

Data Security Breaches — A Dealership's Biggest Risk



Randy Henrick

Associate General Counsel

Dealertrack Inc.

Lake Success, NY

516.734.3644

Randy.Henrick@dealertrack.com



@Dealertrack
#NADA2016

The views and opinions presented in this educational program and any accompanying handout material are those of the speakers, and do not necessarily represent the views or opinions of NADA. The speakers are not NADA representatives, and their presence on the program is not a NADA endorsement or sponsorship of the speaker or the speaker's company, product, or services.

Nothing that is presented during this educational program is intended as legal advice, and this program may not address all federal, state, or local regulatory or other legal issues raised by the subject matter it addresses. The purpose of the program is to help dealers improve the effectiveness of their business practices. The information presented is also not intended to urge or suggest that dealers adopt any specific practices or policies for their dealerships, nor is it intended to encourage concerted action among competitors or any other action on the part of dealers that would in any manner fix or stabilize the price or any element of the price of any good or service.

Agenda

- Impact of a data breach
- What puts you most at risk for a data breach?
- Best practices for limiting your risk



The Impact of a Data Breach

- Data security breaches and associated costs are at an all-time high
 - 43% of U.S. organizations were breached in 2014*



Financial Implications

- Total costs estimated at \$201 per record compromised*
- 60% of small firms go out of business within six months of breach**
 - 3 out of 5 attacks target small business†



*Ponemon Institute

**Experian (2015)

†Symantec (2015)

What Causes a Data Breach?

- Brute force attacks on systems are no longer the norm
- Compromising user endpoints is easier for hackers
- Employees are biggest risk



What the Safeguards Rule Requires

- Protect data against
 - Unauthorized access
 - Hazards to security
 - Administrative, physical, and technical threats
- Confidentiality of customer information
- Compliance \neq secure



FTC Safeguards Enforcement

- FTC entered into over 53, 20-year safeguards consent decrees
- Safeguards shortcomings are unfair trade practices-violating Section 5 – FTC Act



Penalties for Violations and Recent Case Law

- Dealers incur state penalties plus cost of notifying consumers
- Plaintiffs finding ways to allege actual harm to bring class actions



What puts you most at risk?

- Storing/sending consumer information in readable text files
- Neglecting encryption
- Failing to address system attacks
- Failing to patch/upgrade systems



Data Safeguards Shortfalls

- Failing to
 - Keep firewall and anti-virus software current
 - Employ measures to detect unauthorized access
 - Regularly do system penetration tests
 - Train/monitor employees



Safeguarding Shortfalls

- Failing to
 - install Data Protection Software
 - change default passwords
- Neglecting to
 - review and monitor service providers
 - securely dispose of data



Safeguards Disparities

- Failing to
 - require complex system passwords and frequent password changes
 - implement, test, and update a security incident response program
 - update Safeguards Program



Best Practices for Limiting Risk

- Store customer information on a secure server
- Know system data flow
- Monitor user access to PII
- Monitor irregular patterns of activity



Recommendations to Help Eliminate Risks

- Disable
 - download of PII to external devices
 - local administrator privileges
 - download of unapproved software
- Limit points of entry into systems



Build an Incident Response Plan

- Plan is critical because time matters
- Designate individuals for tasks and retain experts
- Do mock tabletop drills and revise plan accordingly



Address the Human Element

- Train employees regularly
- Get a proxy server to prevent access to sites with malware
- Cut off terminated employees immediately



You've won a \$100 Amazon Gift Card to redeem instantly

From **Amazon** contact@primehealthbook.com **hide details**

To **wrhenrick** wrhenrick@aol.com

Protect your Dealership

- Limit permissions to customer data to specific job roles
- Employ procedures to detect unauthorized access and fake users



Protecting Dealerships in a Mobile World

- Create BYOD policy
- Use MDM software for all devices connected network
- Use “container” software for access to/from your system



Paper Files

- Appoint “gatekeeper” to control access files
- Audit data flows and monitor access to paper files the same as electronic files



Security Defense Practices for Dealers

- Use systems with audit trails
- Review unusual activity
- Inventory all employee devices



Protect Customer Information

- Don't leave customer data exposed
- Short PC screen time-outs
- Wipe hard-drives before discarding equipment



Make Access to Customer Data More Difficult

- Use two-factor authentication for any access
- Encrypt devices allowed to connect to your internal network
- Review anti-keylogging software



Security Measures for Dealers

- Get a static IP address; enable access only from that IP address
- Authentication for PII servers
- Limit access to “view only”



Safeguards Considerations for Dealers

- Update your program and **train, train, train**
- Consider **Cybersecurity Insurance**



How Do I Respond to a Security Incident?

- Deploy security incident response team
- Notify cyber-insurance company
- Consider:
 - monitoring logs to identify infected systems and devices
 - forensics person to examine systems



How Do I Respond to a Data Breach?

- Forensic images of systems
- Determine if the bad guys still have access
- Have email gateways been compromised?
- Contact local F.B.I. office



Data Breach Counter Measures

- Tell media that we are investigating—
DON'T SPECULATE
- Additional requirements if payment cards compromised
- Do a post-mortem





- Employees are your biggest risk
 - Hackers need to only compromise one person
- Monitor data access
- Do penetration tests
- Develop an incident response plan

Questions ?

Data Security Breaches — A Dealership's Biggest Risk



Randy Henrick

Associate General Counsel

Dealertrack Inc

Lake Success, NY

516.734.3644

Randy.Henrick@dealertrack..com



Please visit the **NADA Pavilion** in the Expo Hall for information on accessing electronic versions of this presentation and the accompanying handout materials, and to order the workshop video recording.

@Dealertrack
#NADA2016