BANK OF AMERICA

Cyber Security in the Auto Industry

A dealer’s guide to stopping threats

LEADERSHIP TEAM

Marisa Carnevale-Henderson
Market Executive
Dealer Financial Services
Bank of America
marisa.carnevale-henderson@bofa.com

Jim Cockey
Market Executive
Dealer Financial Services
Bank of America
james.d.cockey@bofa.com

Derek Comestro
Market Executive
Dealer Financial Services
Bank of America
derek.comestro@bofa.com

Brian Gruber
Market Manager
Dealer Financial Services
Bank of America
brian.gruber@bofa.com

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

Defending your dealership against cyber criminals

As you focus on the many challenges of today's environment, cyber criminals are counting on businesses to let down their guards. Dealers can be uniquely susceptible to cyber threats for many reasons, including the significant amounts of customer data you store, and your high-value transactions. That's why protecting your dealership and financial data from theft should be a top priority.

Criminals have developed viruses and spam emails aimed specifically at dealership computer networks. And while new schemes can quickly emerge, some of the most effective intrusions still rely on techniques, such as business email compromise, which resulted in nearly $2 billion in losses last year.

What are some important steps you can take today to limit your exposure? With more people working remotely, securing your computers and networks is often a good place to start. In addition, equipping your employees with the skills to detect phishing attempts can help turn them into a source of strength instead of unwitting accomplices.

With diligence, commitment and a smart approach, you can help defend against cyber criminals and keep moving your business forward. We hope this guide provides a useful framework, and we welcome the opportunity to speak with you about this crucial topic.

Why cyber criminals are a big deal for dealerships

Automobile dealerships are vulnerable to cyber crimes, particularly in certain areas of their business, and the risks today are higher than ever. On an average day, for instance, 153 viruses and 84 malicious spam emails are aimed at dealership computer networks — and are blocked by technology.[1]

Why are dealerships a target, and what makes them susceptible to a cyber event? Why should dealership owners and managers take action? Consider these facts, issues and concerns:

Customer data and high-value transactions can make dealers a magnet for cyber threats

Dealerships possess a significant amount of customer data. Auto dealerships collect, process and store a vast amount of customer information in their databases and management systems. Purchase agreements, credit reports, finance contracts and credit applications include Social Security numbers, bank account information and credit card numbers — information particularly coveted by criminals.

Dealerships conduct high-value transactions. Because individual dealership transactions involve high dollar amounts, they are also big targets for criminals. A lot of money moves into and out of stores, and stealing one transaction can mean a large payout for a criminal. The Federal Trade Commission said more than 38,000 cases of identity theft connected to auto loans and leases were reported in 2019, more than double the previous year. PointPredictive, an auto finance company that tracks fraud, says business email compromise incidents are of particular growing concern to luxury dealerships.

Dealerships too often are using outdated technology, with IT staff not professionally trained to recognize and handle cyber events. Only 30% of dealers employ a network engineer with computer security certifications or training, and more than 70% lacked up-to-date antivirus software.[2] Dealers need to view IT and IT security as an investment, not an expense.

Dealerships often allow vendors broad access to their systems. Vendor incidents have become a key cyber security concern and are on the rise globally. Some dealership groups report that as many as 20 vendors have access to their computer network or internal data management systems. Each vendor with access multiplies the opportunities for a criminal to gain access to a dealership's information.

Dealerships are exposed not only through obvious devices like computers, phones and tablets but also through other machines and devices connected to the Internet—the so-called Internet of Things. IoT objects are typically simple devices or sensors that wirelessly connect to a network to perform certain limited tasks or functions. At a typical dealership building, that list might include connected devices like heating, ventilating and air-conditioning systems; sensors; cameras; fax machines; and video monitors. Each internet connection is a possible entry point for a criminal.

Dealerships must comply with new data privacy laws — such as the California Consumer Privacy Act and similar pending legislation—that demand tougher standards in managing and protecting consumer data.

Dealerships encounter high costs if they do suffer a data breach. Penalties for violations and incidents are expensive, amounting to tens of thousands of dollars for both the California Consumer Privacy Act and the Gramm-Leach-Bliley Act. Consider that when a customer's data is stolen from a company database, that company is responsible for paying for credit monitoring for the exposed customer. Then multiply that cost by the number of customers in the database. In addition, a victimized dealership often must deal with the cost of replacing compromised computers.

Dealerships, like other businesses, face a growing threat from ransomware attempts. Helion Technologies calls ransomware the second-greatest cyber security issue for dealerships. Ransomware installed on a dealership computer system can not only shut down business but also require rebuilding the computer network, costing some dealerships hundreds of thousands of dollars.

Dealerships risk one of their most valuable assets — long-term customer relationships — if they do suffer a data breach. Loss of reputation is an unfortunate byproduct of cyber crime. Nearly 84% of consumers said they would not buy another car from a dealership after their data had been compromised.[3]

84%

Share of consumers who wouldn't buy again from a dealer who's been breached

Dealerships are increasingly exposed as their employees do more business on mobile phones, laptops and tablets. As is the case in other industries, mobile devices and remote connectivity are becoming essentials at dealerships. With the rise in digital retailing and communications, staff members are using mobile devices more often to communicate with each other, customers and vendors. That means important and sensitive information or documents today may be transmitted via text message or email on a phone, laptop or tablet and potentially intercepted by a criminal.

As digital retailing grows, dealerships face new potential threats. The use of digital tools has opened up new sales and marketing possibilities but also has created new security risks. For instance, dealerships have increased their use of videoconferencing during the pandemic, opening the possibility for criminals to eavesdrop on conversations and gather sensitive information.

Dealerships, like all businesses, are exposed to new security challenges when employees work from home. The coronavirus and stay-at-home orders issued by many states and municipalities have turned the spotlight on working at home. Although unavoidable, that creates new cyber security challenges. Employees may use different devices and tools in these makeshift home offices—and may not know how to use them safely. Dealership and personal data can be exposed through employee phones and home internet service providers that might not have the same safeguards in place.

The dangers of phishing

Being held for "ransom" after malicious software is installed on the company computer system. Stolen customer data. An employee inadvertently transferring money to a fake vendor account. The impact of cyber crime presents a serious, expensive and growing threat to all businesses. Dealerships, with expensive inventory and valuable customer data, are a prime target.

Company-related cyber fraud often begins with a type of phishing called business email compromise. Financial losses connected to such incidents rose to $1.7 billion in the U.S. in 2019, up 37% from the previous year.[4] It's important to understand what business email compromise is and how to spot it.

Business email compromise losses were $1.7 billion in 2019, up 37% compared to 2018

Emails look legitimate but are sent from fake addresses — or from hijacked real addresses — to a business email account. The seemingly legitimate address serves as the "Trojan horse" to get an employee's attention, and persuades the employee to change payment information or send a wire transfer by mistake. Attachments or links in a fraudulent email provide a way for criminals to deploy malware or ransomware; it just takes one click from an unassuming recipient.

Business email compromise campaigns are getting harder to recognize. They may reference current news events, and may be personalized and professionally written. Gone are the days of easy-to-spot emails with spelling errors and poorly replicated company logos.

In 2020, opportunistic criminals have been tailoring their campaigns to reference the latest coronavirus news, often addressing changes in payment schedules that have been created by disrupted workflows and employees working from home. Cyber criminals understand that concerned and distracted employees — particularly those working from home — are vulnerable and have targeted people working with devices that are insufficiently secured.

Business email compromise succeeds because it exploits people's trust and their impulse to help when presented with an apparent emergency. An effective way to earn someone's trust is to send a fake message that sounds real, with legitimate details and information.

The availability of information on the Internet and the rise of social engineering provide cyber criminals an opportunity to study their potential targets. Criminals can conduct research on company websites, Securities and Exchange Commission databases, news sites and third-party retail websites.

In addition, they may scour social media sites and gather personal information about targeted individuals, including roles and responsibilities listed in social media profiles or on social platforms, then use those personal details to tailor messages. These individual cyber criminals also work with organized-crime organizations to share information on how to best get access to corporate email. Criminal use of hijacked or compromised email accounts is on the rise.

In the past, attempts at business email compromise have been aimed primarily at financial gatekeepers, including employees in treasury, and particularly business owners, general managers or CFOs. But criminals' targets have expanded to other departments that can provide access to money as well as access to third-party vendor payments.

Common phishing tactics in 2020

- Coronavirus news
- Changes in payment schedules
- Employees working from home on unsecured devices

The FBI recently reported an increase in payroll diversions that resulted from cyber criminals targeting staff in human resources and payroll, requesting changes to employees' direct-deposit accounts. Vendor-specific incidents also are on the rise. Criminals impersonate a legitimate, trusted vendor and try to persuade someone at the company to make payment for contracted services. Or an email asks that a vendor's information be changed, diverting payments to the criminal's address or a fraudulent bank account.

Meanwhile, ransomware, sometimes the end result of a successful business email compromise, is a perennial threat. The idea is no longer new: Using an email link or attachment, a criminal delivers software that automatically downloads and then locks or corrupts a computer system — until a hefty ransom is paid.

In recent months, the deployment of ransomware has skyrocketed. In 2019, more than 200,000 organizations said they had files that had been hijacked in ransomware incidents, a 41% increase from the previous year. The ransom paid to release files can range from thousands to millions of dollars and averaged $84,000 in the fourth quarter of 2019.[5]

Ransomware has become so lucrative that criminal organizations now offer prepackaged ransomware kits and sell them on the portion of the internet known as the dark web. It's popular because it works. Victimized businesses pay ransoms because they face a ticking clock and the threat of a data breach or compromised business operations if they don't pay the criminal.

As the number of connected devices grows and the techniques that cyber criminals use improve and evolve, dealerships will need to remain vigilant and proactive. Employee education and a relentless eye for cyber security are the best tools to protect susceptible staffers and company resources.

What does business email compromise look like?

Most attempts at business email compromise fall into a few general categories:

1. **Vendor email compromise:** A cyber criminal takes control of a legitimate email account from a vendor, forging or spoofing that email address. The emails might include requests to change payment or bank account information in an effort to divert vendor payments to the criminal.
2. **Executive payment requests:** A criminal impersonates a supervisor or business owner by using a spoofed or compromised email address. The message often asks an employee to make a payment and typically stresses the need to make it quickly — hoping the employee will avoid checking the request through proper channels.
3. **Payroll diversion schemes:** A criminal pretends to be an employee and sends a request to change direct-deposit account information, hoping to reroute the paycheck to a fraudulent bank account the criminal can access.

Suspicious keywords

The most common words and phrases used in business email compromise attempts:[6]

Transaction request
Important
Outstanding payment
Important update
Notice of payment received
Urgent
Request
Payment
Info
Attention

! Best practices to avoid worst-case scenarios

While dealership use of digital tools continues to expand, cyber criminals are simultaneously finding new ways to compromise businesses. Consider these best practices that can help protect your dealership, your business operations and your employees from cyber crime.

Remember that the first line of defense is your people. Make sure that all employees — from treasury to fixed ops, sales and F&I — are aware of the basics in answering email and text messages and especially in handling money requests:

- **Be careful when responding to emails or texts from unknown senders, and don't click on attachments and links.**
- **Confirm unusual money requests for a check or wire transfer, in person or on the phone.**
- **Employ a "trust but verify" approach — trust that the person communicating or making a request is legitimate, but verify it.**

You can fight back

Equip your employees | Secure your systems | Train, test and train some more

Regularly review how account information is updated and payments are approved, for both employees and vendors. Any requests to change account information should be approved through a different channel than the original inquiry.

Require compliance training and security awareness updates for all personnel. Keeping staff members educated about the latest criminal techniques will help them detect suspicious activity and respond safely.

Run regular phishing exercises. Send employees emails with links they shouldn't click, and have them review cyber security materials.

Offer more in-depth training to employees who are most likely to be targeted, including the dealer principal, general manager and CFO — along with their personal assistants — as well as staff in F&I, payroll and human resources.

Provide ongoing security training or certifications for IT personnel.

Consider hiring an IT services provider for additional help. Often dealerships ask an employee to oversee IT as a part-time responsibility. That may not be enough to properly monitor security.

Display training certifications in the dealership to reassure customers that you take security seriously.

Regularly test security systems and processes, updating where necessary. Conduct a risk assessment to identify possible internal and external problems.

Back up information and databases regularly, and be sure that all software being used has the latest updates and patches. Make sure basic operating systems are supported with security updates — and if they can't be supported, upgrade to newer software.

Don't forget about the connected devices that make up the Internet of Things. Identify, classify and locate all IoT devices connected to the dealership network, and be sure to keep them secure. IT staff should be responsible for restricting the access of IoT devices to the broader network, for keeping the software on those devices updated and for making all employees aware of IoT security concerns.

Keep third-party vendor lists updated and regularly reevaluate vendor access to dealership computer networks. Ask to review each vendor's own security and backup processes.

Use email filtering software to help identify spam and fraudulent email designed to trick or compromise employees. Filtering software analyzes incoming messages, searching for suspicious header and domain information — for instance, an email apparently from a company executive that comes from an external account is an immediate tipoff to directly verify that request with the executive.

Consider asking criminals' key targets — including executive assistants, payroll, HR, treasury and F&I staff — to limit the personal business-related information they share online. Those bits of personal information can be used to prey upon employees and fraudulently gain their trust.

Create and carry out a formal process and written plan to respond to a data breach. Make a list of employees needed as a response team, and don't forget to include IT, legal and communications/public relations experts.

Offer a refresher course on cyber security to all employees at least once a year

Educate employees about how to keep their personal phones safe. That includes basic security protocols like password management, automatic software updates and multifactor authentication.

Provide a security checklist for employees working from home or on their personal devices. That might include salespeople checking a phone while on a test drive or a back-office employee working remotely. The list should begin with these items:

- **Every employee should be aware of the dealership's data privacy policies and make it a priority to protect customer information.**
- **Try to avoid printing confidential customer files at home. If it's necessary to print out a client record, be sure to keep paperwork private from family and friends and to securely dispose of all printouts after use.**
- **Do not allow anyone else — family, friends or customers — to use a work-issued device for any reason, and make sure to turn off the device when not in use.**
- **When working off-premises or even away from your desk, practice cyber security best practices. Avoid public Wi-Fi and charging stations, don't transmit sensitive information over personal devices, and make sure computer and phone screens are not visible through a window or to anyone else.**
- **Regularly back up information on company servers.**

Finally, offer a refresher course on cyber security to all employees at least once a year, with information about new and emerging threats and best practices. When it comes to cyber security, there's always something new to learn, because cyber criminals are always presenting new approaches. Even the most robust process won't work without continual updates. The safest business is one that's aware of what's new.

In extraordinary circumstances, a dealership should be prepared with accelerated and ongoing training to keep employees and data safe.

A secondary benefit of regular cyber security training and awareness is that it can help foster a culture of security across a company. Everyone feels part of the initiative, and everyone can feel safer.

A cyber glossary

Cyber security is a fast-moving field and difficult to track partly because criminals use new techniques and tools all the time. Here are some of the sometimes confusing terms you might not recognize:

Business email compromise: The targeted individual is contacted through their work email in an effort to trick the target into sending funds.

Internet of Things: The global network of connected or "smart" devices, each containing embedded technology used to communicate information to other devices using the cloud. In simple terms, it's every device connected to the internet and designed to "talk" with other devices. The IoT includes everything from traditional computers and smartphones to automated thermostats and heating, ventilating and air-conditioning systems; security systems including sensors and cameras; intelligent lighting; telephone equipment; credit-card terminals; smart speakers; smart traffic controls; fleet management systems; and electronic toll collection systems.

Malware: Software — including spyware, banking malware, ransomware and adware — designed to infiltrate personal and company-owned phones and computers.

Man-in-the-middle threats: A cyber criminal intercepts communications between two parties — a dealership and financial institution, for instance, or between two dealerships — in an effort to intercept a wire transfer, steal data or load malware onto a computer system.

Network spoofing: Cyber criminals set up fake Wi-Fi hubs with the goal of prying passwords and personal details from unsuspecting people.

Phishing: A form of social engineering in which seemingly legitimate messages are sent via email or messaging platforms to gain access to systems or data or to install malware (malicious software).

Ransomware: A sophisticated extortion system. Malware is delivered through links in and attachments to email messages, then it is loaded onto a company's computer system. Ultimately the leaders of a business are presented a ransom note typically threatening to freeze or destroy data on the computer network if demands for payment are not met.

Smishing: Cyber criminals utilize SMS and messaging apps to scam people out of their data and money or prompt them to install a malicious app.

Social engineering: A term used to describe all attempts to psychologically manipulate or trick people into providing confidential information or performing actions with the goal of acquiring data or money. Rather than physically hacking into a computer system, these criminals use information available on social media to take advantage of victims, exploiting their natural human tendencies and emotional reactions in order to gain access to a computer system.

Spyware: Malware specifically designed to allow the criminal to spy on a computer user, capturing keystrokes used for user IDs, passwords and other information.

Vishing: A cyber criminal impersonates a legitimate source, or utilizes tactics such as robocalls, to scam people out of data and money over the phone.

FYI on IoT

Three questions to ask when buying devices that use the **Internet of Things**:

Can its firmware or OS (operating system) be updated?

Firmware is permanent device software. With more complex devices, firmware updates may be necessary to keep devices secure.

Will the manufacturer support and provide security updates?

Some devices are programmed to check for and download updates. Others require users to check with manufacturers. Make sure you know what your staff is responsible for.

Can the device be remotely controlled and monitored?

IoT monitoring may allow users to access device data, gauge its performance and evaluate its security status.

Sources:

[1] "Retailers prime targets for data theft, *Automotive News*, Dec. 9, 2019. https://www.autonews.com/finance-insurance/retailers-prime-targets-data-theft.

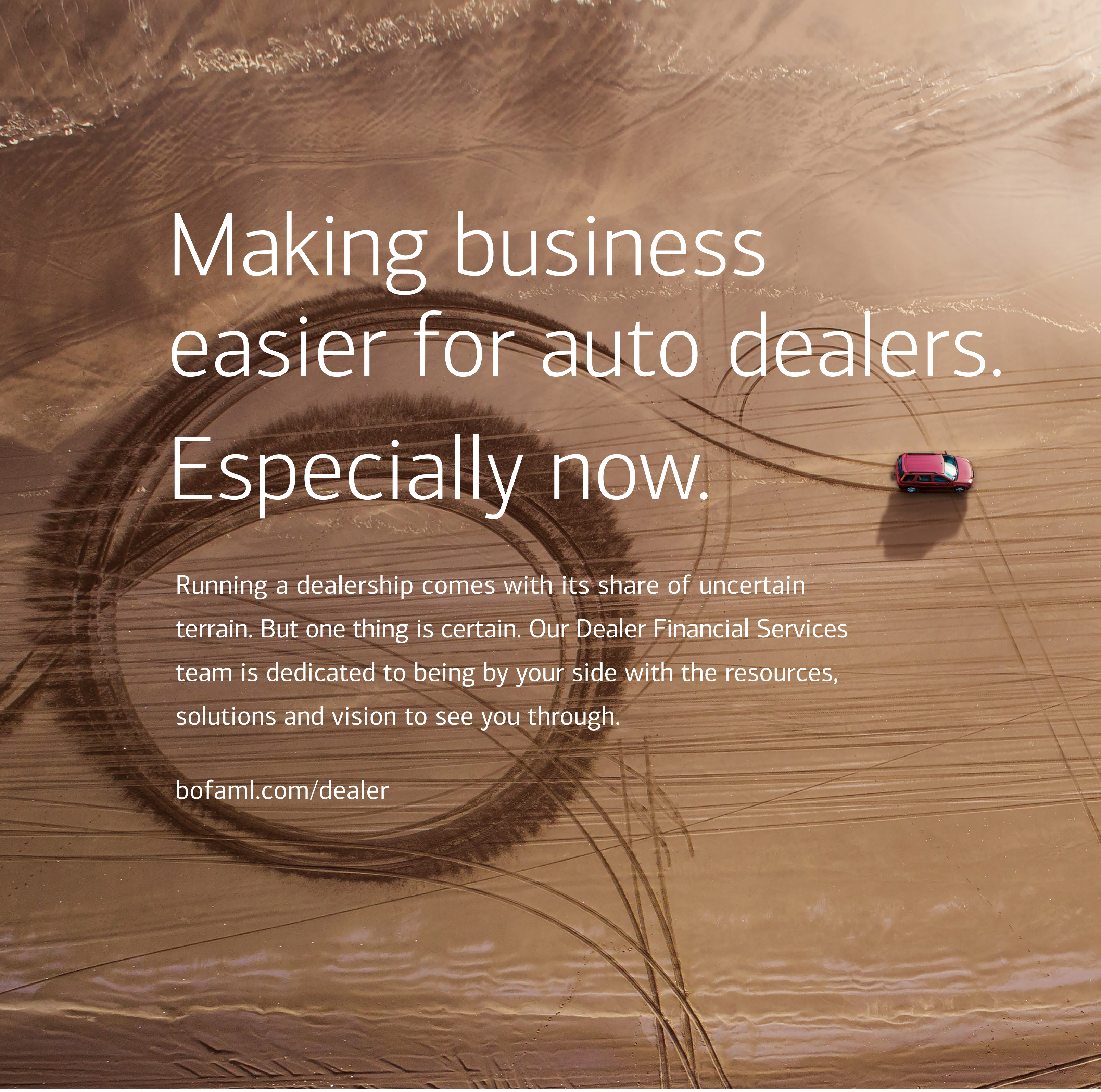
[2] "Over 80% of Consumers Would Not Purchase A Car From Dealership With A Data Breach," Total Dealer Compliance press release, June 2015. https://www.totaldealercompliance.com/Computer%20Security%20Press%20Release.pdf.

[3] Ibid.

[4] FBI Internet Crime Complaint Center, 2019 Internet Crime Report, February 2020.

[5] Emisoft 2019 statistics.

[6] Symantec analysis of top 10 keywords used July 2018 – June 2019. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bec-scams-trends-and-themes-2019.



Making business easier for auto dealers.

Especially now.

Running a dealership comes with its share of uncertain terrain. But one thing is certain. Our Dealer Financial Services team is dedicated to being by your side with the resources, solutions and vision to see you through.

bofaml.com/dealer

BANK OF AMERICA

“Bank of America” and “BofA Securities” are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation (“Investment Banking Affiliates”), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates: Are Not FDIC Insured • May Lose Value • Are Not Bank Guaranteed.