Three Birds, One Stone: Comply with the new FTC Safeguards Rule, Adopt a Cybersecurity Framework & Reduce Insurance Premiums

Presented on March 24, 2022

by Chris Cleveland

CEO & Co-Founder, ComplyAuto

www.complyauto.com

Comply with the new FTC Safeguards Rule Requirements

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

COMPLY 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).

CIS Center for Internet Security®

CIS Controls®

CONTROL 01 Inventory and Control of Enterprise Assets — 5 Safeguards — IG1 2/5 — IG2 4/5 — IG3 5/5	CONTROL 02 Inventory and Control of Software Assets — 7 Safeguards — IG1 3/7 — IG2 6/7 — IG3 7/7	CONTROL 03 Data Protection — 14 Safeguards — IG1 6/14 — IG2 12/14 — IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software — 12 Safeguards — IG1 7/12 — IG2 11/12 — IG3 12/12	CONTROL 05 Account Management — 6 Safeguards — IG1 4/6 — IG2 6/6 — IG3 6/6	CONTROL 06 Access Control Management — 8 Safeguards — IG1 5/8 — IG2 7/8 — IG3 8/8
CONTROL 07 Continuous Vulnerability Management — 7 Safeguards — IG1 4/7 — IG2 7/7 — IG3 7/7	CONTROL 08 Audit Log Management — 12 Safeguards — IG1 3/12 — IG2 11/12 — IG3 12/12	CONTROL 09 Email and Web Browser Protections — 7 Safeguards — IG1 2/7 — IG2 6/7 — IG3 7/7
CONTROL 10 Malware Defenses — 7 Safeguards — IG1 3/7 — IG2 7/7 — IG3 7/7	CONTROL 11 Data Recovery — 5 Safeguards — IG1 4/5 — IG2 5/5 — IG3 5/5	CONTROL 12 Network Infrastructure Management — 8 Safeguards — IG1 1/8 — IG2 7/8 — IG3 8/8
CONTROL 13 Network Monitoring and Defense — 11 Safeguards — IG1 0/11 — IG2 6/11 — IG3 11/11	CONTROL 14 Security Awareness and Skills Training — 9 Safeguards — IG1 8/9 — IG2 9/9 — IG3 9/9	CONTROL 15 Service Provider Management — 7 Safeguards — IG1 1/7 — IG2 4/7 — IG3 7/7
CONTROL 16 Applications Software Security — 14 Safeguards — IG1 0/14 — IG2 11/14 — IG3 14/14	CONTROL 17 Incident Response Management — 9 Safeguards — IG1 3/9 — IG2 8/9 — IG3 9/9	CONTROL 18 Penetration Testing — 5 Safeguards — IG1 0/5 — IG2 3/5 — IG3 5/5

Cybersecurity Insurance

How to reduce 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

If you don’t already have a cybersecurity insurance policy . . . get one. Data breaches are one of single biggest exposures a dealership has today.

HOT ISSUE WITH CYBER POLICIES: IMPLEMENT MFA FOR SYSTEMS WITH NPI

APPLICABLE LAW OR REGULATION

16 CFR § 314.4(c)(5)

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

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

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

- **Third-party Applications**. Start by enabling MFA for all of your online or cloud-based applications and software that store or access customer NPI (e.g., your CRM, DMS, and credit-related systems).Popular dealer systems like DealerTrack and RouteOne already have a way to enable MFA for all users.

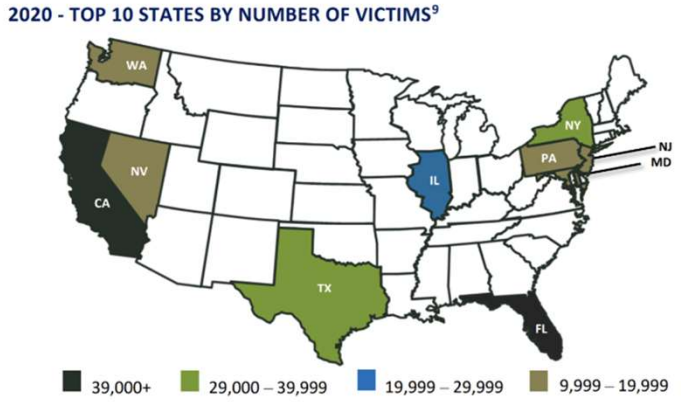
- **On-premises MFA**. If dealers are storing NPI on their own internal devices, networks, or servers (including an on-premises DMS), they should strongly consider enabling MFA on logins to the employees' workstations/operating systems.

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

Data Breach Implications

- **Network/system downtimes**. Prepare to start handwriting contracts and calling bank analysts.
- **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).

COMPLYAUTO PRIVACY

NADA AFFINITY PROVIDER njcar

*The only vendor trusted by both the **NADA** and **NJ CAR** for dealership privacy and cybersecurity compliance.*

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

CONTACT ME

chris@complyauto.com
https://www.complyauto.com
(385) 277-5882

About ComplyAuto

"By Dealers. For Dealers."

- 60+ years of combined dealership compliance experience
- ComplyAuto was created organically to solve problems faced by the owners at our own dealerships.
- In just the past year, over **1,000** dealers used the ComplyAuto software to achieve compliance with state and federal privacy and cybersecurity laws and reduce their insurance premiums.