NADC
National Association of Dealer Counsel®

DEFENDER

The National Association of Dealer Counsel Newsletter MAY 2019

Mendoza v. Lithia Motors, Inc.: Revisiting Dealer Retention and Disclosure Obligations

By Jeremy D. Sacks and Kennon Scott, *Stoel Rives LLP*


Sacks


Scott

An automobile dealer's retail installment sales contract ("RISC") is a heavily regulated piece of paper, and rightly so, because a car is one of the most significant investments made by a consumer. A large part of that regulation governs financing and the sale of additional services and products, a portion of which often is retained by the dealer to compensate it for arranging financing and reselling various products. There is nothing wrong with a dealer retaining a portion of the buyer's payment as long as that retention is adequately disclosed.

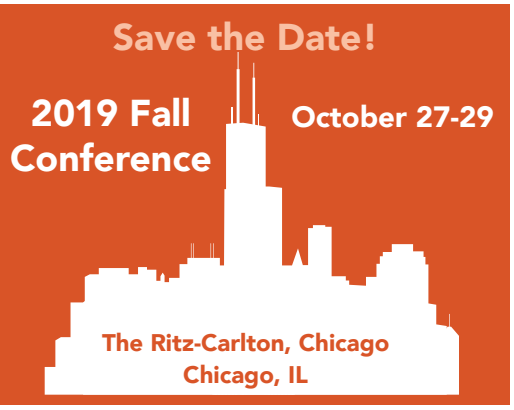
Although federal and state disclosure requirements are well settled, case law addressing these rules is often not precise, leaving room for enterprising lawyers to test the law. The game goes like this: a lawyer threatens a class action unless the dealer pays up to head off potential liability. That is exactly the position in which Lithia Motors, Inc., and a number of affiliated companies found themselves in *Mendoza v. Lithia Motors, Inc.*, Case No. 6:16-CV-01264-AA (D. Or.), a putative class action. After a series of motions to dismiss and a motion for summary judgment, the District of Oregon entered orders in favor of the defendants and produced critical opinions directly reinforcing key aspects of the disclosure regime upon which dealers nationwide can rely in the future.

The Plaintiffs' Claims

The representative plaintiffs, who purchased automobiles from dealerships that were affiliated with Lithia Motors, made a number of claims. The common theme among these claims is that the defendants were required to disclose the amount of profit they made from the sale of certain items. If plaintiffs were correct, then dealerships across the country would be subject to a disclosure requirement that applied to no other type of market transaction.

First, the plaintiffs alleged that the defendants failed to properly disclose under the federal Truth-in-Lending Act ("TILA") the existence and amount of compensation the dealership

In this Issue:



Contact Us:

NADC
1800 M Street, NW
Suite 400 South
Washington, DC 20036
Phone: 202-293-1454
Fax: 202-530-0659
info@dealercounsel.com
www.dealercounsel.com

received for arranging financing for a consumer. More specifically, they asserted that the dealership had an affirmative obligation under federal law to disclose the difference between: (1) the rate of the loan obtained by the dealership for the consumer at the consumer's request; and (2) the rate of the loan ultimately offered to the consumer by the dealership. The difference between those rates is known as the dealer reserve (or yield spread premium), and it is used to compensate the dealership for obtaining financing for the buyer. Additionally, in some instances, certain lenders offered a flat fee to a dealer instead of a dealer reserve. The plaintiffs asserted that the dealers' failure to disclose the existence or the amount of the dealer reserve or the flat fee violated the law, as did the dealerships' alleged failure to disclose the profit they earned on their sale of products supplied by third parties (such as GAP insurance, service contracts, lifetime oil, etc.).

Second, the representative plaintiffs alleged that Lithia's disclosure practices constituted common law fraud and violated various provisions of the Unfair Trade Practices Act ("UTPA") and its regulations, including the Oregon bird-dog rule. They again alleged that the dealers did not sufficiently disclose that they were retaining a portion of the purchase price of various third-party products.

The Defendants' Response

The plaintiffs' complaint had two problems: (1) it was wrong on the law; (2) and it was wrong on the facts. From the defendants' perspective, it was hard to see how the RISC and the related sales and disclosure documents could give rise to these claims, particularly because the RISC they used was very similar–and in some cases, identical–to the Oregon Automobile Dealers Association's form. In other words, if the defendants' RISC disclosures were problematic under state and federal law, then every dealer in Oregon using this form might have similar issues. There was no question that the stakes were high or that the defendants had little choice but to fight.

Moreover, both the TILA and the UTPA issues–particularly the bird-dog rule–seemed as if they were well-settled. This was especially true of the TILA claims, where courts in other jurisdictions had weighed in on similar claims and where the Federal Reserve itself offered clear guidance, Regulation Z, on what needed to be disclosed to consumers. The defendants thought they were following that guidance to the letter. The plaintiffs, however, rejected that defense and sought to create new law that would result in a significant new disclosure regime for the industry–and, not coincidentally, a huge damage award were a class to be certified in the case.

Many of the Oregon UTPA claims, too, challenged settled law, though some were so fact intensive that they would require fact development in order for them to be resolved at summary judgment. The bird-dog claim was one of those, because there was no Oregon case law explaining exactly what the bird-dog regulation meant. Automobile industry members know exactly what the bird-dog rule was designed to do–stop kickbacks over a certain amount from being paid for the referral of a potential consumer. However, Oregon's bird-dog regulation could be read by aggressive plaintiffs' lawyers to apply to *any* payment to a third-party, not just to payments for a customer referral. And, if the regulation applied to any third-party payment, arguably it applied to a host of third-party products sold by dealers across the state.

Resolution of the TILA Claims

The TILA cause of action was resolved against the plaintiffs on one of the defendants' motions to dismiss. The claim encompassed two courses of conduct–the arrangement of financing and the sale of third-party products.

The court quickly disposed of the third-party products issue. Not only did plaintiffs allege that the defendants failed to disclose that the dealerships retained certain amounts identified in the RISC as "amounts paid to others," but also that the defendants failed to itemize each amount that was paid to third parties by the creditor on the consumer's behalf–that is, the defendants did not break out how much profit they retained from the sale of the third-party products. In their briefing, the defendants pointed out that TILA did not require a dealership to disclose the amount of profit that it made but only that the dealer may be retaining some portion of the sales price. And that is exactly what the defendants' RISC stated. The court agreed. The following Reg Z passage was critical to the court: "For example, the creditor could add to the category 'amount paid to others' language such as 'we may be retaining a portion of this amount.'" Based on this plain language, and the many state and federal cases that considered the issue previously, the court declined the plaintiffs' demand to require disclosure under TILA of the exact amount retained. The court also found the defendants satisfied TILA's requirement with regard to the sale of third-party products, because the RISCs in question each contained the required disclosure. (They each provided, "*Seller may be retaining a portion of this amount.")

The plaintiffs made a similar argument with respect to the dealer reserve or flat fee, claiming that TILA required disclosure of that amount retained by the dealerships related to the arrangement of financing. The court again rejected the plaintiffs' attempt to add language to the statute. TILA and Reg Z require disclosure of the "finance charge" which is "the cost of consumer credit as a dollar amount. The "finance charge" includes any charge payable directly or indirectly by the consumer and imposed directly or indirectly by the creditor as incident to or a condition of the extension of credit." 12 C.F.R. § 226.4(a). In other words, the "finance charge" that must be disclosed is the *total* cost to the consumer, and the use of the term "any charge" in Reg Z recognizes the fact that the total charge may include components. TILA, however, does not require itemization of those components. In fact, the statute says that the finance charge disclosure is not itemized, 15 U.S.C. § 1638(a)(3), and courts have held uniformly that TILA does not require the lender to identify the components of the finance charge, including the existence of a dealer reserve. The court found that because the RISCs at issue disclosed the finance charge, they satisfied the TILA requirement. The court

dismissed this portion of the TILA claim, as well as the Oregon UTPA claims predicated on the alleged TILA violations.

Resolution of the UTPA Claims and Common Law Fraud

The court dispatched a series of UTPA claims on the defendants' motion to dismiss, all of which were based in whole or in part on the plaintiffs' allegations that the defendants did not disclose their profits or the fact that they would retain part of the price of third-party products. Among other things, these included claims for passing off services, causing confusion as to source of services, causing confusion as to affiliation or connection, making false or misleading representations of fact concerning price reductions, and making a false or misleading representation of fact concerning the offering price. Each of these claims failed at the pleading stage. As these statutes are specific to Oregon, we will not go into granular detail on each, but the court's reasoning was similar to that discussed above–the pleadings simply misread the language of the statute, and the defendants met their disclosure requirements.

One of the plaintiffs' UTPA arguments deserves some scrutiny. The RISC's itemized payment disclosure included the following headline language before listing each product individually: "Charges other than Finance Charge, including Amounts Paid to Others on My Behalf: (*Seller may be retaining a portion of this amount)." The plaintiffs asserted that this statement violated certain UTPA sections because, they argued, it insinuated that *all* amounts listed included sums paid to others (and not defendants or an affiliate) on the consumer's behalf and because the UTPA provisions at issue required disclosure of the exact amounts retained. The court rejected this argument: Nowhere did the UTPA require the amount of the profit to be disclosed, and the language at issue meant that the goods or services may be–but are not necessarily–purchased from a third party. Thus, for example, the fact that a lifetime oil product was sold by a defendant affiliate (which was fully disclosed in the RISC) did not support plaintiffs' various UTPA claims. Each entry for which a defendant dealership may have retained a portion of the fee was identified and was marked clearly with an asterisk, referencing the disclosure in the heading; that was all the defendants needed to do.

The plaintiffs supported their common law fraud argument with the same textual reading of the RISC. They argued that the language stated or implied that all service products were supplied by third parties, which was contrary to the facts, because a defendant affiliate supplied the lifetime oil product. The court again found that the headline disclosure said all that was necessary and that the RISC was not fraudulent: Although some amounts may be paid to third parties, the document did not falsely state that all amounts would be paid to third parties, and the defendants disclosed in the RISC exactly who

was being paid.

The court's handling of the bird-dog regulation under the UTPA is perhaps more important, because bird-dog rules exist in jurisdictions nationwide and some are not clearly written. Our research did not uncover any reported decision explaining how they function or why they exist.

The Oregon bird-dog regulation, issued pursuant to the state UTPA, is found at OAR 137-020-0020(3)(k), entitled "Undisclosed Fee Payments":

> [a] dealer who sells or leases a motor vehicle to a consumer and makes any payment to any non-employee third-party in conjunction with the sale or lease, other than a referral fee of $100 or less (also known as a "bird-dog" payment), must specifically itemize such payment on the consumer's purchase order, lease agreement and retail installment contract.

According to the plaintiffs, this rule required a dealer to itemize *every* payment made to a third party, other than a $100 referral fee. In other words, the plaintiffs alleged that the defendants serially violated the bird-dog rule when they did not itemize the fees paid to third-parties for the sale of their products.

The court rejected the plaintiffs' argument at summary judgment. It considered declarations from a witness who served on the advisory committee drafting the rule as well as the official commentary and other relevant documents. The witness was adamant that the rule was adopted to regulate only the disclosure of bird-dog fees. Moreover, the official commentary on its face addresses only payments for referral of a consumer to a dealership. The court further found that the plaintiffs' expansive reading of the regulation would "impose an expansive itemization requirement upon dealers," who "would be required to itemize a litany of payments on the customer's documents, thus volunteering the profits made on any third-party product associated with the sale. The dealer's personal cost of the very vehicle itself, being a third-party payment, would presumably fall under this expansive disclosure requirement." That sort of burdensome disclosure had never been discussed by the rule's drafters, was not addressed by the rule's text, and made no sense given the history of the regulation.

In the same order, the court dispatched two final claims. First, it rejected a UTPA argument under OAR 137-020-0020(3)(u), "Yield Spread Premium Disclosure." The plaintiffs asserted that the dealers did not clearly and conspicuously disclose that it may receive compensation for arranging financing. The court disagreed. It reviewed the entire deal packet for the sale at issue and found abundant evidence of significant, clear, and conspicuous disclosure of the required information. The court also cited the deposition transcript of the consumer, who agreed that the disclosure language in the documents disclosed what was required by law. Then, having dismissed all of the underlying claims in the case, the court rejected the elder financial abuse claim pursued by two senior citizen plaintiffs. Without a predicate UTPA violation, the claim for abuse could not stand.

Takeaways

Although the plaintiffs have signaled their intention to appeal the District Court's ruling, there are some key lessons that bear reviewing:

- TILA: The District of Oregon fully endorsed what was the common understanding of the disclosure requirements and it adopted the Reg Z commentary in full. These rulings can be used to bolster a TILA defense involving similar facts. TILA does not require disclosure of a dealer's profits.

- Bird-Dog Rule: With the District Court's summary judgment ruling, there is now a decision addressing exactly what the bird-dog rule was intended to cover. This development is critical, because prior to this case there was no decision with a clear discussion of the scope and intent of the bird-dog rule.

- The Litigation Process: It can take a long time. Be persistent and patient, read the statutes and regulations, and do your homework. Not all claims will be resolved on a motion to dismiss, and the court may grant leave to replead. Develop the record and do all you can to resolve the case prior to class certification. Be well prepared for depositions, and walk the putative class plaintiffs through all of the written disclosures; you never know what people will say.

- Facts Matter: Make certain your dealership clients have updated forms that make all the disclosures required under state and federal law. Also make certain the disclosures are clear and conspicuous (as defined in your jurisdiction). At the end of the day, the defendants prevailed in this matter at District Court because they cared about compliance and got ahead of any potential problem. You will do your clients a tremendous service if you help them do the same. ■

Jeremy D. Sacks is a partner in the Litigation Practice Group at Stoel Rives LLP in Portland, Oregon. His practice focuses on complex litigation on a region and national basis in a variety of businesses, including the automotive retail, energy, and health care industries. He has experience litigating business torts, contract disputes, securities fraud, False Claims Act issues, shareholder disputes, class actions, licensing disputes, and antitrust claims in a variety of private, state, and federal forums.

Kennon Scott is an associate in the Litigation Practice Group at Stoel Rives LLP in Portland, Oregon. Her practice focuses on complex business litigation, representing clients in a variety of industries, including industrial goods and consumer products manufacturers, automotive retailers, and health care providers. She has experience defending clients in government investigations and enforcement actions and litigating contract disputes, Fair Credit Reporting Act issues, securities and other class actions, and insurance coverage disputes.

Executive Director's Message

Erin H. Murphy
NADC Executive Director

Updated Member Contact Information

Please make sure to notify NADC Staff (info@dealercounsel.com) if your contact information has changed so that your records can be updated accordingly. We list updated contact information in *The Defender* so all members can be aware of the change.

I am pleased to report that our 15th Annual NADC Member Conference in Dana Point, CA, April 28-30, was yet another successful event! 226 NADC members attended the conference! I think everyone in attendance would agree that the Monarch Beach Resort was a beautiful property – even if we did get some rain in southern CA! The lovely setting could only be matched by the excellent program. Thanks to the Program Planning Committee for providing attendees with an outstanding, timely program.

The conference opened with the annual meeting of the membership during which the NADC membership elected four directors to their first term. Jim Appleton, New Jersey Coalition of Automotive Retailers, Inc.; Alisa Reinhardt, California New Car Dealers Association; Timothy Robinett, Manning, Leaver, Bruder & Berberich, LLP; and Kyle Sipples, Autosaver Group. The directors will serve a three year term.

The officers were then elected by the Board of Directors. Johnnie Brown of Pullin, Fowler, Flanagan, Brown & Poe, PLLC was elected President, replacing former President Andrew Weill of Weill & Mazer. Jami Farris of Parker Poe Adams & Bernstein LLP was elected Vice President. Scott Silverman of Prime Motor Group & Capstone Automotive Group was elected Treasurer and Eric Baker of Boardman & Clark LLP was elected Secretary. The officers will serve two year terms.

Andy Koblenz, Executive Vice President of Legal and Regulatory Affairs and General Counsel for NADA, and Paul Metrey, Vice President, Regulatory Affairs and Chief Regulatory Counsel, Financial Services, Privacy, and Tax for NADA kicked off the conference program by highlighting salient and breaking federal regulatory developments affecting auto dealers, including tariffs, the Military Lending Act, and the rollout of the optional NADA/AIADA/NAMAD Voluntary Protection Products Policy.

Next, Melinda Levy-Storms with The Niello Company, Shirly Wang with Davis Wang, PLC, and Rick Warren with Ford & Harrison LLP gave an hour long presentation on best practices for conducting a thorough and effective workplace investigation.

After lunch, Erika Ahern Curran with CNA National, Mark Barnes with Portfolio and Andy Weill with Weill & Mazer gave a hands on presentation for reviewing and negotiating F&I provider contracts. During Session four, retired FBI Special Agent John Iannarelli and Robert Shimberg with Hill Ward Henderson gave a humorous and eye opening presentation on how to handle a cyber attack at the dealership.

During the last session of the day, John Forehand with Kurkin Forehand Brandes LLP, Todd Milbury with NADA, and Joe Roesner with The Fontana Group addressed the need for a manufacturer to allocate new vehicles among its franchised dealers.

The second day of the conference opened with a presentation from Mike Charapp with Charapp & Weiss LLP and Eric Chase with Bressler, Amery & Ross on several of the top legal issues for dealers in 2019, and how dealers may act proactively in response to them. Always a popular session!

Following that session, Joe Aboyoun with Aboyoun Dobbs LLC gave a presentation on several special considerations in buy/sell negotiations and drafting, the contingencies, tax considerations, the ROFR and other automotive-sensitive issues.

Terry O'Loughlin and Timothy Yalich with Reynolds & Reynolds and Edward Somers with Buckley LLP next presented on how electronic document law is effectuated through technology.

The last session of the conference was a presentation by Anthony Bento with the California New Car Dealers Association, Michael Cypers with Glaser Weil LLP, and Andrew Stearns with Robards & Stearns, PC on manufacturer-offered new vehicle subscription programs. One hour was clearly not long enough for this session as attendees had many thoughts and questions. A great way to end the conference!

On Sunday afternoon, NADC offered an introductory level course for attorneys who are new to practicing auto dealer law or attorneys who wanted a refresher on dealership operations. This course was led by Deborah Dorman with ENYCAR, Shari Patish with Hall Automotive LLC, Stuart Rosenthal and Melinda Levy-Storms with The Niello Company.

On Monday morning, a tax breakfast session was offered to NADC members interested in learning more about the key aspects of tax reform, what dealers should focus on and what they should be doing to maximize their benefits. Stephen Bedell with Crowe LLP led this session.

On Tuesday morning, a breakfast session was offered to in-house counsel members and other NADC members interested in cutting edge litigation strategies. Johnnie Brown with Pullin, Fowler, Flanagan,

Brown & Poe, PLLC, Evan Nahmias with City Enterprises, LLC, and Harold Oehler with Lazydays RV shared battle-tested and state-of-the-art strategies on how to resolve claims at a fraction of the cost.

Thank you to all of the speakers who presented at the conference. I encourage all of you not in attendance to visit www.dealercounsel.com and benefit from the conference materials that have been uploaded. Please look under "Discussions & Publications" then "Documents & Discussions" and filter by "Conference Presentations."

I would like to thank all of our event sponsors for their contributions to the Annual Conference. These sponsors help to elevate the quality of the event while keeping the cost low for our members. Many thanks to:

The Fontana Group, Inc.
Bank of America Merrill Lynch
Moss Adams LLP
Dave Cantin Group
Rosenfield & Co.
Capital Automotive Real Estate Services, Inc.
Crowe LLP
Dealer Risk Services
GW Marketing Services
Haig Partners LLC
CNA National
PORTFOLIO
Anderson Economic Group
HBK CPAs & Consultants
CounselorLibrary.com/Hudson Cook, LLP
DHG Dealerships
MD Johnson, Inc.
Kerrigan Advisors

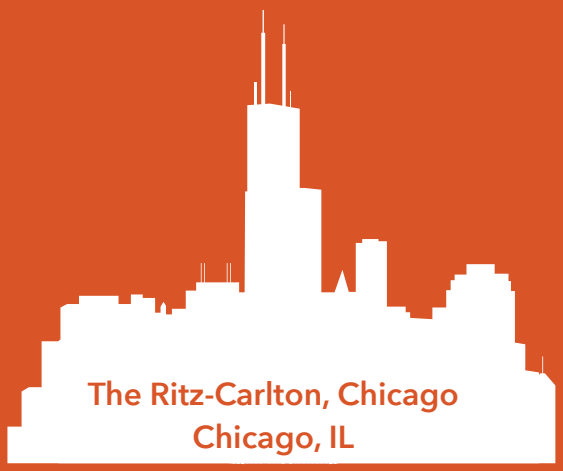
Be sure to Save the Date for the 2019 Fall Conference! The Conference will be held October 27-29 at The Ritz-Carlton, Chicago. All NADC educational programs rely on members' suggestions for topics and speakers. If you have a suggested session and/or topic you think should be covered at Fall Conference please email me at emurphy@dealercounsel.com. ■

NADC Welcomes New Members

Fellow Member:

David Stork
Lithia Motors, Inc.
Medford, OR

2019 NADC Fall Conference October 27-29, 2019



HOTEL RESERVATIONS
The NADC room rate at the Ritz-Carlton, Chicago is $295.00 per night plus applicable taxes. Reservations can be made here. You may also call the hotel's reservations line at 1-800-542-8680. Please reference the NADC Fall Conference to get our special rate.

All reservation requests will require a credit card and a deposit for one (1) room night. Deposits will be refunded for rooms cancelled more than seventy-two (72) hours prior to arrival.

Last day to officially book is Friday, October 4, 2019 (if the hotel room block does not sell out earlier)!

Are you interested in presenting at the NADC 2019 Fall Conference?

The Conference will be held October 27-29 at the The Ritz-Carlton, Chicago in Chicago, IL. If you have an interesting and timely program idea, please submit the following to emurphy@dealercounsel.com by Friday, June 21, 2019:

- Session Topic
- Outline and/or short description of session
- Names and bios of presenters
- Requested length of time

The Program Planning Committee will review all proposals. Proposals not chosen for the Conference will be considered for future webinars, articles and/or the 2020 Annual Member Conference.

Please contact Erin Murphy at: emurphy@dealercounsel.com with any questions.

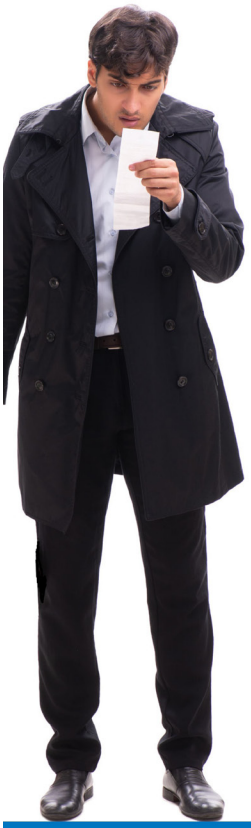
The Leading Sell-Side Advisor to Auto Dealers Nationwide

"We are very grateful for the guidance and support that the Kerrigan Advisors team provided us in the sale process."

Steve Bloomer
President and CEO of
Village Automotive Group

In the past five years, Kerrigan Advisors has sold 79 dealerships, including five of the Top 100 Dealership Groups, more than any other firm in the industry. Kerrigan Advisor's customized sale process is confidential, effective and proven. **If you would like to learn more about Kerrigan Advisors, contact Erin Kerrigan or Ryan Kerrigan at (949) 202-2200 or visit KerriganAdvisors.com.**

KERRIGAN ADVISORS



SALES SLOWING DOWN?

WE CAN HELP

With over 20 years in the Automotive Industry, we are more than your average accounting firm.

ROSENFIELD & Co. PLLC
TRADITIONAL VALUES | EXTRAORDINARY RESULTS

1-888-556-1154
WWW.ROSENFIELDANDCO.COM
TAX | ATTEST | CONSULTING

PORTFOLIO REINSURANCE

My Rights. My Portfolio.

As the national leader in dealer reinsurance programs, only Portfolio offers automotive dealers all the rights of ownership, and the maximum profitability that true ownership generates.

Exclusive for NADC Members

To better help you serve your dealer clients, we can provide an unbiased analysis of their current or prospective reinsurance program.
We will produce a comprehensive evaluation covering risk, profit, cash flow, exit strategies and taxes based on our 29 years in the business.

Contact Mark Barnes, Senior VP
949.789.6200

Portfolio
It's Your Portfolio.™

2018 DEALERS' CHOICE AWARDS

Is Your Dealership Prepared for a Cyberattack?

By Erik Nachbahr, *President and Founder, Helion Technologies*

Cybersecurity is an issue that is becoming increasingly important for automotive dealers. Today we are seeing dealerships being attacked on a regular basis. If you believe that your dealership is unlikely to be targeted by cybercriminals, think again. Dealerships make ideal targets for cybercriminals because they tend to keep a lot of cash in their bank accounts, conduct a lot of electronic financial transactions, and have large computer networks with minimal security. According to Total Dealer Compliance, only 30 percent of dealers employ a network engineer with computer security certifications and training, and 70 percent of dealers are not up to date on their anti-virus software.

Although no-one knows exactly how many auto dealerships have experienced a security incident, 75 percent of small and mid-sized businesses in the U.S. have experienced some type of breach, according to Osterman Research. I expect the percentage is the same among automotive dealers.

A common perception I run into with dealers is that they believe cybersecurity is a technology issue that can be handed off to the IT guy to address. This is a big mistake. At its core, cybersecurity is a business issue that deserves the highest priority from dealer principals and senior management. the dealer's money, customer data, and brand reputation are all at risk.

Being a cybercriminal is very lucrative, so the probability that a dealership will experience a cyberattack increases every year. In fact, it is really not a matter of if, but when, a cyberattack will happen. To properly defend against such an attack, it helps to understand what you are dealing with.

What Is a Security Breach?

I have received many calls from dealers in which the first thing they say is, "We've been hacked!" When I ask what happened, the dealer explains a scenario that was not, in fact, caused by hacking. I think many people get their ideas of what hacking is from the movies. They believe a hacker is a lone wolf closeted in a dark room or a kid living in his parents' basement, literally hacking his way into your system through a hole in your firewall.

In reality, most cybercriminals are employed by large, multi-national organizations. The job is very lucrative with experienced cybercriminals earning up to $2 million per year. Even an entry-level hacker can earn $42,000 annually.[1] These organizations and their smart employees spend their time thinking of ways to access a dealership's money and/or data. They use sophisticated schemes such as phishing, spear phishing, CEO fraud, malware, and ransomware to compromise the dealer's network. Even seemingly innocuous activities such as web surfing or clicking on social media posts can lead your employees to malicious websites designed to capture login information.

Additionally, dealers cannot ignore the potential threat from insiders with malicious intent. The high rate of employee turnover at dealerships means that a dealership could hire a person who installs malware on the server who is long gone before the resulting incident is detected.

Cybercriminals are motivated by one thing: money. In dealerships, this means they primarily go after:

Customer data. This information includes personal and sensitive information such as social security numbers, addresses, names, credit card numbers, copies of driver's licenses, bank account numbers, and credit reports. The criminals sell this information or use it to file false tax returns, order credit cards, and/or siphon money out of bank accounts.

Cash. Cybercriminals are surprisingly adept at tricking employees to wire money out of a company's bank account and into theirs. This has happened in several dealerships I know. Once it was discovered that the wire requests were fraudulent, the money was gone with no way to get it back. Another way cybercriminals make money is with ransomware, holding computer files and data hostage until they are paid a ransom with cryptocurrency.

If successful, a cyberattack results in a security breach. A dealership can have a strong firewall, anti-virus software and all the recommended technologies in place. None of it will protect against these threats, because cybercriminals rely on humans—dealership employees—as the weak link to grant them access.

Dire Consequences

The consequences of a security breach are not always devastating, but they can be. Ransomware requests are typically small, ranging from hundreds to several thousand dollars.

If an employee falls victim to a wire transfer scam, a business's damages are limited to the amount that you wired. One successful scam resulted in a dealership losing a total of $60,000 in two separate $30,000 transfers. In another scam that involved a salesperson, a dealership lost $251,000.

In some respects, these dealers are the lucky ones. For example, if a dealer's customers' sensitive data is compromised, costs escalate rapidly--roughly $30 per record. If a dealership has 100,000 customers in its database, it could be on the hook for $3 million.

Why so much? First, the dealership is legally required to inform its

customers about the breach. Depending on the state, the dealership might also be required to pay for credit monitoring for two years, to insure the customers are not adversely affected.[2]

Additional costs potentially include FBI and forensic investigations (for which the dealership is required to pay), mandatory security audits, consumer lawsuits, and FTC action for non-compliance with the Gramm-Leach-Bliley Act and software copyright laws.

Besides monies lost, the dealership will likely suffer damage to its brand's reputation and customer trust. Nearly 84 percent of consumers claimed they would not buy another car from a dealership if their data had been compromised, according to Total Dealer Compliance.

Common Tactics Used by Cybercriminals

Devious minds have invented numerous ways to circumvent firewalls and security software, most of them involving your employees. These are the most common tactics we have seen used in dealerships:

Phishing

Ninety-one percent of successful data breaches start with a phishing attack. Like a fisherman casting a wide net, a cyber thief creates an email and sends it out to a large group of people. The email is designed to look like it is coming from a well-known institution, such as a bank or retailer's (Target or Amazon). The email might purport to alert the recipient to a problem with his account, ask for verification, and encourage him to click on a link. The link connects to an official-looking website where the recipient is asked to login. His login information is captured and the thief immediately goes to the real website and uses his login information to gain access.

More sophisticated phishing emails might appear to be from a vendor or customer requesting additional information. One variant lures victims into revealing their credentials for file-sharing services, such as Microsoft OneDrive or Dropbox.

Recently cybercriminals have broadened how phishing links are delivered. In addition to emails, phishing links are now embedded into digital ads, social media postings, and browser extensions. These links are all designed to lead unsuspecting individuals to malicious websites where login credentials can be captured.

Spear phishing/ whaling/ CEO fraud

These are highly sophisticated attacks that often involve months of extensive research on individuals and companies. In one instance, a controller at a Toyota dealership received an email from someone who he thought was the principal. The controller and "principal" exchanged a couple of emails before the principal asked the controller to transfer $30,000 to a bank account in Florida. A few days later the controller received another request from the dealer. Once again, he transferred $30,000. Shortly after, the controller had a few questions and called the dealer. It was only then they both realized they had been scammed. By the time they found out, the money was long gone.

Impersonating a high-level executive in an email is pretty brazen, but these attacks are becoming more common.

Ransomware

Phishing links are often used to install computer viruses or malware. Ransomware is a form of malware that wreaks havoc on thousands of businesses every year.

Imagine getting an email from one of a suppliers that says "Invoice attached." The email addresses the recipient by name and includes a friendly little message from the known account rep at a supplier. The recipient trusts the sender, so she clicks on the email attachment, resulting in the ransomware being downloaded onto her computer. From there it spreads into the dealership's computer network. The danger in ransomware is that it lies dormant for a period of weeks or even months. Back-ups of data performed during this period of dormancy will also back-up the ransomware. Once the ransomware goes "live," recent back-ups will also be encrypted, so it is impossible to restore files from recent back-ups. In order to decrypt the files, the cyber thieves demand a ransom.

At this point the dealer has two choices: lose years' worth of files and data or pay the ransom. The majority of cyber thieves demand the ransom in bitcoins, a form of currency that is untraceable.

Keylogger

Keylogger, which tracks every keystroke on the user's keyboard, is another type of malware installed via the same tactics as ransomware. One dealership I know suffered serious financial consequences from a Keylogger attack launched from Facebook. The F&I manager was browsing Facebook and was somehow tricked into downloading a file. The file installed Keylogger on his keyboard.

That day the F&I manager logged into the dealership's credit bureau and the criminals captured the login credentials. Later that night they pulled credit reports on over 200 customers. Fortunately, the credit bureau identified the suspicious activity and stopped the credit pulls.

The aftermath was painful. An FBI investigation ensued, and the

dealership was forced to hire security experts to conduct a security audit. In the end the dealership paid out more than $150,000 in remediation. That is one expensive Facebook session!

Securing Your Dealership: Technology Solutions

As business owners, dealers have a legal and ethical responsibility to protect their customers' data. For dealerships today, a multi-layered technology approach is required to keep customer information safe. This includes:

Anti-virus software. As long as it is kept updated, a good anti-virus software will detect and block many unwanted email threats. After an extensive review process, the brand we recommend—and use—is Webroot. It is a light product, which means that even if PCs are three to four years old it will not weigh them down.

Firewall. The problem with most industry standard firewall products is that they do not update in real-time. The brand we use is Cisco Meraki. It is state-of-the-art and, because it updates in real-time, it is more likely to detect and stop a threat as it is happening.

Spam filter/spam firewall. This software is specifically designed to detect and block email threats and it's pretty effective at doing its job. The brand we use is Barracuda and it blocks about 95 percent of emails to our clients, which tells you how much bad email is out there.

Intrusion prevention systems. These systems monitor network traffic. When a threat is detected the system takes immediate action to block all traffic from the offending IP address or port.

Web-filtering software. This monitors employee activity online and prevents them from accessing dangerous websites. Many cyberattacks come in the form of emails that contain links encouraging employees to click through to a malicious website.

Centralized administration. Many dealerships do not have a centralized administrative set-up, which is really unfortunate. An important security best practice is to restrict employees from being able to perform administrative functions on their PCs, such as installing and removing software.

Securing Your Dealership: Processes and Employees

The weakest link in any organization is its employees. Cybercriminals rely on humans to make mistakes, and unfortunately, they often do. That is why it is important to implement these best practices:

Patching/software updates. The huge Equifax breach occurred because of a simple failure to install a software update/patch. I cannot emphasize enough how important this is to do on a regular basis for all of Microsoft/desktop applications, email applications, Internet browsers, and web-based applications.

Employee passwords. Passwords to all systems should be changed every ninety days, and for goodness sake do not allow employees to display passwords on Post-it Notes stuck to their computers.

Verbally confirm all wire transfers. Several controllers at dealerships have been fooled into wiring thousands of dollars to a bank, where the money subsequently disappeared. In all instances the controller

received email instructions from the dealer principal, but the emails were actually sent from an imposter. The only surefire way to prevent this is to verbally confirm all wire transfers.

Security awareness training. Most dealership employees are not adequately trained how to deal with issues like phishing, spear phishing, social media, and web surfing. In a test we conducted for a dealership, we sent 120 employees an email that appeared to be coming from the dealer principal. The email said, "Congratulations! You qualify for an employee bonus. Click on the link to sign in, and you can see what your share of the bonus will be." Half of the employees opened the email, eight people clicked on the link, and three employees entered their user names and passwords when prompted. If this email was sent by cybercriminals, they would have had immediate access to this dealership's network. All employees should receive ongoing training, so they know how to spot and report phishing emails and are kept up to date with the latest security threats. The good news is security awareness training is inexpensive and, over time, reduces the risk of a successful phishing attack from 27 percent to 2 percent.

Logging records. In the event of a breach, investigators will ask for logging records for all devices including PCs, servers, firewalls, and mobile devices. It is important to keep records so the source of the attack can be identified.

IT security audit. Have this done at least once a year. Hire an outside firm with security specialists. They are trained to spot network vulnerabilities that an every-day IT person may not know about.

Cyber liability insurance. Costs incurred by a security breach can easily run into hundreds of thousands of dollars, if not millions. Losses due to a data breach are not covered by property or casualty insurance policies, Directors and Officers Liability policies, or business umbrella policies. Losses for damaged equipment, such as PCs, laptops, and other "hardware" are covered by most property policies, but again, the data stored in them is not. Cyber liability insurance is something that every dealership should absolutely have, but many do not. Remember that insurance is a cost you only hate paying until the day you need it.

FTC Safeguards Rule: Are You in Compliance?

Under the Gramm-Leach-Bliley Act, dealerships classified as financial institutions are required to safeguard their customers' sensitive data. Dealers must also comply with the FTC Safeguards rule, which requires the same institutions to develop a written information security plan and to provide security awareness training to employees. Many dealerships are currently not in compliance with the Safeguards Rule.

Dealers should also create a cyber incident response plan. This does not have to be complicated–one-sheet may be sufficient, with phone numbers for the dealership's point of contact, its attorney, and its cyber liability insurance company.

What if Your Dealership Is Breached?

No matter how proactive a dealer is about having the right technologies and procedures in place, an attack can still happen. In most cases a breach is not discovered for several weeks. More often, the dealership is notified by a third-party, such as a bank or credit union with Positive Pay, a fraud detection tool. In the case of ransomware or other type of attack that brings down the network, the incident will happen suddenly, with no warning.

The first thing a dealership needs to do is pull out its cyber incident response plan and call its attorney and its cyber liability insurance company. The appropriate response will be determined in large part by the type of attack. he cyber liability insurance company will connect the dealer with a breach response team that will coach the dealer through the steps, which may include:

Notifying authorities. Contact the local police department as well as the local FBI field office and report the incident to the Bureau's Internet Crime Complaint Center. This step is not legally required, but it can be helpful as the authorities may have gathered evidence from similar attacks and have information that will be useful.

Notifying customers and stakeholders. If customers' data has been compromised, the dealer is legally required to inform them immediately. In some states, the dealer may also legally be required to pay for a credit monitoring service for affected customers. The dealer may also have to file a notice with the state general attorney's office. The dealer should wait to notify its employees and stakeholders until the same time it notifies its customers. this helps prevent employees or others from leaking the information, which could create a public relations nightmare.

Crisis communications. There is no point in trying to hide a cyberattack. If discovered later, one of the first questions that everyone asks is, "How long have you known?" It is best to be transparent to both the local press and the customers.

Forensic investigation. Depending on the nature of the attack, the dealer may also be required to hire a team of forensic experts to investigate how the attack happened. Ideally, the dealer will have at least a month's worth of replay security logs, so that investigators can learn the following:

- which IP address was used to gain access to the network;
- the type of viruses installed and which computers were infected; and
- whether hackers cleared the logs to eliminate traces of their fingerprints.

Sometimes a forensics team will require that the dealer suspend business for a period of days or weeks while they investigate an attack. The dealer should have a contingency plan that details how it can still operate, service, and communicate with customers, if possible.

Dealerships are a prime target for cyber thieves so it is critical to be prepared. Know what the potential threats are, implement technology and procedures to prevent them, and have a plan for if and when it happens. ■

Citations

[1] Tara Seals, *Cybercriminals Earn Millions, and Spend It Wildly,* Infosecurity, Apr. 13, 2018, https://www.infosecurity-magazine.com/news/cybercriminals-earn-millions/.

[2] Federal Trade Commission, Data Breach Response: A Guide for Business, May 2019, https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf.

Erik Nachbahr is the founder and president of Helion Technologies. Erik is a Certified Information Systems Security Professional (CISSP) with more than two decades of experience working with dealers to secure their data and optimize their IT environments. Today, Helion is the largest IT service provider focusing on the needs of dealers.

NADC Member Announcements

Do you have an announcement or accomplishment that you would like to share with the NADC community? Please send any news that you would like to share to: emurphy@dealercounsel.com.

2019 DEFENDER Advertising Opportunities

☐ ½ page ad $150.00
5" high x 7.5" wide, no bleeds

☐ ¼ page ad $100.00
5" high 3.75" wide, no bleeds

Months:
- ☐ June 2019
- ☐ July/August 2019
- ☐ September 2019
- ☐ October 2019
- ☐ November/December 2019

Contact:
Erin Murphy
emurphy@dealercounsel.com

NADC
1800 M Street, NW
Suite 400 South
Washington, DC 20036
Phone: 202-293-1454
Fax: 202-530-0659

BE A CONTRIBUTOR!

We are always looking for submissions to publish in the Defender. Please send your contributions or proposals for articles to: jamifarris@parkerpoe.com

NADC
NATIONAL ASSOCIATION OF DEALER COUNSEL®

Volume XV, Number 5
MAY 2019

Jami Farris, Editor
jamifarris@parkerpoe.com

Michael Charapp, Assistant Editor
mike.charapp@cwattorneys.com

Defender, The NADC Newsletter is published by the National Association of Dealer Counsel
1800 M Street, NW, Suite 400 South, Washington, DC 20036
Phone: 202-293-1454 • Fax: 202-530-0659 • www.dealercounsel.com