BDO Driving Profits
NEWSLETTER

INSIGHTS FROM THE BDO AUTO DEALERSHIPS PRACTICE

NEWLY UPDATED FTC SAFEGUARD RULES & THE IMPACT TO DEALERSHIPS

BDO

Auto dealerships have plethora of business-related items to deal with on a day-to-day basis. With the level of customer data needed to transact most dealership services and sales, security of systems and information is a key area that can greatly impact a business's reputation and bottom line. For the auto industry, there are a number of regulatory requirements to take into consideration when it pertains to customer data. While regulatory standards, such as the **Federal Trade Commission's (FTC) Part 314 – Standards For Safeguarding Customer Information**, are not new, there are continued updates to understand in order to stay in compliance.

Staying on top of the continual updates may be a little frustrating, but the ongoing changes are necessary. Threats to systems and data continue to evolve as businesses and consumers use more technology. The expanded use of technology and large volumes of data create an opportunity for those who want take advantage of others. While companies implement solutions to protect systems and data, hackers use advanced technology, techniques and processes to cause problems.

As a result, reasons for updates to regulations, such as the FTC part 314 can be summarized as follows:

Cyber-attacks and security breaches will occur and will negatively impact the business.

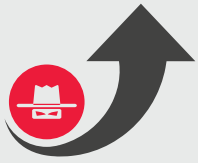
According to most cybersecurity surveys,

over 60%

of all data breaches originate from unauthorized access from one of the organization's current or former employees, or third-party suppliers.

Cyber liability insurance premiums are significantly increasing in cost and often do not cover all the damages caused by a cyber breach.

Security attacks are on the rise, with a



50% increase

in cyberattacks year over year.

Achieving information security compliance with one or more government regulatory standard for information security (i.e., ISO 27001, NIST 800-171, HIPAA, NYDFS, SOC 2, and so forth.) is good when working with third-parties, but is not sufficient to holistically address security.

WHAT ARE THE NEW FTC RULES?

The most recent of the FTC's amendments went into effect on January 10, 2022, and requires implementation by December 9, 2022. While a full overview of what an information security program may look like for a business is referenced on the **FTC website** and includes additional details for the items listed below, the information security program can be summarized as follows:

a. Designate a qualified individual to implement and supervise your company's information security program.

b. Conduct a risk assessment.

c. Design and implement safeguards to control the risks identified through your risk assessment. This includes eight detailed, security related solutions, tasks, or action items.

d. Regularly monitor and test the effectiveness of your safeguards.

e. Train your staff.

f. Monitor your service providers.

g. Keep your information security program current.

h. Create a written incident response plan.

i. Require your qualified individual to report to your Board of Directors.

WHAT DOES THIS MEAN FOR YOUR DEALERSHIP?

For dealerships to address the new requirements outlined in the information security program and reduce risks, key steps to take include:

1. **Training your workforce** to understand the purposes of security processes, monitoring results, and enhancing the training to address changing threats and risks.

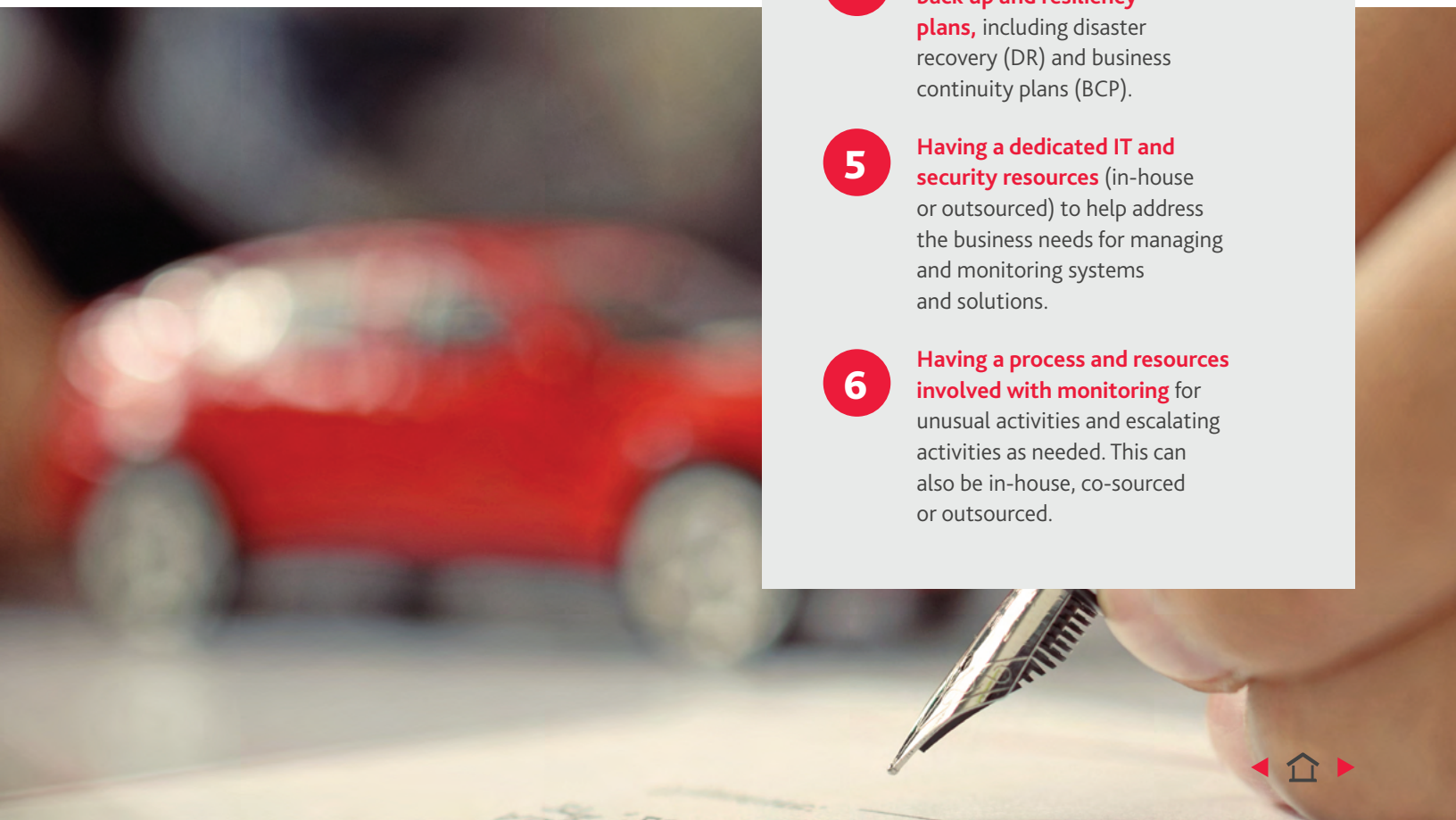
2. **Implementing multi-factor/ two factor solutions** for all users, contractors and vendors accessing the company systems. This would apply to customers access their personal information that the company may host/manage.

3. **Implementing and/or updating security related software.**

4. **Defining and implementing back up and resiliency plans,** including disaster recovery (DR) and business continuity plans (BCP).

5. **Having a dedicated IT and security resources** (in-house or outsourced) to help address the business needs for managing and monitoring systems and solutions.

6. **Having a process and resources involved with monitoring** for unusual activities and escalating activities as needed. This can also be in-house, co-sourced or outsourced.



DUE DILIGENCE FOR 3RD PARTY VENDORS IS A MUST

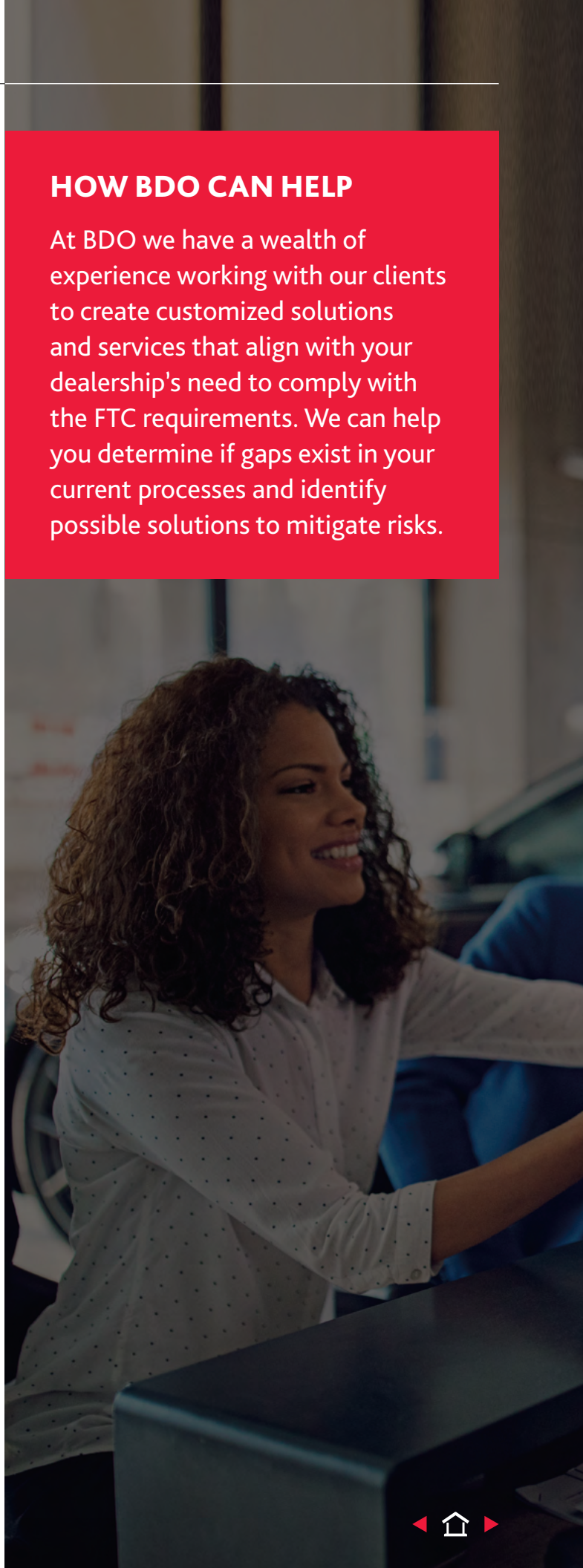
Of particular note in the amendments is item f. monitor your service providers. As systems and even organizations are "connected" for business solutions, monitoring your service providers is a standard that needs structure and processes. When co-sourcing or out-sourcing services, this does not eliminate the risk to the Company for those activities. Service providers have been defining shared responsibilities, which means the Company is required to perform tasks or are responsible for activities, even though a process has been outsourced. As part of the service provider monitoring, and due diligence process you should understand:

- Does the provider have a SOC2 report or security assessment report?
- Has the provider engaged a third-party to test or assess the control environment or services related to the out-sourced solutions the Company is using?
- Does the provider have cyber insurance?
- Does the provider require everyone to use multifactor solutions?
- Does the provider have unique login identification?

Security threats to systems and data will continue as technology use expands and evolves, so dealerships need to be prepared to address issues on a on-going/regular cadence, not just from an annual perspective. To help reduce risk of a possible event, dealerships need to train staff to understand and embrace security practices, make strategic investments in updating security solutions and processes (both in-house and outsourced), and design, implement and test incident response and/or back up plans. By understanding the FTC standards and following the security program guidance, dealerships can address the potential system and security risks in addition to protecting your organization's data, reputation and daily business activities.

HOW BDO CAN HELP

At BDO we have a wealth of experience working with our clients to create customized solutions and services that align with your dealership's need to comply with the FTC requirements. We can help you determine if gaps exist in your current processes and identify possible solutions to mitigate risks.



People who know Auto Dealerships, know BDO.

www.bdo.com

HAVE QUESTIONS OR WANT TO LEARN MORE? CONTACT US!

GREG SCHU
Partner and National Practice Lead, Cyber Compliance & Assessments
gschu@bdo.com

MEGAN CONDON
Tax Partner, Auto Dealerships Practice Co-Leader
mcondon@bdo.com

JORDAN ARGIZ
Audit Partner, Auto Dealerships Practice Co-Leader
jargiz@bdo.com

ABOUT BDO'S AUTO DEALERSHIPS PRACTICE

BDO is a valued business advisor for auto dealerships, bringing a wealth of experience on traditional and emerging accounting, tax, and advisory issues. The firm's Auto Dealerships industry practice works with a variety of companies across the dealership sector, including automotive, motorcycle, marine, RV, rental equipment and more. We help dealerships of all sizes achieve their desired business outcomes.

ABOUT BDO USA

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. www.bdo.com