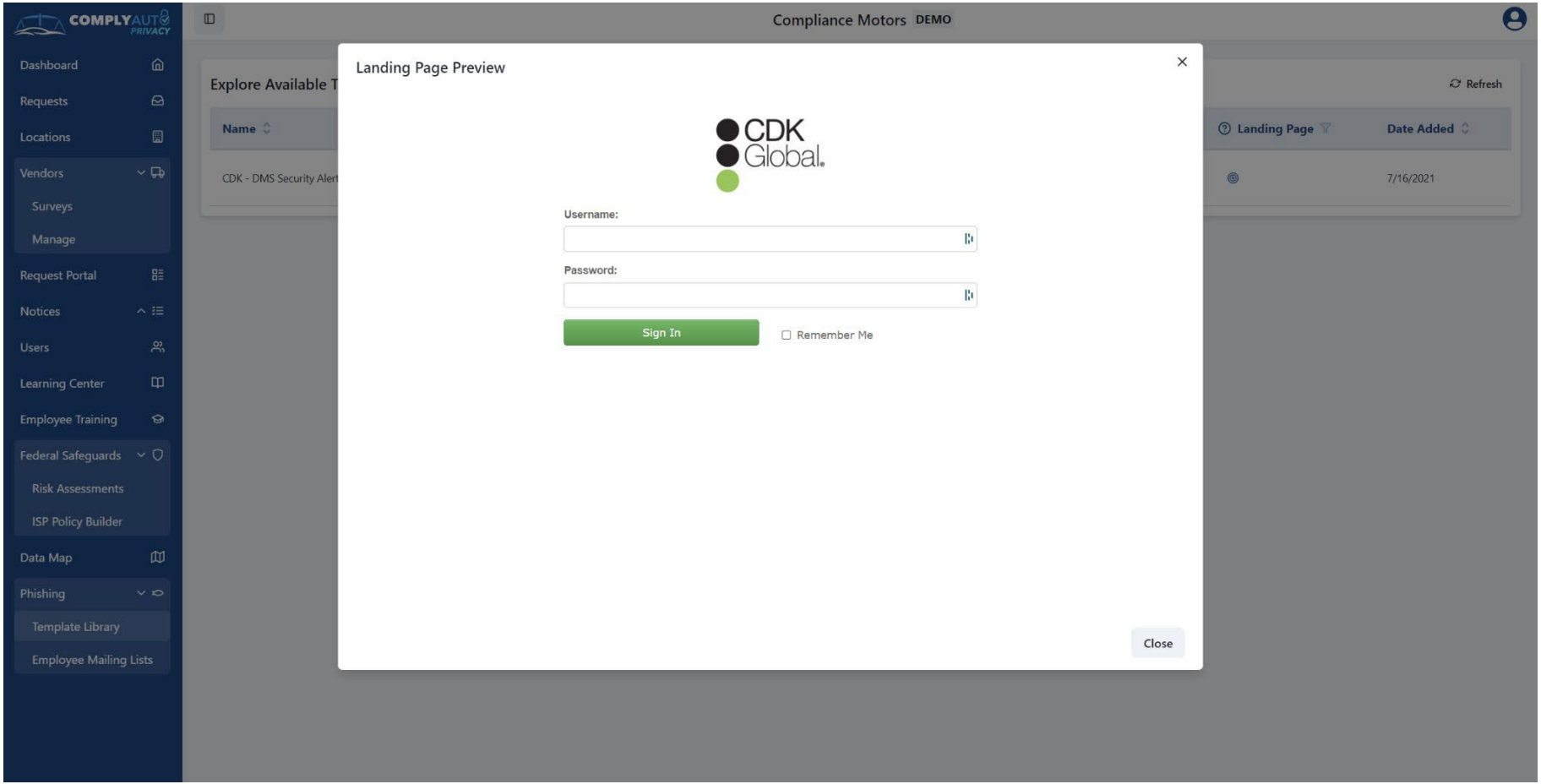
First Fall Favorite on Us!

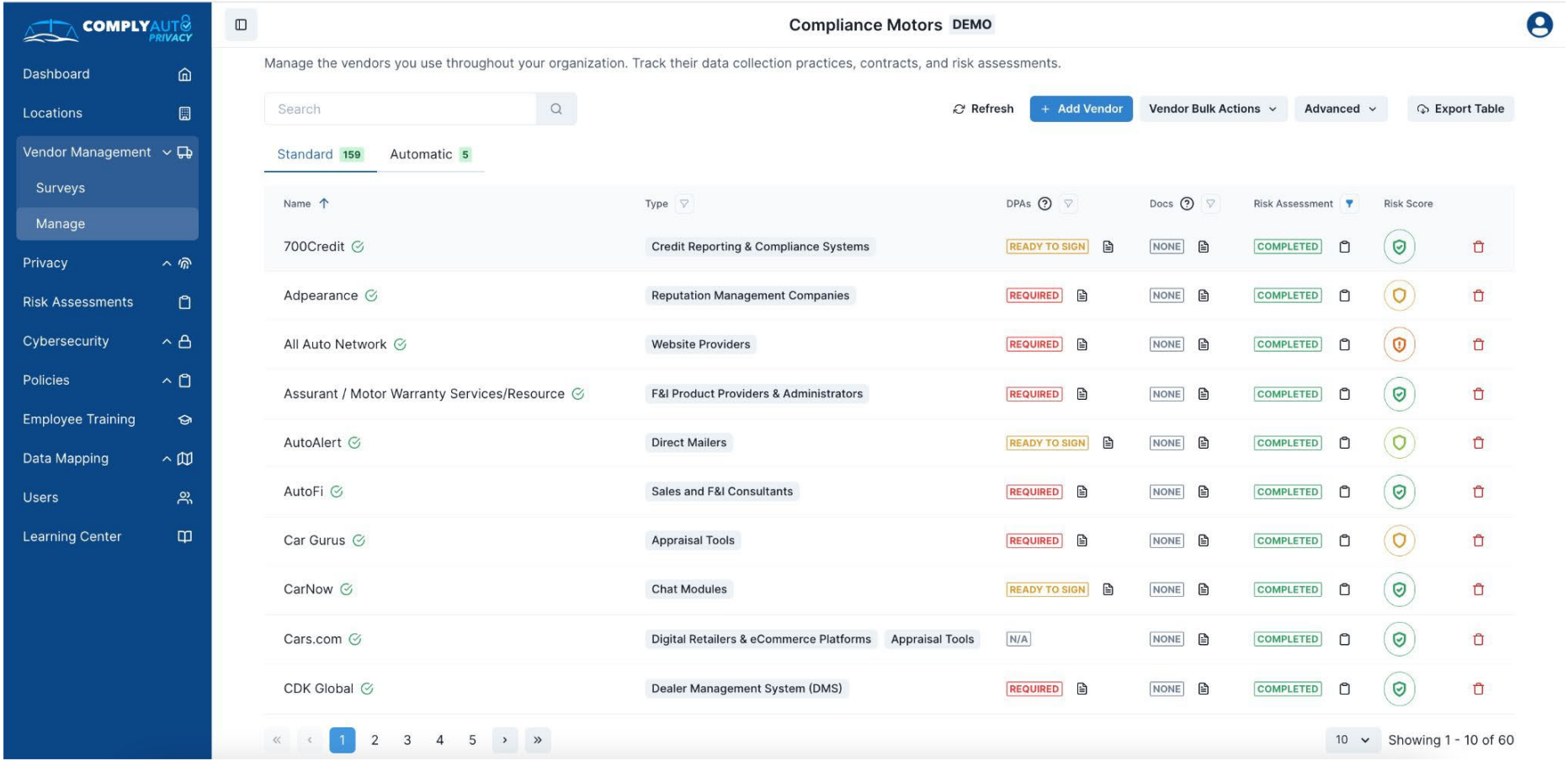
Fall flavors are in full swing with the return of Pumpkin Spice Latte and Salted Caramel Mocha, and the arrival of our new Chile Mocha. Each can be enjoyed hot or blended to satisfy your seasonal craving. And your first one's free!

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


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

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)

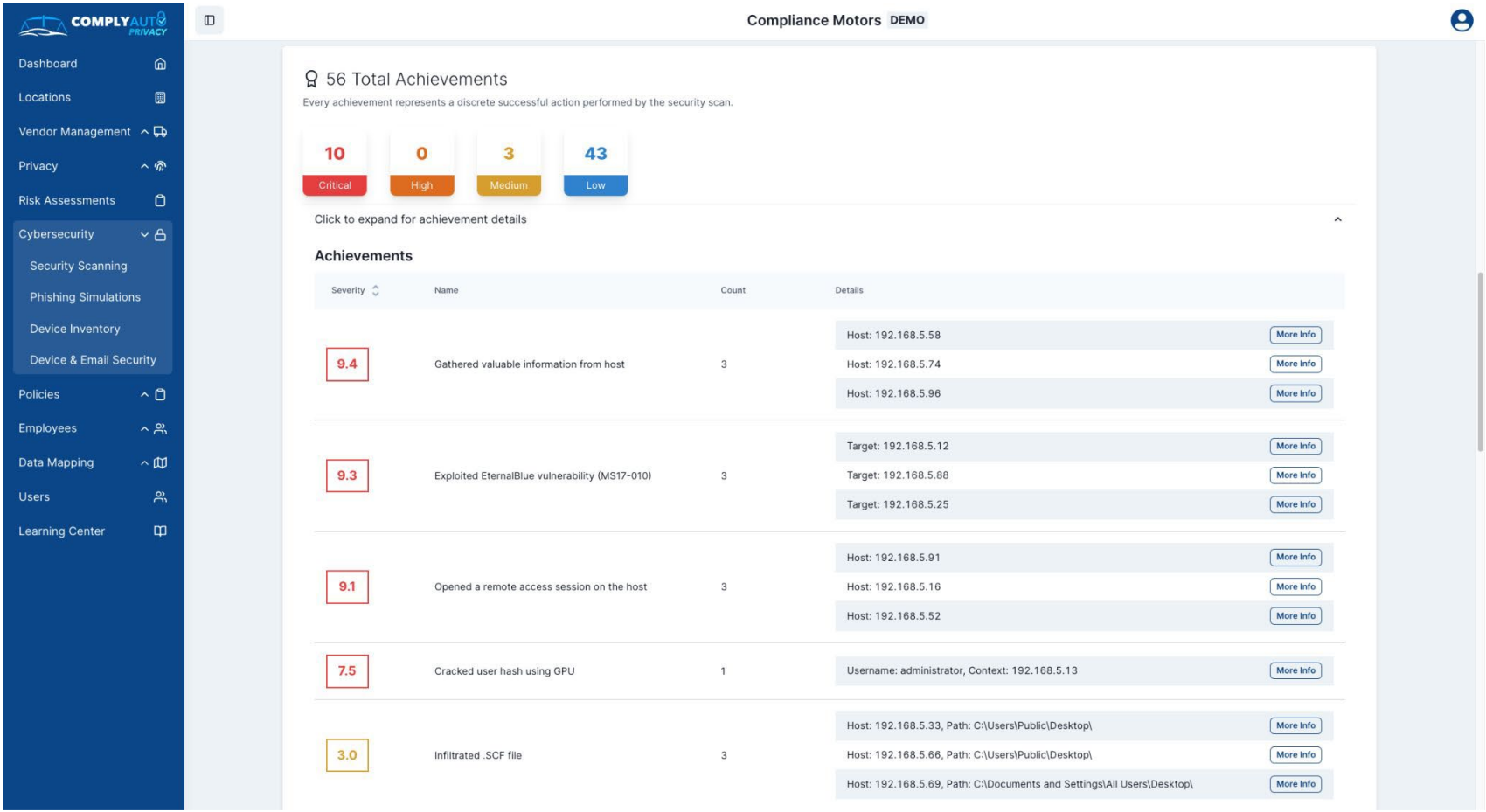
PRACTICAL TIPS
No, the law doesn't require human testers. It can be automated.
ComplyAuto services include a full internal penetration test (performed biannually) that satisfies regulatory requirements and does everything from password cracking, remote code execution, credentials sniffing, ransomware 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

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)

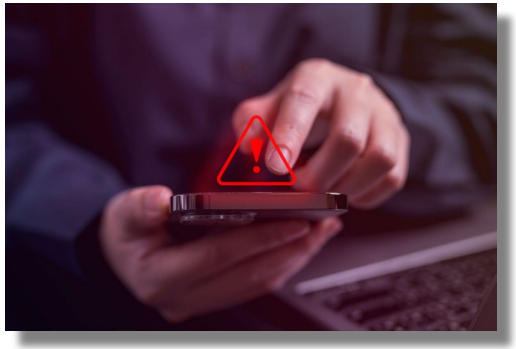
FTC Safeguards Rule Encryption In Transit Requirement

16 CFR 314.4(c)(3)

Dealers shall *"Protect by encryption all customer information transmitted in transit over external networks . . ."*

COMPLYAUTO PRIVACY

Limitations of Traditional Email and Text for Sensitive Information & NPI



- **Inherent Security Risks:** Lack of end-to-end encryption; vulnerable to cyber-attacks, data breaches, and interception during transit.
- **Phishing Attacks:** High susceptibility due to difficulty in verifying the sender's identity, increasing the risk of information leakage.
- **Insufficient Access Control:** Emails and texts can be easily accessed if the device is lost or stolen, leading to potential unauthorized access.

Typical Dealership Problems

- Sales & finance staff commonly request that bank stips are sent to their phone via text or unencrypted email
- Most are using personal phones (what happens when they leave?)
- Common for the average salesperson to have hundreds of drivers licenses, POI, POR, and even SSN cards on their phones that were sent via text message.
- Losing a device could mean a reportable data breach
- Existing encryption tools are cumbersome and cause staff to resort back to unsecure methods

COMPLYAUTO PRIVACY

ComplyAuto is solving the text/email problem.

Easily satisfy technical requirements for encryption of data in transit. 16 CFR § 314.4(c)(3).

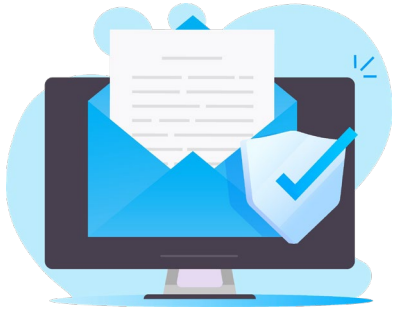
STEP 1

Scan QR or enter unique URL to access encrypted messaging portal.

STEP 2

Generate a secure file request link and text or email it to the customer.

STEP 3



Get notified when customers upload files and securely download them.

- Control who can request & receive files
- Include a secure link in email signatures so customers can easily send stips and other sensitive info
- File access protected by MFA in accordance with FTC requirements
- Customize auto-delete settings for files

Allow your staff to effortlessly comply with compliance requirements with free end-to-end encryption tools

Don't invest in other encryption tools that don't verify data-handling compliance.

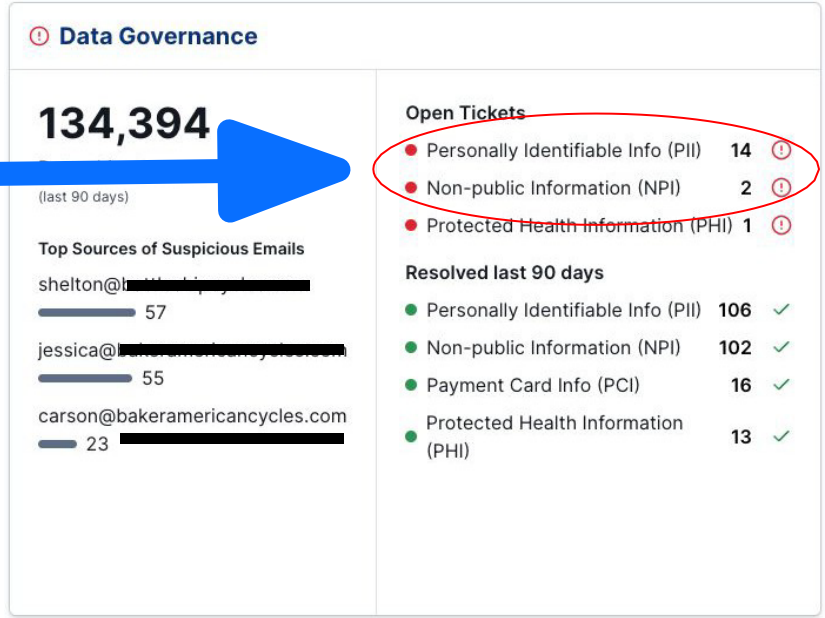
User & Employee Monitoring & Logging

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).

Dealers already have access to Data Loss Protection who use our ComplyAuto add-on cybersecurity tools (Coro Dashboard).

This means every device and email is scanned to detect employee data security violations (i.e., sending messages asking for PCI, NPI, PII sharing).

Experience real-time monitoring, exclusive to ComplyAuto, ensuring active use of CompyCrypt to stay compliant.



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

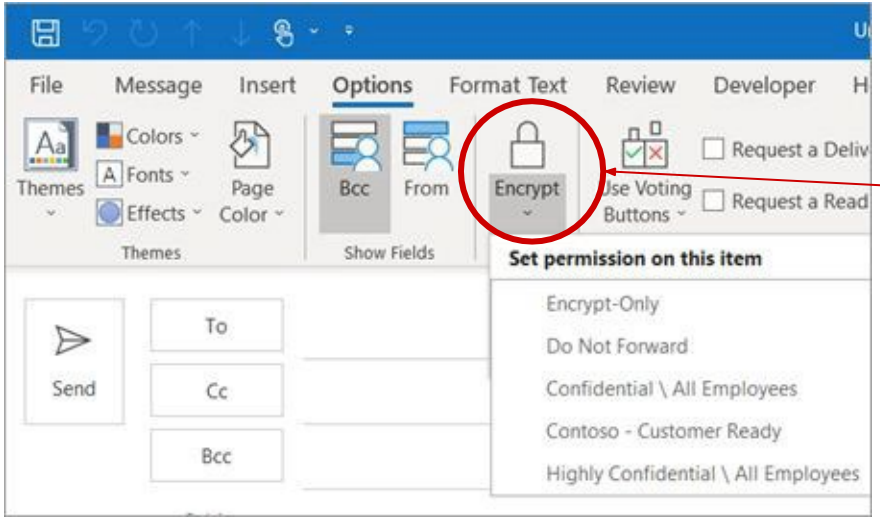
- Firewall Disabled
- Malware on Endpoint
- UAC Notification Missing
- Device Password Missing
- Unencrypted Endpoint Drive
- Non-genuine Windows copy

Data Governance

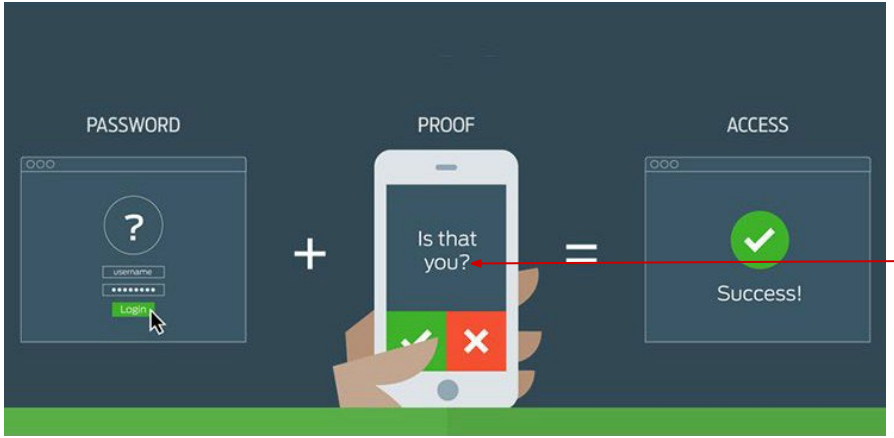
96,697
Data objects processed
(last 90 days)

Email

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



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 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

COMPLYAUTO PRIVACY

Risk # 2 - State Specific Consumer Privacy Laws

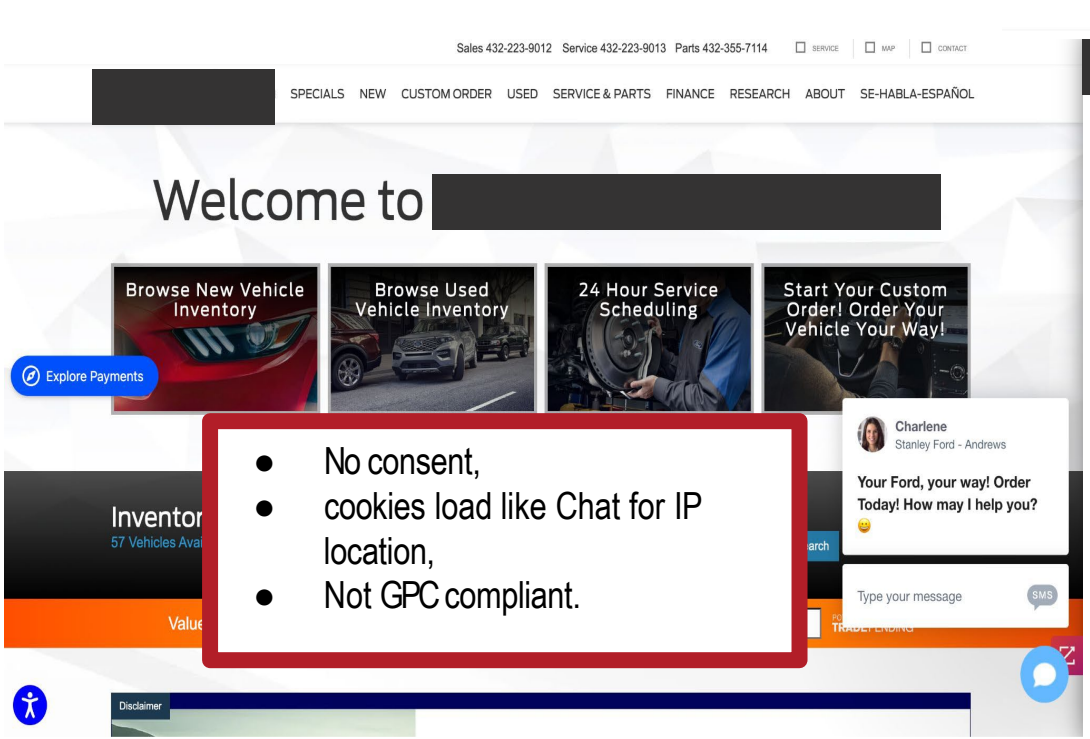
Consumer Privacy Rights Compliance

Compliant Cookie Banner

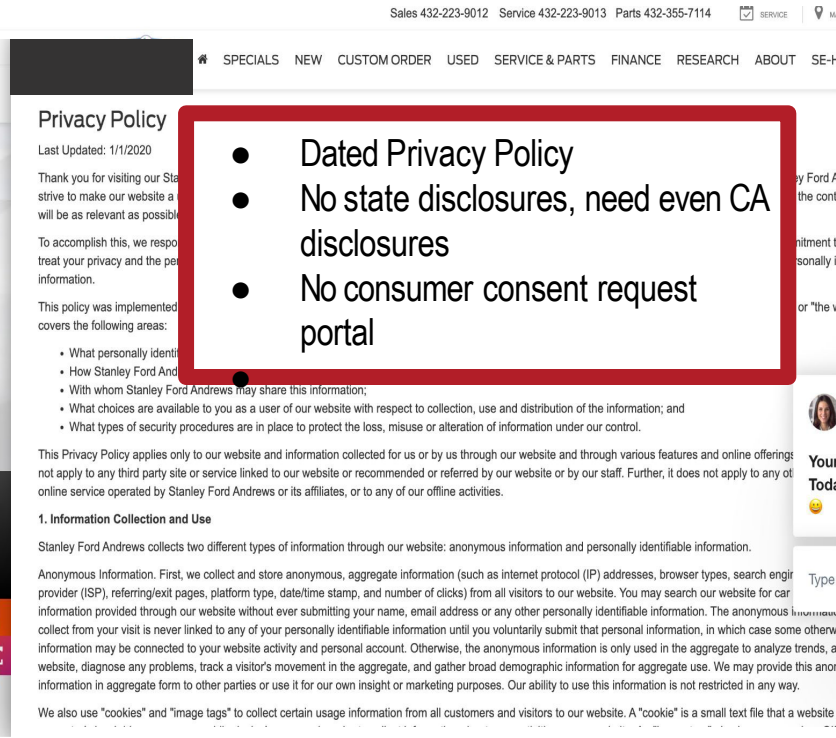
Most out-of-the-box cookie banners provided by website providers are non-compliant and cause more harm than good. Our banner actually blocks third-party advertising cookies, records consent, and respects global privacy controls (GPCs) in accordance with applicable privacy laws.

- Fully customizable and branded
- Identifies and blocks applicable 3rd-party cookies
- Tested on all common dealership website providers
- Manage other requirements such as:
    - 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

Typical Dealership Websites



- No consent,
- cookies load like Chat for IP location,
- Not GPC compliant.



- Dated Privacy Policy
- No state disclosures, need even CA disclosures
- No consent request portal

Consumer Privacy Rights Compliance

States Bills Passed to be Signed:

- Oregon
- Delaware

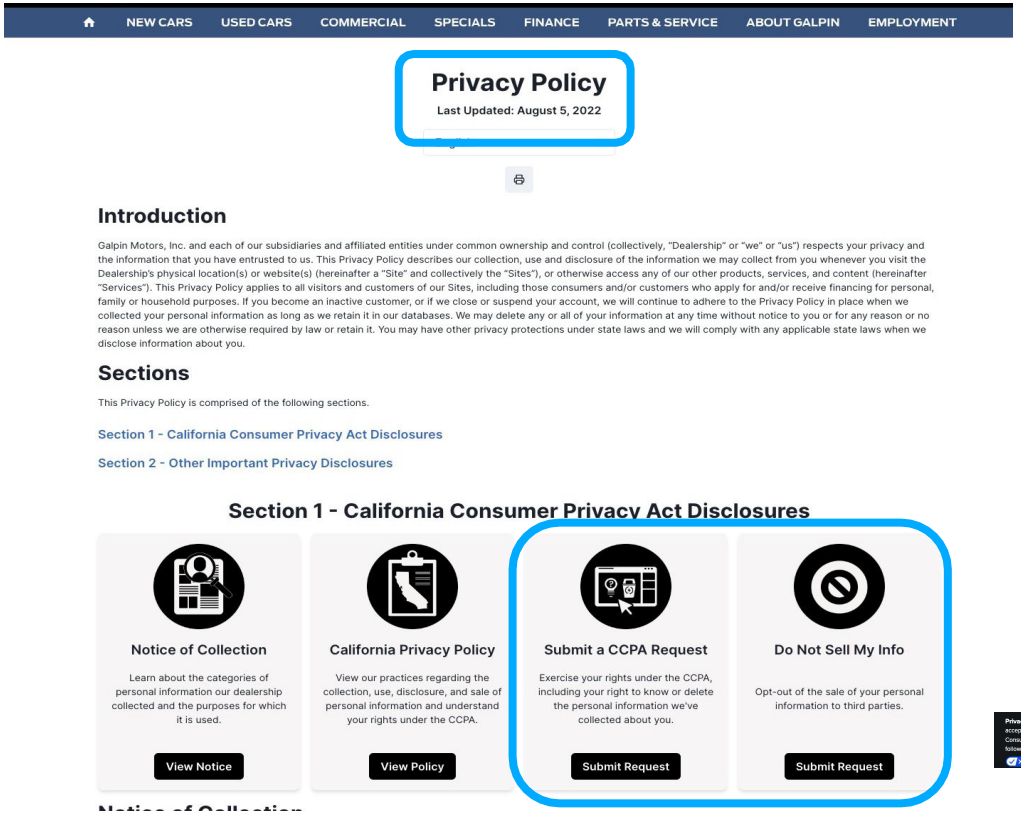
Should you be concerned about cookie consent and privacy rights issues if your state doesn't have a comprehensive privacy law?

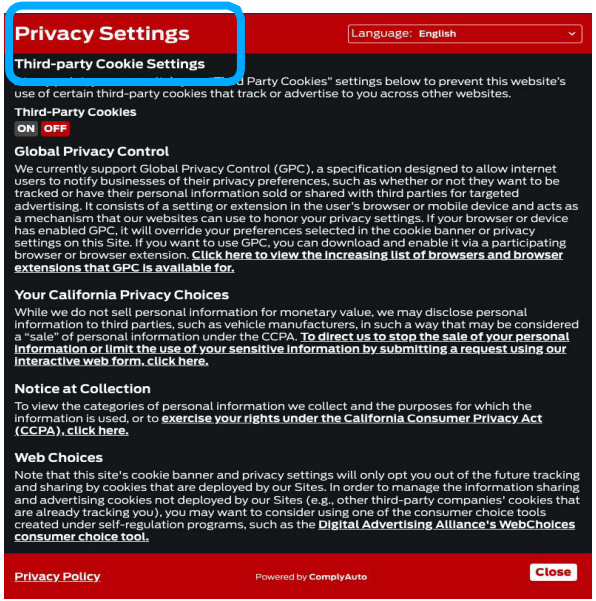
YES, the FTC wants a piece of the state privacy law action!

- 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, **9 states have proposed Consumer Privacy Rights Legislation.**
- Ten States enacted comprehensive privacy laws with **fines ranging from $5,000-$20,000**

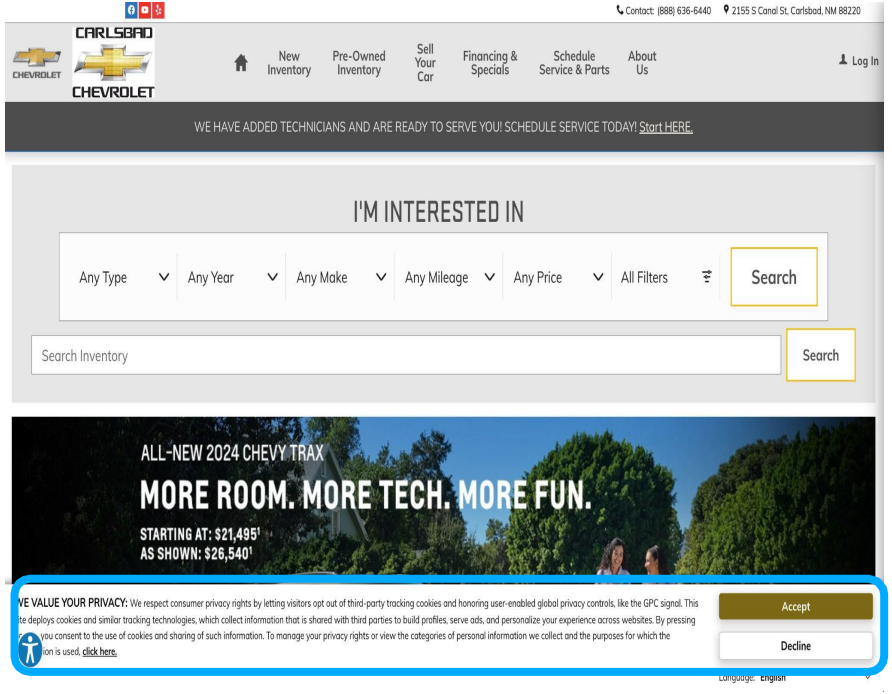
source: US State Privacy Legislation IAAP's Resource Center

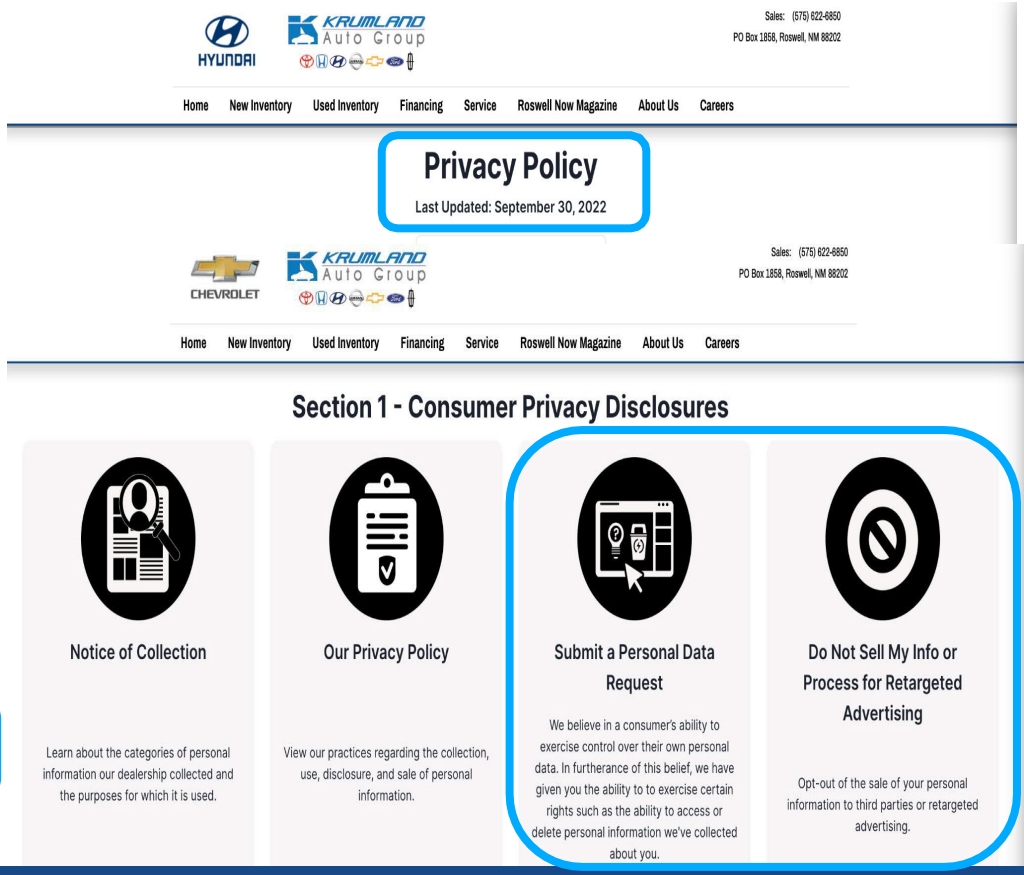
Consumer Privacy Tools and Disclosures





Consumer Privacy Tools and Disclosures





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!

✔ Do update your cookie banner for compliant
✘ Don't rely on your web provider policy for the proper disclosures

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.

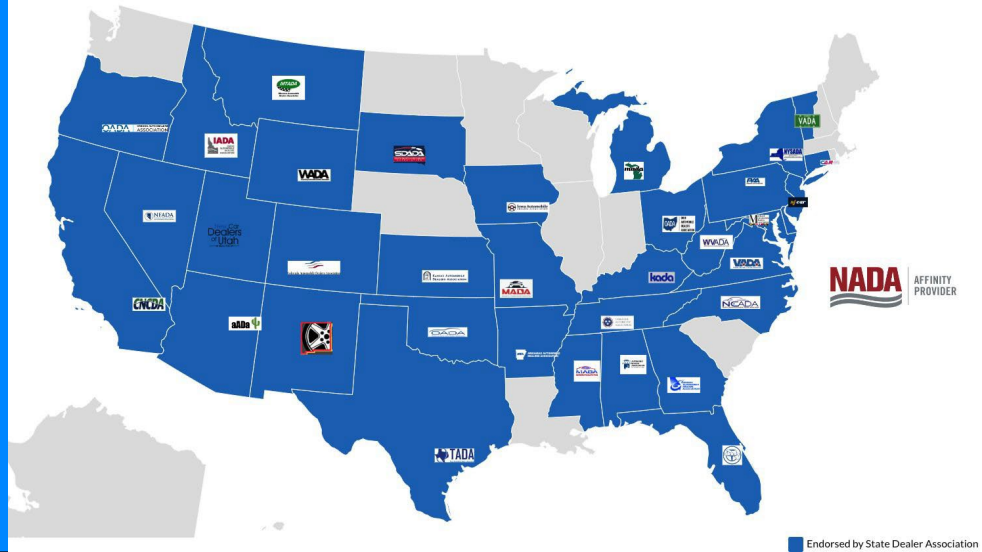
First Month Free
Complete a short setup survey within 2 weeks and get the first month of ComplyAuto completely free!

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 · Motor1 · Serra Automotive · Penske · Norm Reeves Superstores · Jeff Wyler · Sunroad Auto · Koons · LAcarGUY · Impact Automotive Group · Hansel · DGDG · Paul Miller · Payne · Wheelhouse

COMPLYAUTO SAFETY

Risk # 3 - Environmental Health and Safety

THINGS TO CONSIDER IN 2023

1. OSHA regulators have more autonomy to issue fines and can cease dealership operations under unsafe work conditions.
2. OSHA announced this year to expect fines to increase YOY.
3. Ensure equipment inspections are being conducted consistently.
4. LOTO!
5. OSHA just took its first enforcement action for workplace violence.
6. Expect increased enforcement for failure to report/record injuries & illnesses timely and accurately.

OSHA Penalties

The Occupational Safety & Health Administration (OSHA) continues to gain more autonomy to increase fines and now has the power to actually shut down a business for violations.

Below are the maximum penalty amounts, with the annual adjustment for inflation, that may be assessed after Jan. 15, 2023. (See OSHA Memo, Dec. 20, 2022).

Types of Violations	Penalty
Serious Other-Than-Serious Posting Requirements	**$15,625 per violation**
Failure to Abate	**$15,625 per day beyond the abatement date**
Willful or Repeated	**$156,259 per violation**

States that operate their own Occupational Safety and Health Plans are required to adopt maximum penalty levels that are at least as effective as Federal OSHA.

OSHA Top 10 Violations in 2022

The list of OSHA's highest proposed monetary penalties in fiscal year 2022 comprises those stemming from a single incident or related incidents in which one or more employers allegedly failed to adhere to safe work practices. These failures put workers at risk – in some cases, fatally.

The Top 10 Most Cited Workplace Safety Standards for FY 2022

1. Fall Protection – General Requirements: 5,260 violations
2. Hazard Communication: 2,424
3. Respiratory Protection: 2,185
4. Ladders: 2,143
5. Scaffolding: 2,058
6. Lockout/Tagout: 1,977
7. Powered Industrial Trucks: 1,749
8. Fall Protection – Training Requirements: 1,556
9. Personal Protective and Lifesaving Equipment – Eye and Face Protection: 1,401
10. Machine Guarding: 1,370

The 2nd largest OSHA fine last year was for $1.2M at an auto parts retailer where the employer failed to have proper safeguards to protect workers from an accidental machine startup after a vehicle lift crushed a worker's hand.

Other agency findings included the company's willful failure to develop and implement lockout/tagout procedures.

Source: Patrick Kapust, acting director of OSHA's Directorate of Enforcement Programs, as presented at NSC Safety Congress & Expo and Safety and Health Magazine.

What if OSHA shows up at your dealership?

The following are employer/employee rights during an OSHA inspection:

1. **Employers do not need to let OSHA perform an inspection without a warrant. (If you have nothing to hide, then this is not always recommended as it may sour the relationship with the local OSHA office).**
2. **You can make an inspector wait for 60 min prior to starting the inspection; this gives you an opportunity to contact a company representative or attorney.**
3. **If the inspection arose because of a complaint, you can demand to see a copy of the complaint.**
4. **You can have management or any other personnel accompany the OSHA inspector.**
5. **Negotiate to narrow the scope of the inspection; if OSHA has gone through the trouble of getting a warrant it's likely they have a specific issue or area they wish to inspect.**
6. **Inquire as to what the inspection is for - you have the right to know what their probable cause is for the inspection.**
7. **Many OSHA inspectors are moving to audio/visual recording for employee interviews; employees can deny consent to be recorded but they should be aware that anything said during the interview is on the record.**

Workplace Violence Prevention and Response

According to OSHA, companies have an obligation to keep the workplace safe and secure. This means that if an active shooter event occurs and the dealership hasn't trained employees to respond, they haven't met the obligation to address reasonable threats to keep the workplace safe.

PRACTICAL TIPS
Workplace violence and active shooter issues on the rise. Just last year, OSHA enforced this issue for the first time under the General Duty Clause.
Identify risk factors - building security, handling large sums of cash, working in isolation, or late hours.
The best deterrent to workplace violence is to conduct adequate screening that prevents the hiring of individuals with a history of violent behavior.
Employers should establish a zero-tolerance policy for threatening or engaging in violent behavior, providing for employee disciplinary action up to and including dismissal.
Consider incorporating the following policies and trainings in your safety plan: • Workplace Violence Policy and Training. • Weapons in the Workplace Policy. (Check state law) • Active Shooter Policy, Training & Incident Response Team.
Discuss the elements of active shooter incident response planning with guidance from expert instructors. Have an Active Shooter Policy & Incident Response Team.
Incorporate key elements of successful incident management into planning efforts including: Communication and Incident Planning for employees, Emergency Action Plan Development, Recognizing Behavioral Indicators, and Coordinating with First Responders.

Equipment Inspection Management

OSHA safety requirements relating to the stability, function, fire protection, design, maintenance, and use of dealership equipment.

PRACTICAL TIPS

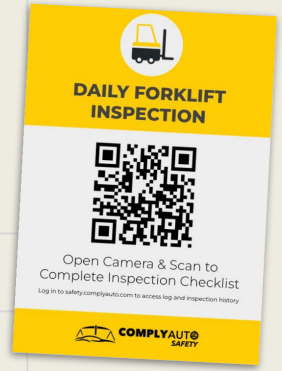
Know what needs to be inspected and frequency of inspections. (Can differ by state)

Typical inspections required:

- Forklifts - daily inspections. Differs by type of forklift, i.e. gas, propane, electric. OSHA Rule 1910.178(l)(1)(i)
- Eyewash stations - general flow, temperature, functionality and cleanliness. Periodic inspections (weekly) ANSI 358.2014, OSHA 29 CFR 1910.151(c).
- Scissor lifts & scaffolds - before each use. Overall inspection, good working condition. OSHA 1926.451(d)(3)(i)
- Aboveground Storage Tanks - Can be required daily or monthly based on state. Overall inspection of control panel function, leaks, pressurized, secondary containment. OSHA 1910.106.
- Underground Storage Tanks - Also required either monthly or annually in most states. May subject the dealership to creating a Spill Prevention, Control, and Countermeasure (SPCC) plan.
- Automotive Lift - annually conducted by a certified company. Do you have a sticker with the date of last inspection on your current lifts? Safety Requirements for Operation, Inspection and Maintenance ANSI/ALI ALOIM: 2020 Standard for Automotive.

If equipment doesn't pass inspection, it needs to be locked and tagged out immediately by a supervisor.

Make it easy for your employees to keep up with regular inspections. Do you have an electronic system?



Lockout Tagout Policies

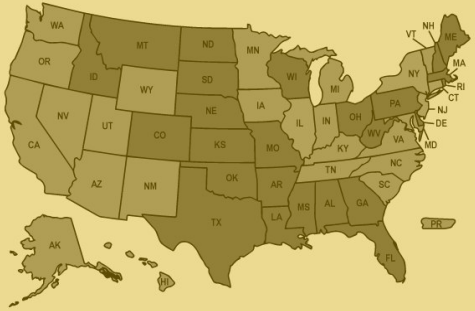
OSHA Standard 1910.147(a)(3)(i) requires employers to establish a program and procedures for affixing appropriate lockout devices or tagout devices to energy isolating devices, and to otherwise disable machines or equipment to prevent unexpected energization, start-up or release of stored energy in order to prevent injury to employees.

PRACTICAL TIPS
Do you have a lockout/tagout policy for your electrical equipment?
A lockout device utilizes a means such as a lock, either key or combination type, to hold an energy isolating device in a safe position and prevent the energizing of a machine or equipment.
If something isn't working properly, a manager needs to lock the machine/equipment so it cannot be used by any employees. Then a tag/sign needs to be on the machine stating Out-of-Order status.
Employees and managers need to be trained on lockout/tagout and need to sign a policy stating compliance on an annual basis.

Injury or Illness Recording & Reporting

The OSHA Standard 29 CFR Parts 1904 and 1952 require employers to keep records of occupational deaths, injuries, and illnesses. OSHA is ramping up enforcement of failure to timely or accurately report injuries and illnesses.

PRACTICAL TIPS
If there is ever an injury or illness that happens on sight, you need to know if it is: recordable, reportable, the timeframe to do so, and the agency to report to.
Know your state laws - in CA an injury or illness that results in permanent disfigurement is reportable within 24 hours. Know type of injuries that must be reported immediately versus annually.
Keep records of each injury or illness for OSHA 300 or OSHA 300A log (annually) and for worker's compensation purposes. Many HR/payroll softwares are inaccurate and some dealers have been fined for relying on such systems.
OSHA Form 300A data for the preceding calendar year must be electronically submitted to OSHA each year by March 2 of the following year and be posted in area accessible to employee from Feb 1st - April 30th.
Privacy cases - employee can request to exclude name from reporting illnesses. (required for HIV, TB, reproductive illnesses and injuries, etc.)



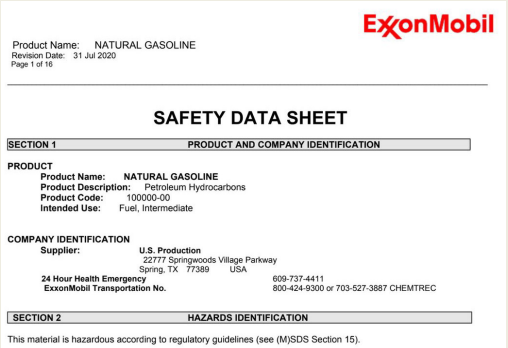
Lightly shaded states have special reporting requirements.

COMPLYAUTO SAFETY

SDS Management Tips

OSHA's Hazard Communication Standard (HCS) requires employers to maintain Safety Data Sheets for chemicals in the workplace and to ensure that employees can easily and readily access them.

PRACTICAL TIPS
SDS must have: PPE required, First Aid info, if medical intervention required, spill clean up instructions.
Need an SDS manifest with each chemical used near locations where chemicals are stored or in use.
Use Secondary Labels on containers not distributed by manufacturers, and must have the same information as primary label (sharpie with just a name is not sufficient.)
Best practice is to include Spanish language SDS sheets.
Doesn't have to be a binder, as OSHA allows electronic manifests, but employees must have easy access (i.e., no passwords)



ExxonMobil

Product Name: NATURAL GASOLINE
Revision Date: 31 Jul 2020
Page 1 of 16

SAFETY DATA SHEET

SECTION 1 PRODUCT AND COMPANY IDENTIFICATION

PRODUCT
Product Name: NATURAL GASOLINE
Product Description: Petroleum Hydrocarbons
Product Code: 100000-00
Intended Use: Fuel, Intermediate

COMPANY IDENTIFICATION
Supplier: U.S. Production
22777 Springwoods Village Parkway
Spring, TX 77389 USA
24 Hour Health Emergency 609-737-4411
ExxonMobil Transportation No. 800-424-9300 or 703-527-3887 CHEMTREC

SECTION 2 HAZARDS IDENTIFICATION

This material is hazardous according to regulatory guidelines (see (M)SDS Section 15).

COMPLYAUTO SAFETY

First Aid, CPR, & AED

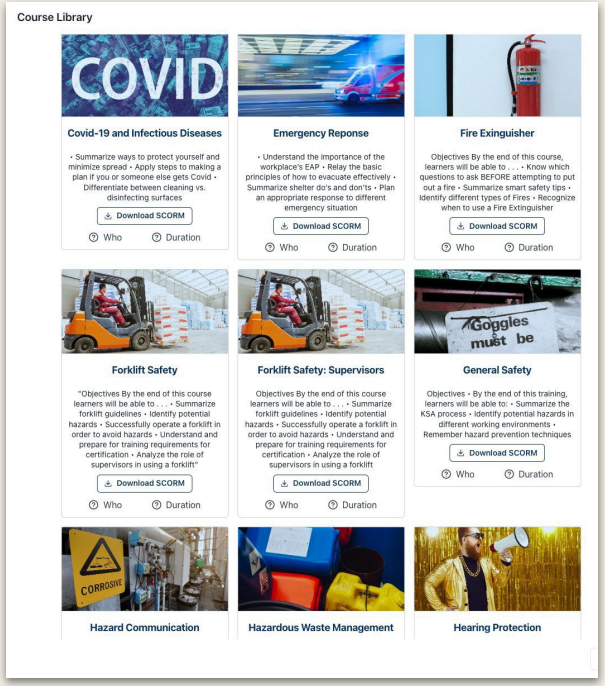
First aid supplies are required to be readily available under § 1910.151(b). When larger or multiple operations are being conducted at the same location, employers should determine the need for additional first aid kits at the worksite and additional quantities and types of supplies in the first aid kits.

PRACTICAL TIPS
Have multiple first aid kits located around dealership. Consider having a least one trauma kit. Make sure to inspect and restock first aid kit annually.
Best practice is to have trained employees on basic First Aid for cuts, falls, or know when to call 911.
Make sure you have enough trained employees for coverage of all shifts or time off/vacations.
Train every employee on emergency procedures and response.
Train employees to check SDS for first aid measures if contact with a chemical occurs.
OEM's are recommending EV dealers to have CPR & AED trained employees on-site.
If you have an AED, OSHA highly recommends to have a certified trained employee(s).

Safety Training

OSHA requires employers to provide training to workers who face hazards on the job. Many OSHA standards include explicit safety and health training requirements to ensure that workers have the required skills and knowledge to safely do their work.

PRACTICAL TIPS
Best practice is to complete training during onboarding, or at time of new equipment added to the worksite (i.e. purchased a new forklift).
Most trainings are required annually.
Train everyone - safety is everyone's job. At a minimum, everyone should be trained on Fire Extinguishers, Back Injury Prevention, General Safety, Covid-19, Emergency Response, and Safe Driving.
Look for training that is engaging and interactive for student retention/recall.
Integrate corresponding policies to be read and signed during training.
Other good training to consider: Heat & Cold Stress, Forklift, Hearing Protections, PPE, Shop Safety, Active Shooter, Wildfires, etc.



Do's & Don'ts

✔ Do routinely educate your workforce through new hire and recurring training.
✘ Don't assume a policy is enough. Part of the training process should include acknowledgement of policies.

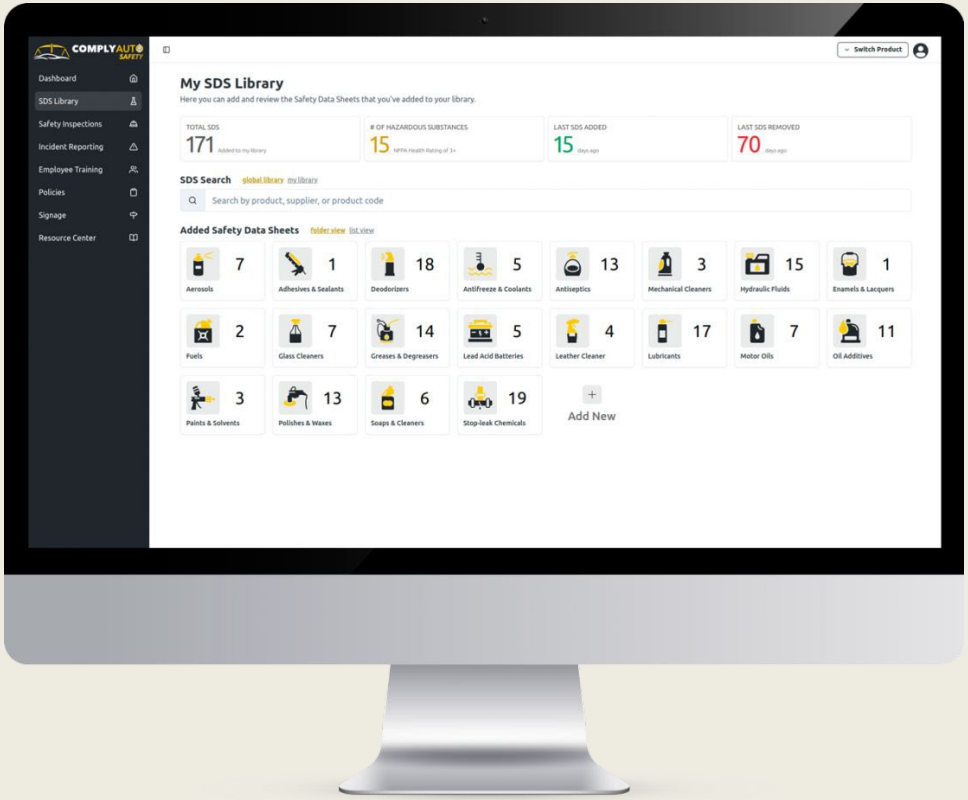
✔ Do report and record necessary injuries and illnesses in an accurate manner.
✘ Don't rely on memory or inaccurate software to determine whether to report/record injuries and illnesses.

✔ Do promote a culture of reporting safety concerns and performing required inspections.
✘ Don't be quiet about unsafe conditions; address and fix.

✔ Do implement a workplace violence prevention program.
✘ Don't ignore this newly enforced safety concern.

✔ Do strictly adhere to lockout/tagout procedures.
✘ Don't underestimate the danger damaged/unrepaired equipment and machinery can pose.

ComplyAuto Safety takes the stress out of EHS



ComplyAuto Safety offers unique and innovative features:

- Onsite inspections, includes one eight-hour mock OSHA audits by certified professionals
- Automated policy and signage builders
- Integrated Safety Data Sheet (SDS) Manager with a 10+ million product database (easy QR codes)
- Digital equipment inspections with QR code label generators and automatic reminders
- Comprehensive online safety training library with true "set it and forget it" enrollments
- Signage Builder and Tracker for all required signs
- The first and only tool automating injury & illness reporting requirements for all 50 states
- AED and CPR training provided by the American Red Cross
- Fisher Phillips, a nationally recognized law firm specializing in dealership workplace safety, routinely reviews and updates content.

COMPLYAUTO SAFETY

COMPLYAUTO

Transparent Pricing

https: /complyauto.com/pricing/

Questions?

Scan for contact info:

Thank you!

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