THE
NATIONAL LAW REVIEW

FTC and Car Dealership Software Company Reach Security Settlement

Monday, June 24, 2019

Article By
Liisa M. Thomas
Sheppard, Mullin, Richter & Hampton LLP
Eye On Privacy

Communications, Media & Internet
Consumer Protection
All Federal

The FTC recently settled with LightYear Dealer Technologies, maker of DealerBuilt software, over allegations that the company failed to provide adequate protection for the personal data it houses. The companies' clients include many car dealers across the country, and allows those dealerships to house consumer information that is collected during the car purchase process. This information includes sensitive personal (Social Security numbers) and financial (payroll information and credit card numbers) information. According to the FTC complaint, a company employee without "guidance or . . . steps to ensure the . . . device was securely configured" attached a new storage device to the company servers. This device created an open connection port during an 18 month period. During that time, no vulnerability scanning, penetration testing, or other diagnostics were conducted, according to the FTC. Instead, the vulnerability went undetected until a hacker exploited it and accessed the backup server for DealerBuilt. As a result, the hacker accessed millions of consumers' information, including downloading five clients' information. This information included almost 70,000 Social Security numbers, drivers' license numbers, and payroll details. The company was, the FTC said, unaware of the breach until it was contacted by an impacted client.

According to the FTC, the company had engaged in several practices that constituted a failure to provide reasonable security, namely (1) not having a **written information security policy**, (2) not having **reasonable training or guidance for employees**, (3) not assessing **risks to personal information** on its networks, (4) not using "readily available" security measures or verifying the effectiveness of protection measures, (5) not having **reasonable security controls**, (6) storing information in clear text, and (7) not having a reasonable way to **select and install devices** that will access personal information. The FTC found these failures to be both a violation of Gramm-Leach-Bliley Act Safeguards Rule as well as Section 5 of the FTC Act. To settle the matter, LightYear has agreed to implement an Information Security Program and take steps not to repeat the alleged procedural failings that the FTC believed led to the breach. The company has also agreed to have the program assessed regularly by a "qualified, objective, independent third-party," who will provide documentation about the assessment to the FTC. The company has also agreed to have a senior official certify, annually, that the company is complying with the settlement.

Putting it Into Practice: This recent settlement outlines for companies the FTC's continued expectations of companies to secure information and systems. The settlement terms provide a good overview of the types of things the FTC expects companies to do, including reasonable training, procedures for implementing new systems, and methods for testing security.