A Dealer’s Solution for the Revised 
FTC Safeguards Rule

Chris Cleveland  
CEO, ComplyAuto  
Compliance Director, Galpin Motors  
chris@complyauto.com

Hao Nguyen  
General Counsel  
ComplyAuto  
hao@complyauto.com

Brad Miller  
Chief Regulatory Counsel, Digital Affairs and Privacy | 
Director, Legal and Regulatory  
NADA  
bmiller@nada.org
Amended Safeguards Rule — the “Basics”

- Abandon “reasonable” standard for list of requirements
- Must comply by December 9, 2022
- Certain requirements do not apply if < 5,000 customer records
- Increased obligations internal systems and re Third Parties
What do the Amendments do?

Require

- Implementation of certain technical changes/tools
- Required policy changes/updates
- Written reports and documentation
- Training requirements

Clarify that “customer record” is viewed very broadly

- Not just SSN or CC#
- Not even just NPPI

Does not change liability per se, still no private right of action, but:

- Enforcement penalties – ($46,517/violation)
- UDAP violation as basis for state claims

Increased obligations re Third Parties

- Increased obligations internal systems and re Third Parties
NADA Driven Guide / Webinar

- Addresses each requirement in detail
- Includes input from IT specialists
- Includes appendices and exhibits
  - Sample written policies
  - Governmental resources
  - NADA Affinity Partner outsourcing resources

- Webinar: The Amended FTC Safeguards Rule - Overview and Update (nada.org)
These presentation materials are provided by the presenter who is solely responsible for the contents of the presentation. NADA assumes no responsibility or liability for the contents of the presentation.
Chris Cleveland  
CEO & Co-Founder, ComplyAuto  
Compliance Director, Galpin Motors

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

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

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

About ComplyAuto  
“By Dealers. For Dealers.”

- 60+ years of combined dealership compliance experience
- We are responsible for privacy and information security at our dealership groups and have implemented compliance with the revised FTC Safeguards Rules.
- ComplyAuto Privacy was created organically to solve problems faced by the owners at their own dealerships.
- Now, over 1,000 dealers are currently using the ComplyAuto software for privacy and cybersecurity compliance.
Legal Disclaimer

This presentation is intended to be used as a compliance aid for motor vehicle 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 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.
Summary of 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
- Phishing simulations & security awareness

- 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
- 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
- Phishing simulations & security awareness
E-SIGN FOR SERVICE PROVIDER CONTRACTS

ComplyAuto has built-in eSign functionality to easily send, receive, and track required service provider contracts required under the GLBA. We also help track who at each vendor will sign the agreements.

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.

MANUAL V/S AUTOMATED

<table>
<thead>
<tr>
<th>✗ Problem</th>
<th>✔ Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail/email each contract individually. Send manual reminders.</td>
<td>Send an eSign request with the click of a button.</td>
</tr>
<tr>
<td>Manually keep track of who signed in spreadsheets.</td>
<td>Everything is automatically tracked in ComplyAuto for demonstrable compliance.</td>
</tr>
<tr>
<td>Low success rate with getting returned contracts.</td>
<td>Vendors recognize our standard contracts and are more likely to sign it.</td>
</tr>
<tr>
<td>Store and organize returned contracts in a binder or scan/upload to an</td>
<td>When a vendor signs the contract, it’s automatically uploaded to the ComplyAuto portal and dropped in the vendor’s folder.</td>
</tr>
<tr>
<td>electronic file.</td>
<td></td>
</tr>
</tbody>
</table>
Dealers must now assess the adequacy of their vendors’ safeguards as well. Before signing with a new service provider (and periodically thereafter), require them to complete a risk assessment questionnaire that assesses their overall risk and ability to maintain appropriate physical, administrative, and technical safeguards.

**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.

---

### Manual vs Automated

<table>
<thead>
<tr>
<th>✗ Problem</th>
<th>✔ Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Difficulty determining which questions to ask.</td>
<td>ComplyAuto has done all the hard work for you by determining exactly which questions to ask.</td>
</tr>
<tr>
<td>Manually keep track of who completed the assessments in spreadsheets.</td>
<td>Everything is automatically tracked in ComplyAuto for demonstrable compliance.</td>
</tr>
<tr>
<td>Low success rate with getting returned assessments.</td>
<td>Vendors recognize our questionnaire and can even save their responses for all future dealers.</td>
</tr>
<tr>
<td>Store and organize returned assessments in a binder or scan/upload to an electronic file.</td>
<td>When a vendor completes the assessment, it’s automatically uploaded to the ComplyAuto portal and dropped in the vendor’s folder. ComplyAuto also automatically assigns a score for the vendor’s overall risk profile.</td>
</tr>
</tbody>
</table>
# Vendors

Manage the vendors you use throughout your organization. Track their data collection practices, contracts, and risk assessments.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>DPAs</th>
<th>Docs</th>
<th>Risk Assessment</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>700Credit</td>
<td>Credit Reporting &amp; Compliance Systems</td>
<td>REQUIRED</td>
<td>NONE</td>
<td>COMPLETED</td>
<td><img src="#" alt="Shield" /></td>
</tr>
<tr>
<td>ActiveEngage</td>
<td>Retargeting Services</td>
<td>REQUIRED</td>
<td>NONE</td>
<td>COMPLETED</td>
<td><img src="#" alt="Shield" /></td>
</tr>
<tr>
<td>Automotive Systems Analysis</td>
<td>Sales and F&amp;M Consultants</td>
<td>REQUIRED</td>
<td>NONE</td>
<td>COMPLETED</td>
<td><img src="#" alt="Shield" /></td>
</tr>
<tr>
<td>Charge Insurance</td>
<td>Workers Compensation Administrators</td>
<td>N/A</td>
<td>NONE</td>
<td>COMPLETED</td>
<td><img src="#" alt="Shield" /></td>
</tr>
<tr>
<td>Compliance Motors Testing Vendor Template</td>
<td>Call Tracking &amp; Phone Solutions</td>
<td>REQUIRED</td>
<td>NONE</td>
<td>COMPLETED</td>
<td><img src="#" alt="Shield" /></td>
</tr>
<tr>
<td>Credit Bureau Connection (CBC)</td>
<td>Credit Reporting &amp; Compliance Systems</td>
<td>REQUIRED</td>
<td>NONE</td>
<td>COMPLETED</td>
<td><img src="#" alt="Shield" /></td>
</tr>
<tr>
<td>CrossCheck</td>
<td>Check Guarantee Companies</td>
<td>REQUIRED</td>
<td>NONE</td>
<td>COMPLETED</td>
<td><img src="#" alt="Shield" /></td>
</tr>
</tbody>
</table>
Send Contract to Vendor for Signing

Vendor Name
Credit Bureau Connection (CBC)

Contract Type
GLBA Service Provider Agreement

Dealer Contact
Chris Cleveland (chris@complyauto.com)

Vendor's Email Address *
Darin Larsen (COO)
dlarsen@creditbureauconnection.com
Completed 100% of recent eSigns.

Suggested Vendor Emails

Your Legal Entity Name *

Your Organization or Group Name *
Compliance Motors

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

Additional Email Addresses to CC
Type or paste email addresses and press Enter or Space...

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

Copy Link to Clipboard

Close Send
AUTOMATED DATA MAPPING & SYSTEMS INVENTORY

Under the Revised Rule, dealers are required to perform both a data and systems inventory. 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. According to the FTC, this inventory forms the basis of an ISP because a system cannot be protected if the dealer does not understand its structure nor know what data is stored in which systems.

A data and systems inventory is the process of identifying and tracking how customer information is collected and flows through the dealership (data mapping), as well as documenting where it is stored, who it is shared with, and for which business purposes it is collected.

MANUAL V/S AUTOMATED

<table>
<thead>
<tr>
<th>❌ Problem</th>
<th>✔️ Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spend weeks calling or meeting with department heads at each location to determine which vendors are being used for which purposes.</td>
<td>Use our vendor survey tool to collect required information in days, not weeks, saving hours of time.</td>
</tr>
<tr>
<td>Manually determine and keep track of which vendors collect which types of info.</td>
<td>Add vendors with the click of a button using our library of dealer-specific templates (over 2,000).</td>
</tr>
<tr>
<td>Spend months mapping and documenting vendors and categories of information in an excel spreadsheet or data flow diagramming software.</td>
<td>Everything is automatically mapped in our interactive data inventory tool.</td>
</tr>
</tbody>
</table>

APPLICABLE LAW OR REGULATION

16 CFR §314.4(c)(2)

Dealers are required to perform a data and systems inventory where they must identify the data in their possession and inventory the systems on which the data is collected, stored, or transmitted.
## Interactive Data Map

### Filter by
- Personal Information

### SubFilter by
- None (Show All)

### Systems
- 10th Degree
- 11 Sight
- 700 Credit
- Accurate Background
- Acura
- Acura Small Claim Service
- Acura
- ActiveEngage
- Alliance Credit Union
- American Fidelity
- American Funds 401
- Associated Pension Consultants
- Audi Financial Services
- AutoAlert
- AutoLoop
- Automotive Product Consultants
- Automotive Product Consultants
- Automotive Systems Analysis

### Departments
- Digital and Telemarketing
- Human Resources
- Parts & Service
- Sales & F&I

### Locations
- All Locations

### Departments
- 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

### Interactive Elements
- 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
### APPLICABLE LAW OR REGULATION

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

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

### MANUAL V/S AUTOMATED

<table>
<thead>
<tr>
<th>✗ Problem</th>
<th>✓ Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using a cookie-cutter template provided by a vendor that isn’t tailored to your dealership.</td>
<td>ComplyAuto has a simple wizard that allows you to tailor the ISP to your dealership.</td>
</tr>
<tr>
<td>Most templates don’t take into consideration potential overlap with state privacy and data protection laws.</td>
<td>We’ve done the research to make our policies 50-state legal and also incorporated safeguards based on FTC enforcement actions and guidance.</td>
</tr>
<tr>
<td>Dealers must manually provide a copy to all employees and ensure they’ve acknowledged it.</td>
<td>Automatically embedded into our online employee training module so you know everyone received a copy.</td>
</tr>
<tr>
<td>Dealers must update the ISP everytime upon completion of a risk assessment.</td>
<td>Automatically gets updated when the law changes and syncs with your most recent risk assessment.</td>
</tr>
</tbody>
</table>

### AUTOMATIC ISP, IRP, DRP & ITCM POLICY BUILDER

Use ComplyAuto’s customizable policy builder to create the required Information Security Program, Incident Response Plan, Data Retention Plan, and IT Change Management Procedures in minutes.
New Info Sec Program - ABC Motors Information Security Program

Security Frameworks for Electronic & Technical Safeguards

Please select the security frameworks that your organization currently employs.
Note: These will be included in your Info Sec Program.

REQUIRED
- Physical & Administrative Safeguards Based on FTC Guidelines & Enforcement Actions

SAFEGUARDS
- Hold On to Information Only as Long as You Have a Legitimate Business Need
- Use Only Fake or Test Data for Training and Testing Purposes
- Restrict Electronic Access to Sensitive Data to Individuals With a Business Need
- Limit Administrative Access to a Neutral Department or Person
- Require Complex and Unique Passwords
- Ensure User Credentials Are Not Stored in Vulnerable Formats
- Enable MFA for All Systems Containing Nonpublic Personal Information
- Disable User Accounts After Multiple Unsuccessful Login Attempts
- Encrypt Data at Rest and in Transit
New Info Sec Program - ABC Motors Information Security Program

Incident Response Plan
Would you like to include an incident response plan in this Information Security Program? 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 Information Security 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
**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.

---

**MANUAL V/S AUTOMATED**

<table>
<thead>
<tr>
<th>✗ Problem</th>
<th>✔ Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hire a full-time data privacy officer or auditor trained in performing</td>
<td>Follow our guided risk assessments that are full of practical dealership</td>
</tr>
<tr>
<td>comprehensive risk assessments.</td>
<td>tips and recommended evaluation methods.</td>
</tr>
<tr>
<td>Outsource the audits to a professional who will perform limited functions</td>
<td>Our tools make performing both physical and technical risk assessments a</td>
</tr>
<tr>
<td>(usually just physical safeguards, such as unattended documents).</td>
<td>DIY task that anyone at the dealership can perform.</td>
</tr>
<tr>
<td>Manually track mitigation efforts and follow-up with offending employees.</td>
<td>Our tools makes mitigating risks easy to track and perform, such as with</td>
</tr>
<tr>
<td></td>
<td>automatically enrolling offending employees in security awareness training.</td>
</tr>
</tbody>
</table>
4. Limit Administrative Access to a Neutral Department or Person

5. Require Complex and Unique Passwords

6. Ensure User Credentials Are Not Stored in Vulnerable Formats

7. Enable MFA for All Systems Containing Nonpublic Personal Information

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?

**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 CEO 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

9. Encrypt Data at Rest and in Transit
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?**

<table>
<thead>
<tr>
<th>Practical Tip</th>
<th>Associated Risk</th>
<th>Evaluation Method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:

- Quad9: Steps for setting up Quad9 on Windows 10 ([https://www.quad9.net/microsoft](https://www.quad9.net/microsoft)).

38. Deploy and Maintain Anti-Malware Software

Risk: HIGH
TRAINING & LEARNING MANAGEMENT SYSTEM

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

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.

MANUAL V/S AUTOMATED

<table>
<thead>
<tr>
<th>Without ComplyAuto</th>
<th>With ComplyAuto</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic training that isn’t tailored to dealerships or the automotive industry.</td>
<td>Our training was developed by attorneys and compliance officers who actually worked at dealerships. Therefore, you can count on it being practical and to the point.</td>
</tr>
<tr>
<td>Locked-in to using a certain platform for tracking required training.</td>
<td>ComplyAuto recognizes that you may want to track training in a single HR platform. Therefore, all our courses are SCORM-compliant and exportable into any other compatible system.</td>
</tr>
<tr>
<td>Many vendors try to charge you extra for certain training modules or even limit the total number of enrollments.</td>
<td>Training is provided at no additional charge with an unlimited number of enrollments.</td>
</tr>
</tbody>
</table>
Privacy, Phishing, and Information Security Awareness

Overview

Both federal and state laws require dealers to implement a variety of safeguards to protect the security and confidentiality of customer information. Dealers are obligated to not only protect sensitive customer information, but also notify customers and regulatory agencies in the event of a security breach and establish both physical and electronic safeguards. Given the nature of dealers’ business practices, most, if not all, employees have access to sensitive customer information. This training will cover policies and procedures necessary to safeguarding customer information. Doing so ensures dealers are protecting their customer base and providing outstanding service to their customers.

Course content

- Privacy and Information Security
- Phishing & Security Awareness

Start course →
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.

**MANUAL V/S AUTOMATED**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours of setup and installation even for technical staff.</td>
<td>Ran automatically through ComplyAuto’s next-gen tools.</td>
</tr>
<tr>
<td>Often relies on obsolete, limited or unreliable open source tools.</td>
<td>Leverages the best vulnerability scanning tools, including those cited by the FTC in the GLBA Safeguards Rule (OpenVAS)</td>
</tr>
<tr>
<td>Produces convoluted results with false-positives that are interpretable only by the most advanced IT professionals.</td>
<td>Focuses on only the important vulnerabilities with simple tips for mitigating the risks.</td>
</tr>
</tbody>
</table>

**BIANNUAL VULNERABILITY ASSESSMENTS**

Dealers must perform vulnerability assessments at least biannually.
ANNUAL PENETRATION TESTING

Penetration testing is a type of IT security test in which evaluators mimic real-world attacks to attempt to identify ways to circumvent the security features of an application, system, or network. A comprehensive internal penetration test will usually include, at a minimum, the following:

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

APPLICABLE LAW OR REGULATION

16 CFR §314.4(d)(1)(i)
Dealers must perform penetration tests of their IT infrastructure and information systems at least annually.

MANUAL V/S AUTOMATED

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-3 weeks onsite</td>
<td>3-8 hours offsite</td>
</tr>
<tr>
<td>Dependent on tester’s skills &amp; methods</td>
<td>Reliable &amp; consistent results; constantly updated</td>
</tr>
<tr>
<td>Expensive: Avg. $15,000 - $30,000 per test</td>
<td>Entire ComplyAuto platform costs less than $11,000/year for a single rooftop.</td>
</tr>
<tr>
<td>Limited in scope to certain types of tests</td>
<td>Full internal pentest that satisfies all regulations</td>
</tr>
<tr>
<td>Disrupts dealer operations with onsite testers and complex setups</td>
<td>Non-disruptive and simple setup that’s done in hours</td>
</tr>
<tr>
<td>No assistance with remediation of identified vulnerabilities</td>
<td>Easy to understand report including recommended actions for each identified issue</td>
</tr>
</tbody>
</table>
Herman Motors

Pen Test Overview

25 Total Vulnerabilities Detected

<table>
<thead>
<tr>
<th>Severity</th>
<th>Name</th>
<th>Count</th>
<th>Found On</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Using easy-to-guess password(s)</td>
<td>1</td>
<td>root</td>
<td>It is recommended to set a stronger password policy for every user 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 A013456 or Pa$$word.</td>
</tr>
<tr>
<td>Medium</td>
<td>Captured credentials by forced authentication of a rogue server</td>
<td>4</td>
<td>FTPSERVER, MSSQLSERVER, workgroup</td>
<td>It is recommended to disable the LLWNR 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 IPv6 or Multicast-DNS hence consider disabling them as well.</td>
</tr>
<tr>
<td>Medium</td>
<td>Discovered closed ports on the host</td>
<td>16</td>
<td>192.168.1.1, 192.168.1.10, 192.168.1.12, 192.168.1.13, 192.168.1.18, 192.168.1.24, 192.168.1.28,</td>
<td>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.</td>
</tr>
<tr>
<td>Low</td>
<td>Host supports SMBv1 protocol</td>
<td>1</td>
<td>192.168.1.45</td>
<td>Disable support for SMBv1 on all Windows hosts in the network.</td>
</tr>
</tbody>
</table>

Click to expand vulnerability details

17 Total Achievements

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

23 Discovered Hosts

Click to see host details
CONSIDER COMPLYING WITH A NATIONALLY RECOGNIZED CYBERSECURITY FRAMEWORK

One popular framework that dealers can work toward is the Center for Internet Security (CIS) Critical Security Controls. Other popular frameworks include the International Standards Organization (ISO) 27001 and US National Institute of Standards and Technology (NIST). Some state laws, like the California, Ohio, Utah, Massachusetts, and Connecticut provide safe harbor or limited liability from data breaches if dealers comply with a nationally recognized cybersecurity framework like those released by the Center for Internet Security (CIS).

ComplyAuto is a CIS SecureSuite Member, which allows us to leverage CIS resources to help dealers perform advanced cybersecurity risk assessments and automated configuration scans of their operating systems, applications, and supported network devices.

<table>
<thead>
<tr>
<th>CONTROL</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Inventory and Control of Enterprise Assets</td>
<td>5.0, 4.5, 5.0</td>
</tr>
<tr>
<td>02</td>
<td>Inventory and Control of Software Assets</td>
<td>7.0, 6.7, 7.0</td>
</tr>
<tr>
<td>03</td>
<td>Data Protection</td>
<td>8.0, 7.8, 8.0</td>
</tr>
<tr>
<td>04</td>
<td>Secure Configuration of Enterprise Assets and Software</td>
<td>12.12, 11.12, 12.12</td>
</tr>
<tr>
<td>05</td>
<td>Account Management</td>
<td>6.6, 6.6, 6.6</td>
</tr>
<tr>
<td>06</td>
<td>Access Control Management</td>
<td>5.9, 7.8, 8.0</td>
</tr>
<tr>
<td>07</td>
<td>Continuous Vulnerability Management</td>
<td>7.7, 7.7, 7.7</td>
</tr>
<tr>
<td>08</td>
<td>Audit Log Management</td>
<td>12.12, 11.12, 12.12</td>
</tr>
<tr>
<td>09</td>
<td>Email and Web Browser Protections</td>
<td>2.7, 4.7, 7.7</td>
</tr>
<tr>
<td>10</td>
<td>Malware Defenses</td>
<td>7.7, 7.7, 7.7</td>
</tr>
<tr>
<td>11</td>
<td>Data Recovery</td>
<td>6.5, 6.5, 6.5</td>
</tr>
<tr>
<td>12</td>
<td>Network Infrastructure Management</td>
<td>1.9, 7.0, 8.0</td>
</tr>
<tr>
<td>13</td>
<td>Network Monitoring and Defense</td>
<td>11.0, 6.11, 11.11</td>
</tr>
<tr>
<td>14</td>
<td>Security Awareness and Skills Training</td>
<td>9.9, 9.9, 9.9</td>
</tr>
<tr>
<td>15</td>
<td>Service Provider Management</td>
<td>7.7, 4.7, 7.7</td>
</tr>
<tr>
<td>16</td>
<td>Applications Software Security</td>
<td>9.9, 9.9, 9.9</td>
</tr>
<tr>
<td>17</td>
<td>Incident Response Management</td>
<td>3.9, 9.9, 9.9</td>
</tr>
<tr>
<td>18</td>
<td>Penetration Testing</td>
<td>0.0, 3.5, 5.5</td>
</tr>
</tbody>
</table>

**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.
A study by Verizon showed that 90% of ransomware and cybersecurity incidents involve clicking on a link in a phishing email. Consider using a phishing simulation software to test employees’ security awareness and susceptibility to social engineering tactics. This normally involves sending out emails designed to look like real-life phishing emails, and then tracking which employees are willing to click on links within those emails or enter credentials on a fake landing page. “Phished” employees are then automatically enrolled in security awareness training. Internal phishing tests can be very effective at conditioning employees to scrutinize emails sent from people outside of your organization. The FTC noted in the regs that phishing simulations are an “important part” of penetration testing.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running your own phishing campaigns requires HTML coding, configuring email servers, etc.</td>
<td>ComplyAuto has hundreds of dealer-specific and other common phishing templates. We manage all the campaigns and setup for you at no additional cost.</td>
</tr>
<tr>
<td>Without owning dozens of domains, internal phishing emails become obvious and predictable.</td>
<td>We have hundreds of domains so that phishing emails never become obvious to the recipients.</td>
</tr>
<tr>
<td>No way to automatically enroll phished employees into dealer-centric security awareness training.</td>
<td>ComplyAuto has a system for automatically enrolling phished employees into a tailored security awareness course.</td>
</tr>
</tbody>
</table>

**PHISHING SIMULATIONS**

**APPLICABLE LAW OR REGULATION**

16 CFR §314.4(d)(1)(i)

The FTC has clarified that social engineering and phishing simulations are an important part of the new penetration testing requirements.
**Campaign Benchmarking**

- **Open Rate**: 1.22%
- **Click Rate**: 5.37%
- **Penetration Rate**: 4.31%

**Your Latest Test**

**Your Average**

**Other Dealers’ Average**

**Active Phishing Simulations**

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Start Date</th>
<th>End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoorDash - Free Cheesecake</td>
<td>2/13/2022</td>
<td>2/27/2022</td>
</tr>
<tr>
<td>United Airlines - Promotion</td>
<td>2/13/2022</td>
<td>2/27/2022</td>
</tr>
<tr>
<td>LinkedIn - Connection Request</td>
<td>2/13/2022</td>
<td>2/27/2022</td>
</tr>
<tr>
<td>UPS - Delivery Update</td>
<td>2/13/2022</td>
<td>2/27/2022</td>
</tr>
</tbody>
</table>

**Testing Effectiveness**

- **Performance Over Time**
- **Reduction Rate**

**Recent Actions**

- **Template**
- **Employee**
- **Action**
- **Date**

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Employee</th>
<th>Action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkedIn - Connection Request</td>
<td>Heber Barton</td>
<td>Replied</td>
<td>2/26/2022</td>
</tr>
<tr>
<td>DoorDash - Free Cheesecake</td>
<td>Neoma Thompson</td>
<td>Hacked</td>
<td>2/26/2022</td>
</tr>
<tr>
<td>LinkedIn - Connection Request</td>
<td>Miller Walter</td>
<td>Opened</td>
<td>2/26/2022</td>
</tr>
<tr>
<td>DoorDash - Free Cheesecake</td>
<td>Heber Barton</td>
<td>Opened</td>
<td>2/26/2022</td>
</tr>
<tr>
<td>LinkedIn - Connection Request</td>
<td>Cameron Leibsack</td>
<td>Hacked</td>
<td>2/25/2022</td>
</tr>
</tbody>
</table>

**Repeat Offenders**

<table>
<thead>
<tr>
<th>Employee Name</th>
<th># of Times Phished</th>
<th>Date Last Phished</th>
</tr>
</thead>
<tbody>
<tr>
<td>Berenice Satterfield</td>
<td>5</td>
<td>2/24/2022</td>
</tr>
<tr>
<td>Willow Douglas</td>
<td>5</td>
<td>2/24/2022</td>
</tr>
</tbody>
</table>

**Training Required**

- **Search**

Showing 1 to 5 of 24 entries
Some state laws regulate the deployment of third-party tracking cookies for retargeted advertising & provide consumers with other privacy rights, such as opt-out, deletion, access, and correction. 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 CA, VA, CO, or UT residents (including cookies and similar information) who shop or browse online. Collecting information on out-of-state residents (and the browsing of your website by those residents) is becoming increasingly common due to inventory shortages and the rise of digital retailing in the automotive industry. ComplyAuto ensures that you have a cookie banner that complies with all applicable state laws, regardless of the shopper's residency.

Some state laws require the honoring of Global Privacy Controls (GPCs) and “Do Not Track Signals”. ComplyAuto installs the necessary code on your website to honor these signals and comply with all applicable state laws in the process.

Plaintiff attorneys often file lawsuits relating to third-party tracking cookies deployed without their consent. Over the past few years, there has been a significant increase in the amount of lawsuits filed (including class actions) relating to cookies and online tracking. The basis of the lawsuit is usually a general “unfair business practice” or “violation of privacy” cause of action relating to the tracking and sharing of information without the consumer’s consent. Some creative plaintiffs have even alleged wiretapping!

State Attorneys General have taken enforcement action related to cookies and online tracking. Even states that do not have comprehensive privacy laws have seen Attorneys General take enforcement action against businesses for what they consider to be unfair and deceptive practices relating to the online tracking of consumers, often citing to the fact that consumer had no way to opt out of such tracking or that there were insufficient disclosures relating to why and how such tracking would occur. The Federal Trade Commission (FTC) has also announced that it intends to take similar enforcement actions. The ComplyAuto cookie banner and privacy policy disclosures accomplish this necessary level of transparency.
Cybersecurity Insurance

- Complying with the GLBA will also help you reduce your dealership’s cybersecurity insurance premiums
- Use a broker to shop the market
- Review the survey/questionnaire carefully and have it double-checked by professionals (vendors, IT Director, legal counsel, etc.)
- Don’t skip the “other” or “what else would you like us to know?” questions
- Set up a one-on-one meeting to show the insurance company what you’re doing to improve cybersecurity
- Have & show proof of compliance
- Implement multi-factor authentication (MFA)!