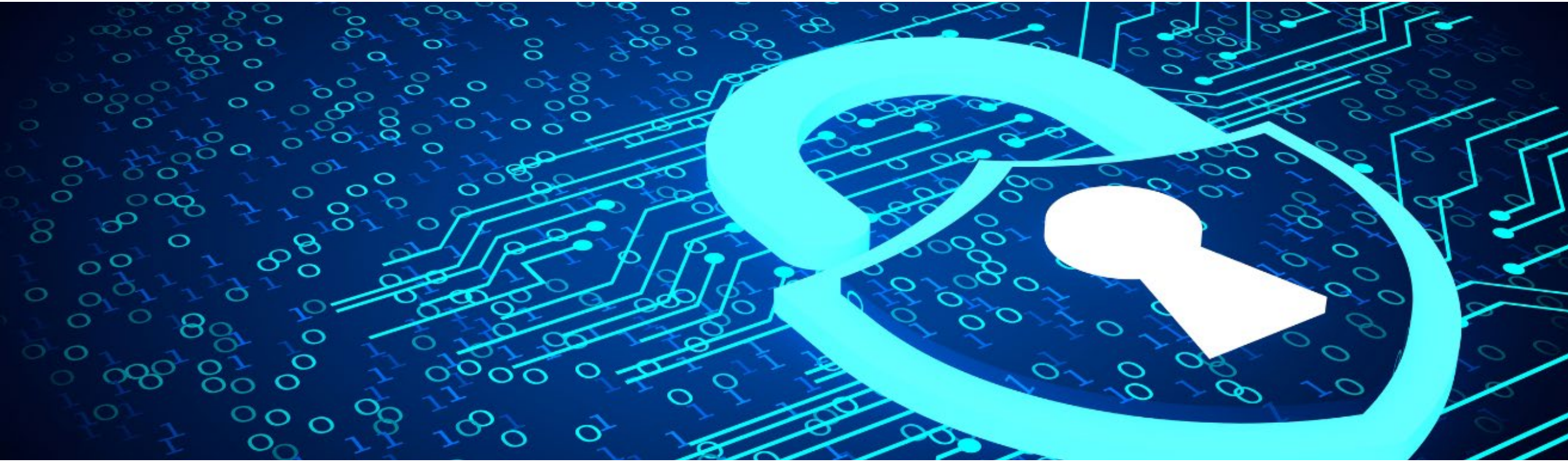


Cyber Threats and Legal Compliance for Today's Dealerships

Thursday, June 18, 2025

GNYADA Dealer Webinars are Sponsored by:

OPENLANE

Marilyn O'Brien
Market Sales Manager
Openlane

Direct 631-671-1888
Marilyn.O'Brien@openlane.com

GNYADA GOLF CHARITY

An Event to Benefit Individuals Pursuing AUTOMOTIVE EDUCATION

GNYADA Golf Outing & Pickleball Challenge

July 21, 2025

Old Westbury Golf & Country Club

SCAN TO LEARN MORE

NETWOLF
CYBER INTELLIGENCE ADVISERS

ArentFox Schiff

GNYADA
Greater New York Automobile Dealers Association

Data Security Rules of the Road:
Cyber Threats and Legal Compliance for Today's Dealerships

Peter Regina, CEO - Netwolf Cyber
Andrea M. Gumushian - ArentFox Schiff

Introductions

Peter Regina, CEO
Netwolf Cyber

Peter is a seasoned cybersecurity expert with a well-earned reputation for strategic thinking, technical acumen, and successful outcomes for his clients. In 2002 Peter founded Impact Technology Systems (now Netwolf Cyber LLC). His career, rooted in an early fascination with technology, reflects a relentless drive to stay ahead of emerging threats and deliver innovative IT solutions. His expertise in ethical hacking and cybersecurity enables proactive risk mitigation and efficient, recognized problem-solving when critical issues arise.

He can be reached at:
pregina@netwolfcyber.com

Andrea Gumushian
ArentFox Schiff

Andrea Andrea advises automotive clients facing complex legal and policy issues at the intersection of regulatory compliance, data privacy, and emerging technology. She is a member of the NADC and regularly helps automotive dealers implement privacy compliance programs and otherwise comply with U.S. privacy laws and regulations. Prior to joining private practice, Andrea spent two and a half years on the legal team of a leading SaaS provider to the automotive and insurance industries.

She can be reached at:
andrea.gumushian@afslaw.com

Netwolf Cyber - Services Overview

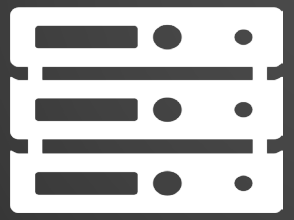
Managed IT Support & Services

Security & Information Protection

Managed VoIP

Public & Private Cloud Solutions

Hardware Procurement & Lifecycle Management



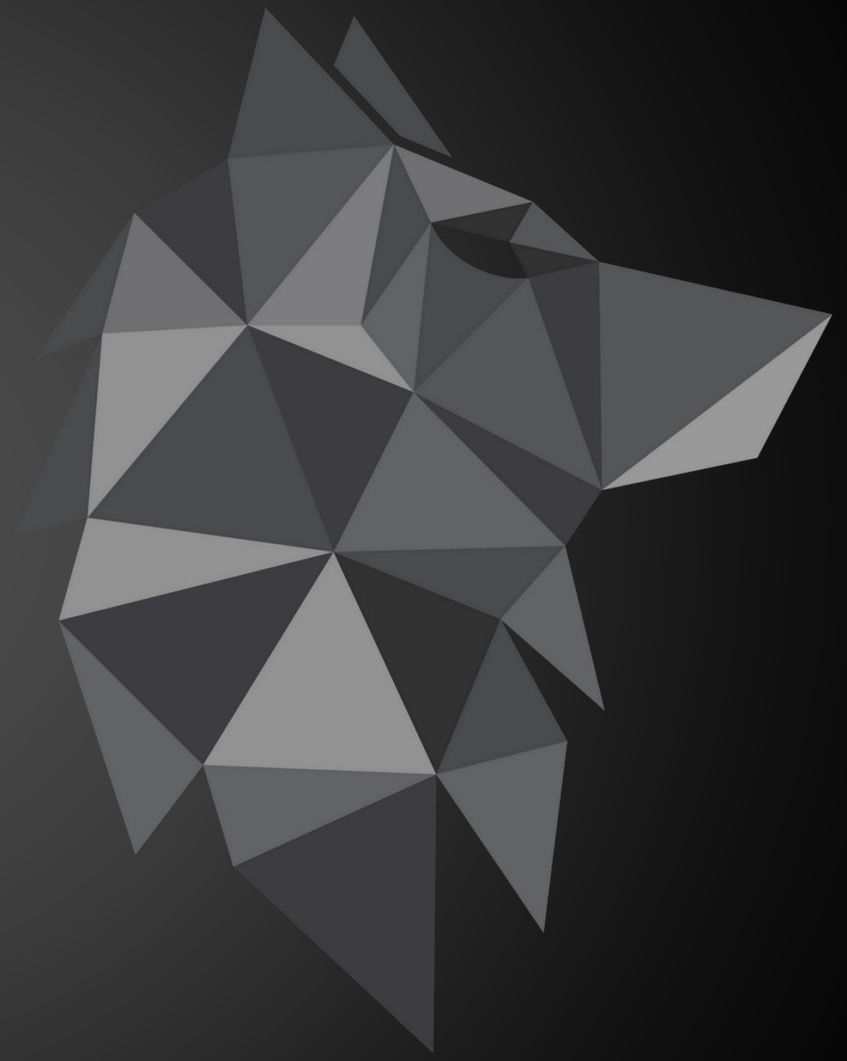
Infrastructure Design and Installation

IT & Cybersecurity Consulting

Managed Compliance

The Netwolf Team

- Network Engineers
- Workstation Support Technicians
- Cyber Security Experts
- VoIP Engineers
- Installation Technicians
- Private Cloud Engineers
- Software Developers



Agenda

Part 1 - Netwolf Cyber

- Cyber Risks
- Cyber Security

Part 2 - ArentFox Schiff

- Compliance
- Case Studies

Part 3

- Q&A

Part 1

Cyber Risks

Common Dealership Offenses

Based on Netwolf Risk Assessments on multiple car dealerships:

- Weak or No Access Control
- No MFA Integrations
- Unprotected Server Rooms
- No Network Asset Inventory
- Unmonitored Network Traffic
- Flawed Network Design

Dealership Risks - according to NADA

- Profitability & Inflation
- Inventory Levels
- Direct Sales
- Talent (Technicians)
- **Cybersecurity**
- System Downtime
- Reputational Damage
- Regulatory Compliance

Source: NADA Show Las Vegas

Is your dealership vulnerable?

Hackers assume most dealerships share these traits:

- Unsegmented WiFi
- Untrained Employees
- No IT Team Oversight
- Insecure Login Processes
- Improper Network Architecture

Source: Crowdstrike - A Guide for Auto Dealerships

What would a Data Breach cost your dealership?

Example:

- **Annual Dealership Group Revenue** - $100 million
- **Amount of Downtime** - 24 hours

Car Dealership's Cost of a Data Breach:

- **Revenue lost** = (revenue/365)*downtime
  - ($100,000,000/365) * 1 = **$273,973 per day**

<u>Excludes Legal Costs, Regulatory Fines, Future Revenue Loss, etc.</u>

Top Cyber Threats - According to CDK GLOBAL

1. **Email Phishing**
2. **Lack of Employee Awareness**
3. **Ransomware**
4. **PC Virus or Malware**
5. **Theft of Business Data**
6. **Stolen or Weak Passwords**
7. **Vehicle Cyberattacks**

90% of dealers say cybersecurity is very or extremely important relative to other aspects of operation.

Only **53%** of car dealers have confidence in their cybersecurity safeguards.

Source: CDK Global. "2023 State of Cybersecurity in Dealerships Study." CDK Global, https://www.cdkglobal.com/insights/2023-state-cybers dealership-study.

CDK Global Data Breach

Case Study

On June 19, 2024, CDK Global's **IT systems were compromised** in a ransomware attack, causing the **disruption of operations for 15,000 dealerships** that were left without access to their Dealer Management System (DMS).

Source: Anderson Economic Group. "Dealer Losses Due to CDK Cyberattack Reach $1.02 Billion." Anderson Economic Group, https://www.andersoneconomicgroup.com/dealer-losses-due-to-cdk-cyberattack-reach-1-02-billion/?highlight=cdk.

CDK Global Data Breach

Case Study

The ransomware attack on CDK led to total losses of **$1.02 billion**

- **Dealers lost 56,200 new vehicle sales**
- **Lost earnings on parts & service**
- **Cost of IT services and additional staffing**
- **Additional floor plan interest costs on inventory**

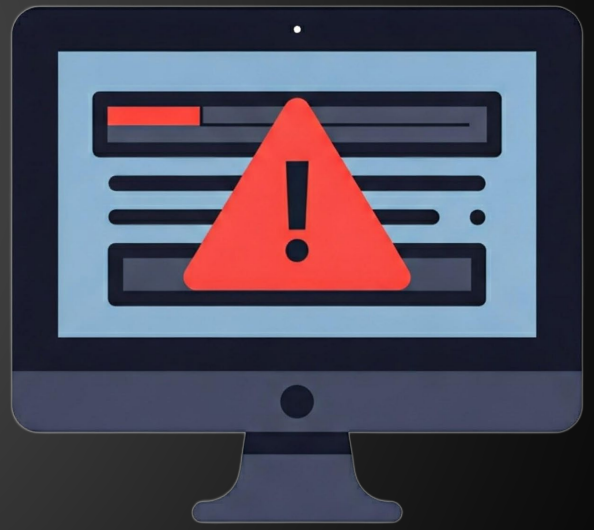
Source: Anderson Economic Group. "Dealer Losses Due to CDK Cyberattack Reach $1.02 Billion." Anderson Economic Group, https://www.andersoneconomicgroup.com/dealer-losses-due-to-cdk-cyberattack-reach-1-02-billion/?highlight=cdk.

CDK Global Data Breach

Case Study

The estimated $1.02 billion in damages **excludes**

- **Damages to consumers (stolen data)**
- **Reputational damages to dealers**
- **Litigation costs**
- **Ransom paid to hackers ($25 million)**



Source: Anderson Economic Group. "Dealer Losses Due to CDK Cyberattack Reach $1.02 Billion." Anderson Economic Group, https://www.andersoneconomicgroup.com/dealer-losses-due-to-cdk-cyberattack-reach-1-02-billion/?highlight=cdk.

Supply Chain Attacks

Every vendor, service, software, and hardware tool can potentially be hacked.

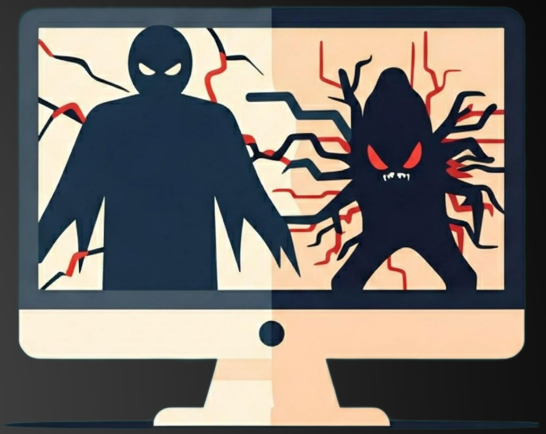
- **Rely solely on trusted entities**

Supply Chain Attacks like the CDK cyberattack demonstrate that **backup solutions are critical.**

- **You need an actionable backup plan**

Malware & Vulnerability Exploitation

Malware targets **system weaknesses** to **infiltrate**, **disrupt**, and **steal** data.

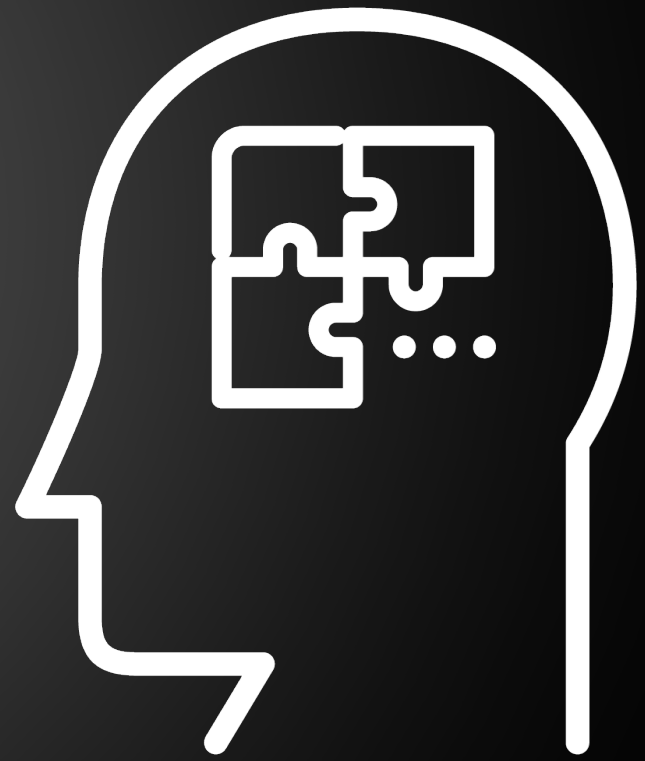


- **Ransomware** - encrypts data until victim pays for decryption key
- **Viruses** - attaches to clean files and spreads across computers
- **Spyware** - secretly monitors and gathers data from where it sits
- **Zero-Day Exploits** - leverages vulnerabilities unknown to developers

Social Engineering

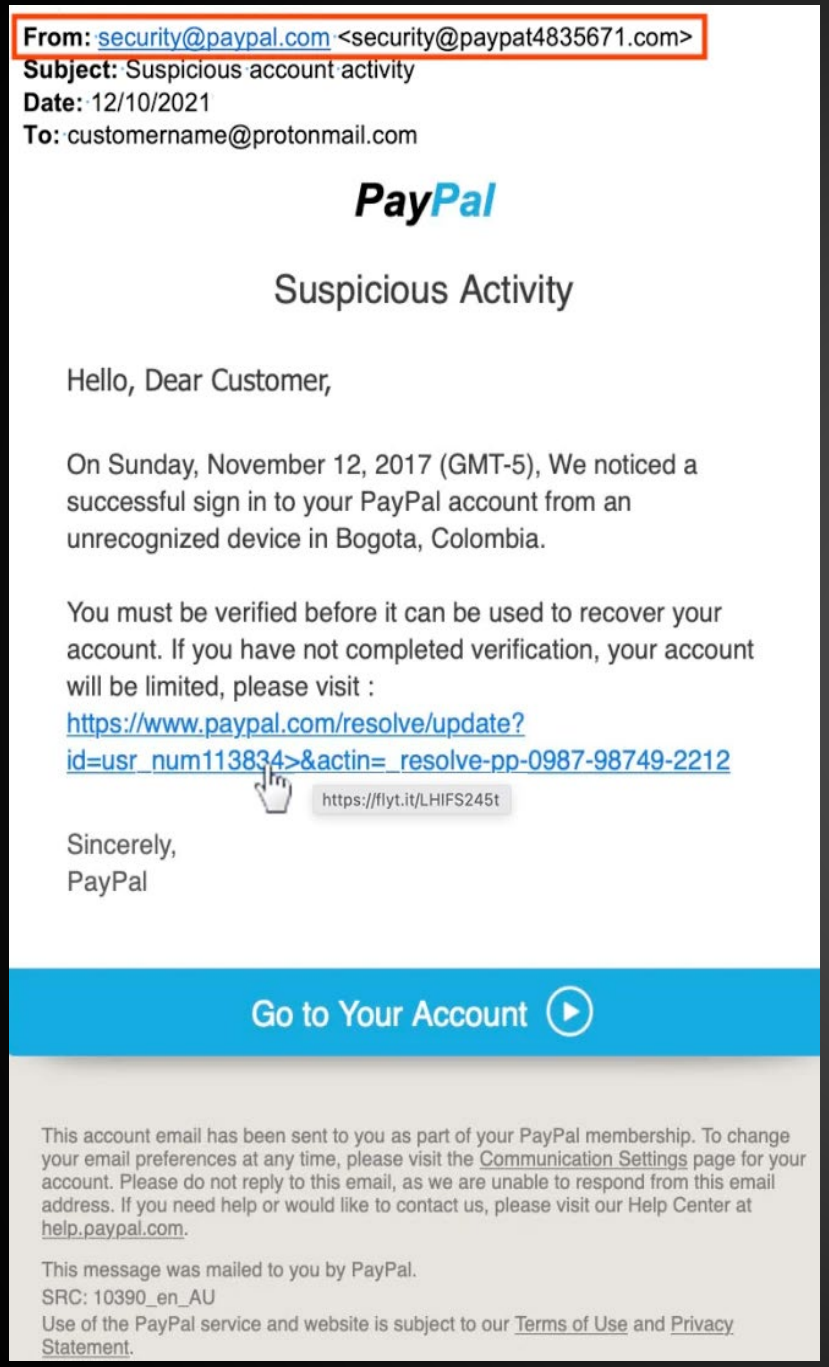
Threat actors use tactics to trick their victims into giving them what they want. Such methods of social engineering include:

- **Urgency**
- **Impersonation**
- **False Promises**
- **Deep Fakes**



Social engineering attacks take advantage of a victim's:

- **Emotions**
- **Psychology**
- **Behaviors**



Phishing

Hackers may impersonate a legitimate entity to try and **steal sensitive information** such as

- addresses
- credit card numbers
- banking information
- social security numbers

A phishing email could ask you to verify your account details with a **link** that takes you to an imposter login screen.

READ YOUR EMAILS CAREFULLY!

Cybersecurity

What does cybersecurity mean to you?

Common answers:

- Firewall
- Anti-Virus
- Two Factor Authentication

Cybersecurity is a shared responsibility.

Protecting your Network

Proactive Cybersecurity

Network Architecture

Remote Connectivity Solutions

Take a Proactive Approach to Security

Most owners & managers only begin to care about cybersecurity after they've been hacked...

Vulnerability Assessments

- Where are your dealership's weaknesses & blind spots?
- Can a hacker breach your dealership(s)?

Information Security Training

- Simulate breaches to test your execution of response plans

Continuous Network Monitoring

- Real-time surveillance and threat intelligence for incident detection and prevention

Network Architecture & Visibility

Network Segmentation

- Divide the network into isolated pieces to reduce potential attack surface

System Patching & Network Application Maintenance

- Routine auto maintenance prevents breakdowns, just as regular updates prevent system vulnerabilities

Zero Trust Security Model

- Implement policies so that no users or systems are automatically trusted

Zero Trust - Network Architecture

Implement Least Privilege Access

- **Only allow trusted & verified entities** to access to private systems
- Grant **minimal permissions to reduce attack surface**

Trust no one - everyone and everything is a potential threat

- **Insiders** such as salespeople, mechanics or admin staff **can cause harm to your IT systems**
  - Insider damage can be **intentional or unintentional**
- Network components including computers, servers, phones, software, etc. may be malicious

Segment your network to limit the possibility and severity of data breaches

- **Isolate systems** critical to dealership operations & **restrict hackers** from lateral movement

VPN (Virtual Private Networks)

Virtual

Private

Network

Remote Access Solution

- VPNs can **connect remote users** to networks to **access private resources & data from any location**
- Permits device connection **without security checks**

VPNs are highly vulnerable to cyber attacks

- **Hackers abuse legitimate VPN gateways** to access private resources by compromising credentials
- **Broad access** through VPN tunnels **can be exploited**

SASE (Secure Access Service Edge)

Secure

Access

Service

Edge

Next Generation Remote Access Solution

- SASE **checks device security posture** before they are allowed to connect to your private network
- Remote **users are restricted** to necessary resources

Why choose SASE over VPN?

- **SASE is more secure than traditional VPN**, using adaptive connections that are difficult to target
- SASE provides **dynamic identity-based controls**

VPN vs SASE: Selecting a Remote Access Solution

	VPN	SASE
Remote Network Connectivity	✅	✅
Security Posture Checks	❌	✅
Identity-Based Access	❌	✅
Adaptive Security	❌	✅
Cloud-Native Scalability	❌	✅
Context-Aware Connectivity	❌	✅

End User Security

Multi-Factor Authentication

Endpoint Protection

Patching

MFA (Multi-Factor Authentication)

MFA significantly reduces your chances of being breached even if your passwords are compromised.

MFA is required by cybersecurity frameworks such as the **GLBA Safeguards Rule, PCI DSS, and more.**

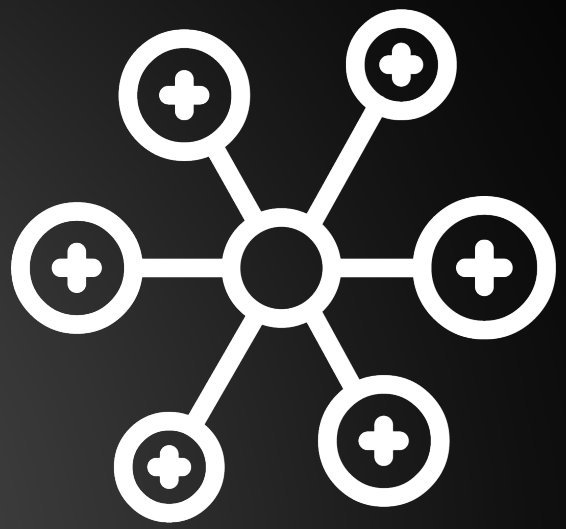
Usage of MFA in 2025 is a non-negotiable.

Accessing a network, device, or application with Multi-Factor Authentication requires:

1. **Something you know**
   - Password
2. **Something you have**
   - Authenticator
   - Biometrics (fingerprint, etc.)

Password **Verification** **Access**

Endpoint Protection



Anti-Virus & Anti-Malware

- Prevents malicious programs from harming devices
- **Outdated level of defense** - focuses on known threats

EDR *(Endpoint Detection & Response)*

- **Monitors behavior** of end users to detect suspicious patterns
- Focus on neutralizing complex, stealthy threats that evade traditional defenses

MDR *(Managed Detection & Response)*

- Combines the capabilities of EDR with management of technical experts
- 24/7 monitoring by network security specialists & advanced AI tools

Workstation Patching

Outdated Operating Systems

- Update devices & systems regularly
  - Legacy software may lack security updates & support

Web Browser Updates

- Defend against known exploits & improve functionality

Business Applications

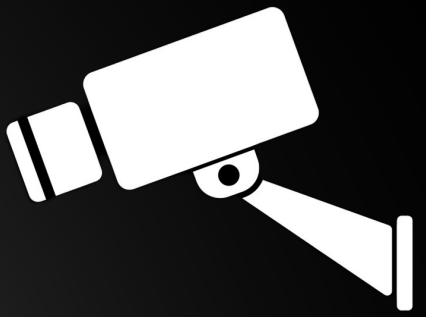
- Maintain patching of business-critical apps for optimal performance

Physical Security

Security Cameras

Hardware & Server Defense

Security Cameras



Use security cameras to protect your physical and digital assets.

- Keep a close eye on your IT infrastructure and showroom floor
- Monitor for unauthorized access of private info & other sensitive materials

Security cameras can be exploitable. Common vulnerabilities include:

- Weak or default credentials
- Lack of MFA
- Outdated software
- Accessibility via public internet connection

Hardware & Server Room Defense

Access Control

- Restrict access to sensitive resources
- Fortify entryway with secure locks
- Maintain visitor logs to track
  - Name, purpose, time, date, etc.

Surveillance

- Place cameras to see entire property
- Store recordings in a secure setting
- Monitor security footage using AI tools or human expertise

Data Backups

Backups, Backups, Backups!

- **Do you keep backups of your IT systems?**
- **What** parts of your IT systems are backed up?
- **Where** do you store your backups?
- **How many** backups do you keep?
- **How long** do you retain your backups for?
- **Have you tested your backups?**

Always follow the 3 - 2 - 1 Backup Rule!

- Maintain at least **THREE** backups in **TWO** locations, and **ONE** must be stored offsite

Cybersecurity is not a product, it is a process.

Please reach out with any questions, concerns, or if you are interested in comprehensive vulnerability assessments.

Visit netwolfcyber.com today!

Part II

Compliance

The New York State Data Breach Notification Law

A "breach of the security of the system" is defined as unauthorized access to or acquisition of computerized data that compromises the security, confidentiality, or integrity of private information. The law covers both acquisition and access (such as viewing) by unauthorized persons.

• **Who Must Be Notified**: Any New York resident whose private information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person must be notified.

• **Timing**: As of December 2024, notification must be made within 30 days of discovering the breach.

• **Method**: Notification can be provided by written notice, electronic notice (with consent), telephone, or, in certain cases, substitute notice (e.g., email, website posting, and statewide media).

• **Content**: Notices must include the business's contact information, a description of the categories of information involved, and contact information for relevant state and federal agencies that provide information on security breach response and identity theft prevention.

The New York State Data Breach Notification Law

A "breach of the security of the system" is defined as unauthorized access to or acquisition of computerized data that compromises the security, confidentiality, or integrity of private information. The law covers both acquisition and access (such as viewing) by unauthorized persons.

• **Who Must Be Notified**: In addition to notifying affected individuals, businesses must also notify:

The New York State Attorney General

The New York Department of State

The New York State Police

The New York Department of Financial Services (if the business is a covered entity under NYDFS regulations)

Providing notification is a non-trivial cost and a time-intensive exercise.

The New York SHIELD Act

Stop Hacks & Improve Electronic Data Security Act, also known as **SHIELD**, is a cybersecurity regulatory framework that **specifically protects residents of New York State.**

It requires car dealers to **implement reasonable safeguards** & **promptly notify affected individuals** in the event of a data breach involving New York residents' personal information.

Administrative, Technical & Physical Safeguard Requirements:

*Failure to maintain safeguards can lead to fines **up to $5,000 per violation**.*

- Identify & assess internal & external risks
- Train employees on security practices
- Monitor & test system controls
- Secure and dispose of data properly

Data Breach Notifications

*Failure to notify can lead to fines **up to $20 per missed notice**, with a cap at $250,000.*

- Notifications must be sent to affected customers as soon as reasonably possible.

Source: https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act

The Safeguards Rule

All financial institutions, such as **car dealerships**, must ensure the **security and confidentiality** of **customer data** according to the **Safeguards Rule** under **Gramm-Leach-Bliley Act (GLBA)**.

Car dealers must adopt strict protocols to comply with the Safeguards and other frameworks. The **FTC takes legal action against** businesses for **privacy and security offenses**.

Source: https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

The Safeguards Rule

Key Requirements:

- Appoint a **Qualified Person** to oversee your Security Program
- Conduct **Risk Assessments**
- Adopt a **Written Information Security Program (WISP)**
- **Implement Safeguards**
- **Test** your Security Program
- **Incident Response Plan**
- **Data Breach Notifications**

Source: https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Qualified Individual

Identify someone who will oversee the security program

- May be a partner or employee of your organization
- Ideally someone with enough skill and experience
- A 3rd party service provider can oversee your security program as long as they collaborate with a senior-level employee at your firm

Risk Assessment

1. **Where is your sensitive data stored?**

- **PII** (Personally Identifiable Information)
- **Client & Dealership Documents**
- **Financial Information**

2. **What risks threaten the security of your data and IT systems?**

- **Cyberattacks & Outages**
- **Physical Damage -** vandalism, natural disaster, etc.
- **Administration -** mishandling of data due to lack of training or experience

Your Risk Assessment MUST BE IN WRITING

WISP (Written Information Security Program)

Adopt a WISP based on your Risk Assessments

- Distribute the WISP too all members of your organization

WISP Contents

- Details procedures and policies for handling Personally Identifiable Info (PII)
- Accountability & Disclosure policies are covered
- Outline of technical safeguards for network security
  - Password & Multi-Factor Authentication Policies
  - Data Governance & Access Control Policies

Implement Safeguards:

1. **Access Controls** - restrict access to private data
2. **Data Inventory** - record systems, personnel, and PII locations
3. **Encrypt PII** (Personally Identifiable Information)
4. **Secure IT Systems** containing dealership data
5. **Adopt MFA** (Multi-Factor Authentication)
6. **Secure Data Disposal** - enforce offboarding procedures
7. **Maintain Logs** of activity & change management

Safeguard Testing and Reporting

1. **Test and monitor all safeguards and controls in place**
   - Includes logs of threats that were mitigated
   - Penetration testing & vulnerability assessment renewals
   - Make any necessary changes based on results

2. **Qualified Individual (or Service Provider) generates a written report to be shared with senior management**

Incident Response Plan

1. **Outline** response protocols & personnel - *Who are you going to call?*
2. **Identify the Incident**, outage, or attack & investigate the cause
3. **Classification** of incident severity - *low, medium, high, critical*
4. **Containment** - Act quickly and thoughtfully to isolate the problem
5. **Eradication** - Removing the problem from your system
6. **Recovery** - Restore your systems to normal operation
7. **Post-Incident Analysis** - How and why did this happen?

Data Breach Notification

Car dealerships must file a data breach notification after a cyberattack.

- Must notify the Federal Trade Commission (FTC) within 30 days

Penalties: Non-compliance fines, lawsuits, & reputational damage

Key Steps:

- Assess breach scope and impact.
- Notify regulatory bodies (e.g., FTC, state Attorney General).
- Inform affected customers promptly.

FTC Clarifies Data Breach Rules for Auto Dealers

Just this week, the FTC promulgated a FAQ, clarifying the financial data breach rules for auto dealers.

According to FTC guidance:

A sufficient information security program under the law should include safeguards including encryption, multi-factor authentication for access to records, and logging of network activity.

Ongoing obligation to safeguard data:

If a dealership arranges or brokers a loan it continues to be responsible for safeguarding personally identifiable financial information provided by the customer of financial information—even if they're no longer a customer.

FTC FAQ: *https://www.ftc.gov/system/files/ftc_gov/pdf/2025-GLB-Safeguards-FAQs-for-Auto-dealers.pdf*

FTC Clarifies Data Breach Rules for Auto Dealers

Just this week, the FTC promulgated a FAQ, clarifying the financial data breach rules for auto dealers.

What is "customer information":

Under the Safeguards Rule, a "consumer" is anyone who seeks a financial product or service from you that is primarily for their own personal, family, or household use.

• That includes anyone who applies to you for credit or who gives you nonpublic personal information so you can determine whether they qualify for financing – for example, to finance or lease an automobile.

• If you provide financing to or arrange financing for the consumer, then you are entering into a continuing relationship with the consumer. Once there is a "continuing relationship," the consumer becomes your "customer."

• Any non-public personally identifiable information the customer provided to obtain the financing is "customer information" that you have to protect under the FTC's Safeguards Rule.

Data minimization is key: only keep what you need.

Case Studies

Arnold Clark

Case Study

The **largest independent car dealer** in UK with 193 dealerships and 160 service centers was **forced to hand record transactions after IT systems were compromised** in a ransomware attack.

Arnold Clark initially stated that customer data was safe, but investigations discovered at least **475 GB of customer PII was leaked to the dark web.**

Over 10,000 individuals have joined KP Law to become potential claimants. The ICO is investigating to determine if Arnold Clark violated GDPR standards.

Source: Arnold Clark - About us, March 2024, ComputerWeekly.com - Arnold Clark data leak victims prepare legal action, June 2023
KP Law - Arnold Clark Data Breach Compensation

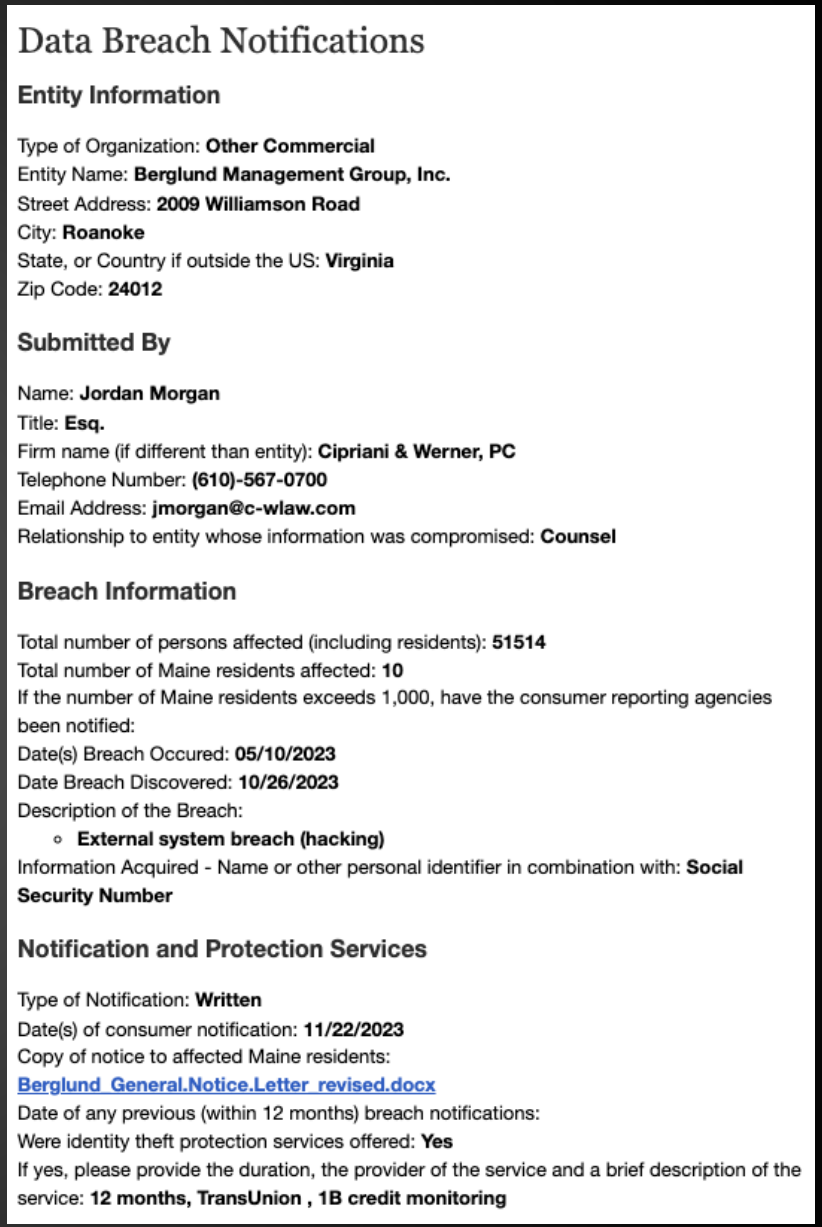
Source: Arnold Clark - X, December 2022

Berglund Management

Case Study

Breached: May 10, 2023
Detected: October 26, 2023
Reported: November 22, 2023

- Dealer of Toyota, BMW, Mercedes-Benz, Kia, and more brands across 20 locations
- Investigation revealed **unauthorized access** of **51,514** individuals' names and SSNs
- Berglund faces legal consequences, as multiple law firms investigate the breach and seek reparations for those affected.



Data Breach Notifications

Entity Information

Type of Organization: **Other Commercial**
Entity Name: **Berglund Management Group, Inc.**
Street Address: **2009 Williamson Road**
City: **Roanoke**
State, or Country if outside the US: **Virginia**
Zip Code: **24012**

Submitted By

Name: **Jordan Morgan**
Title: **Esq.**
Firm name (if different than entity): **Cipriani & Werner, PC**
Telephone Number: **(610)-567-0700**
Email Address: **jmorgan@c-wlaw.com**
Relationship to entity whose information was compromised: **Counsel**

Breach Information

Total number of persons affected (including residents): **51514**
Total number of Maine residents affected: **10**
If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified:
Date(s) Breach Occured: **05/10/2023**
Date Breach Discovered: **10/26/2023**
Description of the Breach:
- **External system breach (hacking)**

Information Acquired - Name or other personal identifier in combination with: **Social Security Number**

Notification and Protection Services

Type of Notification: **Written**
Date(s) of consumer notification: **11/22/2023**
Copy of notice to affected Maine residents:
Berglund_General.Notice.Letter_revised.docx
Date of any previous (within 12 months) breach notifications:
Were identity theft protection services offered: **Yes**
If yes, please provide the duration, the provider of the service and a brief description of the service: **12 months, TransUnion , 1B credit monitoring**

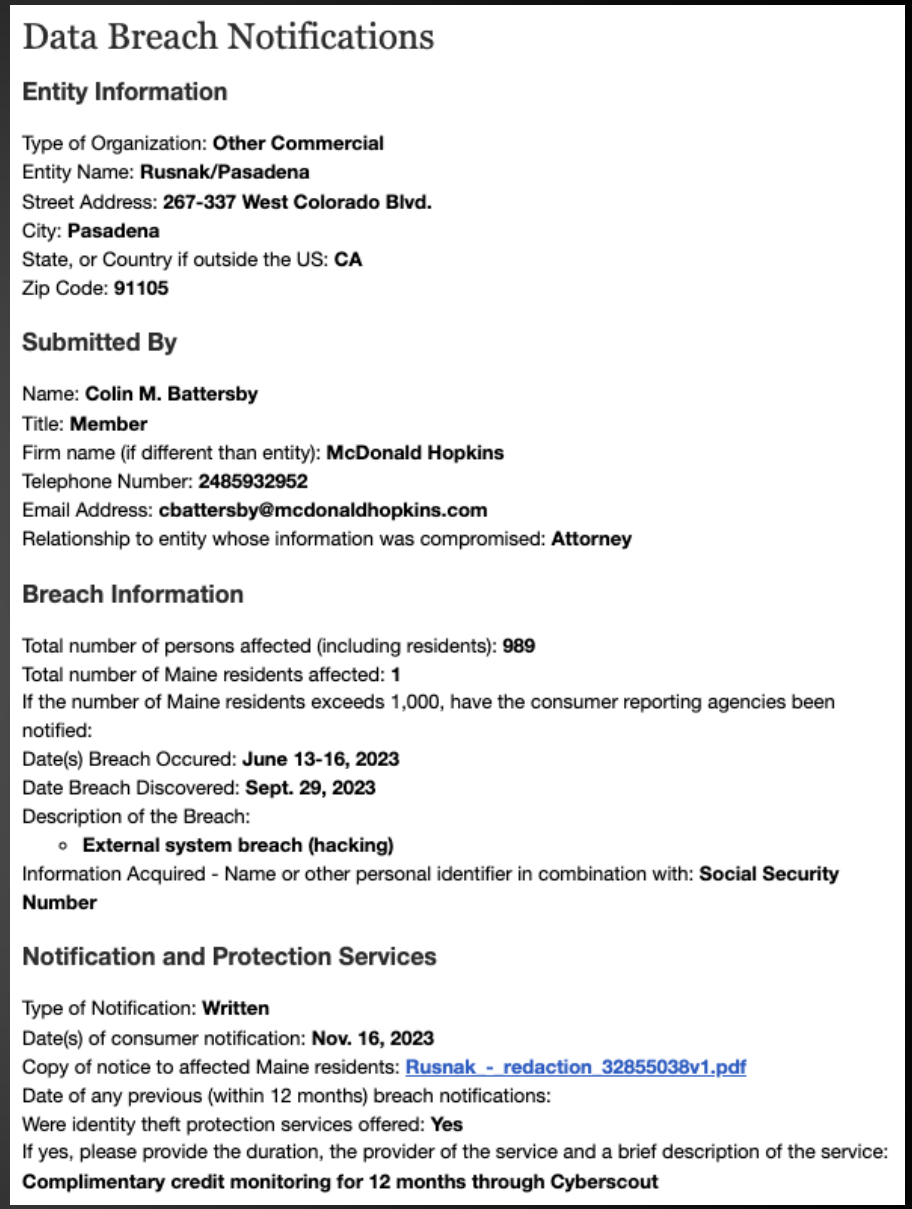
Source: Data Breach Notifications, Office of the Maine Attorney General

Rusnak Auto Group

Case Study

Breached: June 13-16, 2023
Detected: September 29, 2023
Reported: November 16, 2023

- ~800 employees across 18 locations selling 14 different luxury automobile brands
  - (Bentley, Rolls-Royce, Porsche, etc.)
- Unauthorized parties accessed consumer PII
  - (names, SSNs)
- Legal and reputational consequences; law firms investigating and representing victims



Data Breach Notifications

Entity Information

Type of Organization: **Other Commercial**
Entity Name: **Rusnak/Pasadena**
Street Address: **267-337 West Colorado Blvd.**
City: **Pasadena**
State, or Country if outside the US: **CA**
Zip Code: **91105**

Submitted By

Name: **Colin M. Battersby**
Title: **Member**
Firm name (if different than entity): **McDonald Hopkins**
Telephone Number: **2485932952**
Email Address: **cbattersby@mcdonaldhopkins.com**
Relationship to entity whose information was compromised: **Attorney**

Breach Information

Total number of persons affected (including residents): **989**
Total number of Maine residents affected: **1**
If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified:
Date(s) Breach Occured: **June 13-16, 2023**
Date Breach Discovered: **Sept. 29, 2023**
Description of the Breach:
- **External system breach (hacking)**

Information Acquired - Name or other personal identifier in combination with: **Social Security Number**

Notification and Protection Services

Type of Notification: **Written**
Date(s) of consumer notification: **Nov. 16, 2023**
Copy of notice to affected Maine residents: **Rusnak - redaction 32855038v1.pdf**
Date of any previous (within 12 months) breach notifications:
Were identity theft protection services offered: **Yes**
If yes, please provide the duration, the provider of the service and a brief description of the service:
Complimentary credit monitoring for 12 months through Cyberscout

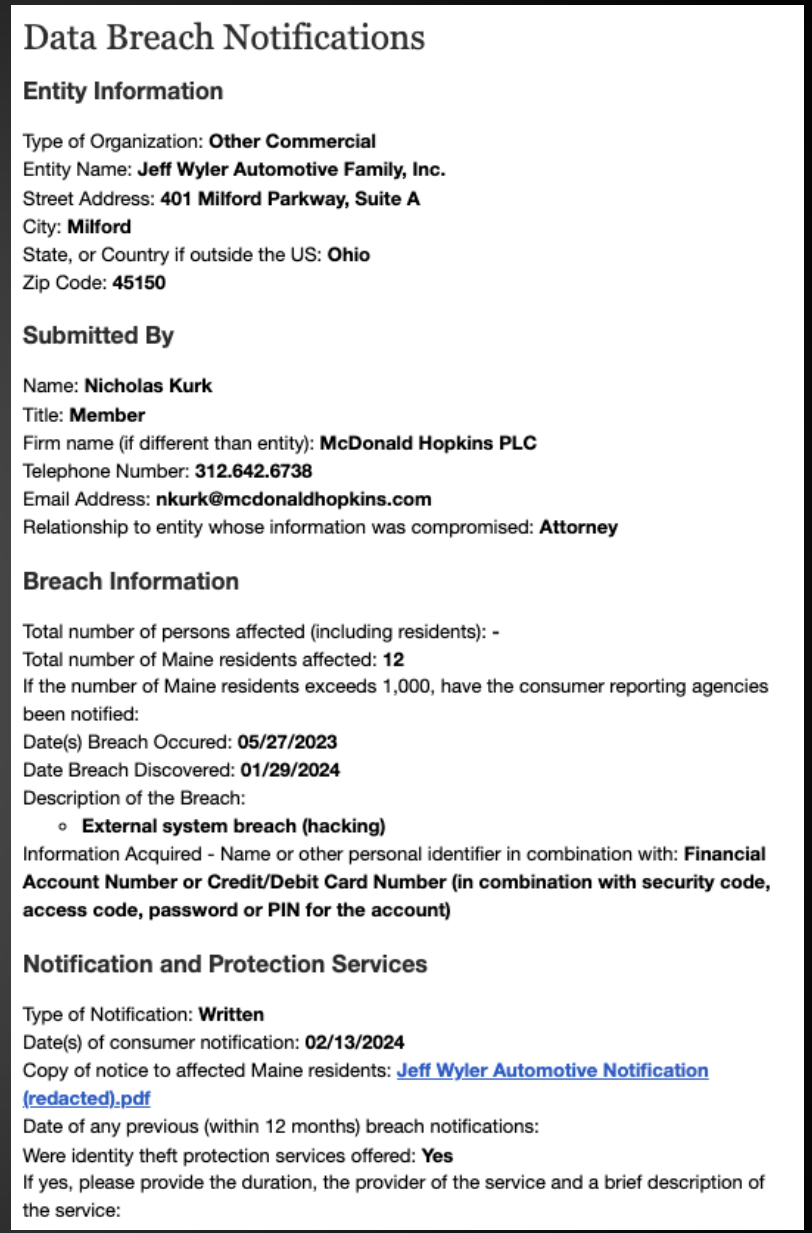
Source: Data Breach Notifications, Office of the Maine Attorney General

Jeff Wyler Automotive Family

Case Study

Breached: May 27, 2023
Detected: January 29, 2024
Reported: February 13, 2024

- Large private car dealership group with over 2,500 employees across 23 locations
- Network breach discovered on May 27, 2023, exposing consumer PII
  - (names, SSNs, financial account info, etc.)
- Legal consequences ensue; numerous law firms are investigating and representing affected victims in this ongoing case



Data Breach Notifications

Entity Information

Type of Organization: **Other Commercial**
Entity Name: **Jeff Wyler Automotive Family, Inc.**
Street Address: **401 Milford Parkway, Suite A**
City: **Milford**
State, or Country if outside the US: **Ohio**
Zip Code: **45150**

Submitted By

Name: **Nicholas Kurk**
Title: **Member**
Firm name (if different than entity): **McDonald Hopkins PLC**
Telephone Number: **312.642.6738**
Email Address: **nkurk@mcdonaldhopkins.com**
Relationship to entity whose information was compromised: **Attorney**

Breach Information

Total number of persons affected (including residents): **-**
Total number of Maine residents affected: **12**
If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified:
Date(s) Breach Occured: **05/27/2023**
Date Breach Discovered: **01/29/2024**
Description of the Breach:

- **External system breach (hacking)**

Information Acquired - Name or other personal identifier in combination with: **Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account)**

Notification and Protection Services

Type of Notification: **Written**
Date(s) of consumer notification: **02/13/2024**
Copy of notice to affected Maine residents: **Jeff Wyler Automotive Notification (redacted).pdf**
Date of any previous (within 12 months) breach notifications:
Were identity theft protection services offered: **Yes**
If yes, please provide the duration, the provider of the service and a brief description of the service:

Source: Data Breach Notifications, Office of the Maine Attorney General

Part III

Q&A

NETWOLF

CYBER INTELLIGENCE ADVISERS

ArentFox Schiff

NETWOLF

CYBER INTELLIGENCE ADVISERS

Fair Use Disclaimer: This presentation contains copyrighted material, the use of which has not always been specifically authorized by the copyright owner. Netwolf is making such material available in our effort to advance the understanding of issues related to cybersecurity. We believe this constitutes a “fair use” of any such copyrighted material as provided for in section 107 of the US Copyright Law. This material has been distributed without profit to those who have expressed a prior interest in receiving the included information for educational purposes.