Inviting Data Hackers to Lunch Without Knowing it

...And Getting Stuck with the Tab

Bob Schaefer, Vice President of Data Services
Reynolds and Reynolds

Inviting Data Hackers to Lunch Without Knowing it

[The Target] breach affected nearly *one third* of the U.S. population.

"...outside service providers connected remotely have the keys to the castle."

"They came in through the Chinese takeout menu." That's the way the first sentence reads in a recent New York Times article on data and network security.

The story went on to say that when the hackers were unable to breach the main network of a large company, they added malware to the online menu of a popular Chinese restaurant that employees used. The result? "When the workers browsed the menu, they inadvertently downloaded code that gave the attackers a foothold in the business's vast computer network," the article said.

When Target was hit with a massive data breach of consumers' personal and payment information last year, the hackers went in through the heating and cooling system software, after Target had granted permission for a third-party vendor to access its network. That breach affected nearly *one third* of the U.S. population.

Commenting on the Target breach, the chief executive of a network security firm was quoted in the media as saying, "We constantly run into situations where outside service providers connected remotely have the keys to the castle."

While online takeout menus and heating and cooling systems are not the most prevalent threats to automotive dealerships, the examples illustrate the difficulty – and vigilance required – in protecting dealership networks and vital business and customer data. As more dealership management systems (DMS) and networks are connected to more remote devices and to other service providers, the vulnerabilities are both more obvious and also more likely to lurk in unlikely places.

The Double Burden of Data

In today's competitive automotive retailing environment – an environment in which dealers are no longer compared simply to other *dealers*, but also to other *retailers* – dealers are adopting a *retail* mindset and harnessing the data already at their fingertips in their customer database.

Harnessing that data often requires the involvement of third-party specialists who can help the dealer turn the data into useful business information to advance the dealership and improve the customer experience. The business imperative to reach the right customers at the right time in the right way with the right messages

...dealers carry a double burden: They *own* a portion of the data in the DMS. They also retain *custody* over a portion of data owned by others... And, they are responsible for protecting *all* of the data...

also puts a higher premium on the data in the dealership's customer database and brings greater scrutiny to how it's handled, protected, and used.

And therein lies the rub.

There was a day when unmonitored, unchecked access to the DMS by third parties – access that often was automated – was the norm. Those days are over.

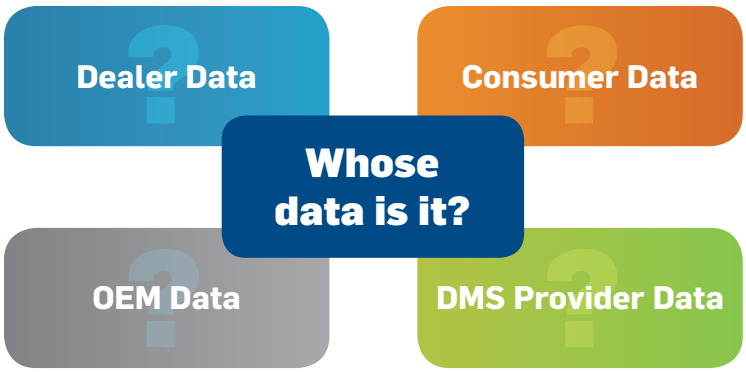
A dealer's permission alone is no longer adequate protection for a third party to access data in the DMS; a third party's assurance to only access the information they are authorized to access is no longer an adequate safeguard for data in the DMS.

That's too simplistic a view of the issue.

It's an equally simplistic view that the data in the DMS *belongs* to the dealer. It was never really the dealer's data to begin with – at least not all of it. Certainly, there is business data in the DMS that belongs to the dealer.

- Yet there is also consumer information that still belongs to the consumer (they haven't relinquished their ownership);
- There is proprietary OEM information that belongs to the manufacturer; and
- There is information from the DMS provider that is proprietary and belongs to the provider.

The result is that dealers carry a double burden: They *own* a portion of the data in the DMS. They also retain *custody* over a portion of data owned by others but that resides in the DMS. And, they are responsible for protecting *all* of the data in the DMS to ensure safeguards and protections within the appropriate business and regulatory framework(s).



...businesses are collecting more personal information about consumers, storing and transmitting it... and creating a greater likelihood that the data may be compromised.

Enter the Federal Trade Commission (FTC)

The FTC's mandate from Congress gives the agency authority over privacy and data security.

Here's how one of the attorneys at the FTC put the issue: "Businesses need to take a hard look at what kind of information they're dealing with day-to-day and what they have on their computer systems."

That should serve as a wake-up call for automotive retailers and OEMs, even though fears of other regulatory actions may have overshadowed it.

Over the past 18 months, the automotive industry and individual dealers have been especially focused on the Consumer Financial Protection Bureau (CFPB) and the potential for more government involvement in dealership F&I practices. While that may be a legitimate concern, it also may have inadvertently lulled dealers into overlooking the potential of a larger disruption to their business practices and operations: data security requirements and regulations. That's the FTC's purview.

In congressional testimony earlier this year, FTC Chairwoman Edith Ramirez noted that information is the new currency in an increasingly connected world and data-driven economy. She also noted that businesses are collecting more personal information about consumers, storing and transmitting it across their own systems, and creating a greater likelihood that the data may be compromised.

"Never has the need for legislation been greater," the testimony said. "With reports of data breaches on the rise… Congress needs to act."

Clearly, if dealerships don't secure their data in ways that pass muster with the FTC, then they'll be pulled further into the FTC's enforcement orbit.

Enter the National Automobile Dealers Association (NADA)

To NADA's credit – and the benefit of the industry – NADA has taken a firm stance for the industry and has stepped forward with critical guidance around dealership data security. NADA put a stake in the ground, drew a sharp line between old and new (here's

how the industry used to operate; here's how we need to operate in the future), and pushed this issue top of mind for the automotive industry and for individual dealers.

In 2013, NADA published a memo with guidelines on service provider contract language and a dealership's obligation regarding Non-Public Personal Information (NPPI). The "Dealer Data Guide" memo also includes a checklist to use to help ensure the safe and secure movement of data to external providers.

Here's how the memo frames the issue: "An important issue to understand is that the FTC may consider any third party 'access' to NPPI to be the equivalent of 'sharing.' In other words, if a third party has access (via your computer network or otherwise) to NPPI or could access it, you may be deemed (or at least alleged) to have 'shared' that data, even if the third party never actually accesses, obtains, processes or relies upon the data."

"Remember, it is not only the data they actually take, but the data they could take (have access to), that you must control."

What does this mean for dealers? The NADA memo says that dealers "need to (1) understand exactly what data a service provider needs to provide the service, and (2) take the appropriate technical steps to ensure that their access is limited to that data and that data only. Remember, it is not only the data they actually take, but the data they could take (have access to), that you must control."

Finally, as part of the Dealer Data Guide, NADA recommends that dealers implement a "strict data 'push' system for sharing data."

What's Next for Dealers?

Several practical conclusions come to mind from the NADA Dealer Data Guide memo and the active interest by the FTC in privacy and data security.

First, access to data equals sharing data. Therefore, if you are concerned about how and where data from the DMS is shared and used, draw the line at access. Prevent access and you prevent sharing.

Second, push data from the DMS, which eliminates the need for third parties to access the DMS directly to pull data from it.

Third, the FTC is adopting a fairly liberal "chain of custody" model that includes a burden of responsibility for "all of those in the chain of handling consumer data."

That makes it virtually impossible for a dealership or third party *not* to leave its digital fingerprints on the data.

That makes it virtually impossible for a dealership or third party *not* to leave its digital fingerprints on the data. Broadly interpreted, this implies that if you touch the data at *any* point then you may have acquired responsibility for what happens to the data at *every* point.

The Challenge Ahead

Ultimately, protecting data in the DMS is a shared obligation between the dealership, the DMS provider, the OEM, and third parties providing services for the dealership or OEM.

In meeting that shared obligation, third-party providers and OEMs own the responsibility to verify which data fields they have accessed in the DMS, how it matches the data the dealership has authorized them to access, and what happens to the data once it leaves the dealership.

In turn, dealerships own the responsibility to implement the technologies and employee practices that help safeguard secure access to data in the DMS.

In the complicated and ever-changing world of privacy and data security:

- Consumers have the right to know how their personal and transaction information with the dealership is being safeguarded or used.
- Dealers have the right to know who is accessing what data in the DMS and how that data will be used – and by whom.
- And the FTC has the authority to oversee and regulate both.

That is the new world order.

Visit ***www.reyrey.com/datasecurity*** to read more about how the automotive industry is changing.

Bob Schaefer is vice president of Data Services at Reynolds and Reynolds. In that role, he and his team are responsible for the secure movement of data for all Reynolds products and services. During his 35-year career with Reynolds, he has led work in dealership management systems, dealer communications systems, and data integration structures.

Note: The content in this whitepaper is believed to be accurate but should not be construed as legal advice.

Acknowledgements:

"Hackers Lurking in Vents and Soda Machines," Nicole Perlroth, New York Times, April 7, 2014.

"Heat System Called Door to Target for Hackers," Nicole Perlroth, New York Times, Feb. 5, 2014.

"Target Data Breach Gets Worse, 110 Million Shoppers At Risk," Laura Heller, Fierce Retail, Jan. 10, 2014.

"Target Says It Ignored Early Signs of Data Breach," Associated Press, March 14, 2014.

"The Privacy Challenges of Big Data: A View from the Lifeguard's Chair," Keynote address by FTC Chairwoman Edith Ramirez, Technology Policy Institute, Aspen Forum, Aug. 19, 2013.

"The FTC is Watching, Making Sure Dealers Keep Customers Private," Editorial, AutoRetailNet, Aug. 6, 2012.

Prepared statement of the Federal Trade Commission, "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime," before the Committee on the Judiciary, United States Senate, Feb. 4, 2014.

"Dealer Data Guidance," National Automobile Dealers Association memo to NADA Members, August 28, 2013.

Published Statement of FTC Commissioner Brill, (Revised Aug. 15, 2011).

Retail Management System

Reynolds & Reynolds®

800.767.7879 | info@reyrey.com | www.reyrey.com