Are You Properly Vetting Your Service Providers?

July 31st, 2019 | and Eric L. Johnson

I'm frequently asked by dealer clients to speculate about whether they have their compliance house in order simply based on what DMS provider, underwriting or scoring system provider, or forms provider they use. "I'm using all of these great and well-known companies in the marketplace," they'll say. "What else can I do?" Well, a recent action by the Federal Trade Commission sheds more light on dealerships' use of service providers and should serve as a warning to dealers to properly vet (and continue to vet) their service providers.

The FTC has accepted, subject to final approval, a proposed consent order with a DMS provider, LightYear Dealer Technologies, LLC, doing business as DealerBuilt, for allegedly "fail[ing] to implement readily available and low-cost measures to protect personal information it obtained from its auto dealer clients." This failure, the FTC claimed, "led to a breach that exposed the personal information of millions of consumers."

Here's what the FTC claims happened. The DMS provider had approximately 180 customers, which comprised nearly 320 dealership locations. The customers were large dealerships with multiple storefronts and hundreds of employees, along with dozens of small businesses with just a handful of employees. The DMS reportedly stored personal information about more than 14 million individual consumers.

The FTC alleged that the DMS provider directed a company employee to buy a storage device and attach it to the provider's backup network. The storage device wasn't securely configured, creating an open connection port that allowed transfers of information for approximately 18 months. Beginning in late 2016 and continuing for at least 10 days, a hacker gained unauthorized access to the backup database through the unsecured storage device, including the unencrypted personal information of around 12.5 million consumers stored by 130 customers. The hacker attacked the system multiple times, downloading the personal information of more than 69,000 consumers and the entire backup directories of five customers.

That's not all. The provider's insecure settings were indexed on Shodan, a publicly available website that hackers may use to locate insecure Internet-connected devices, meaning that other hackers also could gain access to the information. What was stolen? Customers' full names and addresses, telephone numbers, SSNs, driver's license numbers, and dates of birth, as well as the wage and financial account information of dealership employees. Just the type of information a thief needs to commit identity theft and fraud.

The DMS provider learned of the breach and notified its dealership customers and then affected consumers. Dealerships received complaints about the breach and, in some cases, had to hire

lawyers to help them notify their customers.

The FTC brought the administrative complaint against the DMS provider and alleged that it was a "financial institution," subject to the Gramm-Leach-Bliley Act, because it is "significantly engaged in data processing" for auto dealerships that extend credit to consumers. The FTC also alleged that because the provider collected nonpublic personal information, it was subject to the FTC Safeguards Rule.

The FTC alleged that the DMS provider violated the Safeguards Rule in multiple ways, such as by failing to "develop, implement, and maintain a written information security program"; by failing to "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and fail[ing] to assess the sufficiency of any safeguards in place to control those risks"; and failing to "design and implement basic safeguards and to regularly test or otherwise monitor the effectiveness of such safeguards' key controls, systems, and procedures."

The FTC complaint further alleged that the provider's failure to employ these reasonable measures to protect personal information caused or is likely to cause substantial injury to consumers and constituted an unfair act or practice under the FTC Act.

So, is it your responsibility to properly vet and oversee your service providers? In a word, yes. You should carefully review your responsibilities under the FTC's Safeguards Rule. These responsibilities include taking reasonable steps to select and retain service providers that are capable of maintaining the appropriate safeguards for customer information and requiring them by contract to implement and maintain those required safeguards.

Sounds like another discussion you need to have with your friendly lawyer.