5 lessons to learn from software vendor data breach

August 09, 2019

According to a June 12 settlement announced by the **Federal Trade Commission**, back in 2015 an employee of Iowa-based **LightYear Dealer Technologies**, the parent company of **DealerBuilt**, plugged a storage device into the company's backup network to increase storage capacity. However, the employee failed to ensure that the device was securely configured, thereby providing an open, insecure port into the company network, which was open for 18 months.

Subsequently, a hacker penetrated the network and gained access to the company's unencrypted backup data, including personal information — such as Social Security and drivers' license numbers — of about 12.5 million consumers, and the entire backup directories of five dealerships. DealerBuilt failed to detect the breach until an auto dealer's customer complained about personal information becoming public on the internet, and a reporter told the company about the security vulnerability.

The alleged insecure access enabled by the employee's device installation, along with other poor data control and security practices allegedly ongoing at DealerBuilt, led the FTC to allege unfair practices and violation of the Gramm-Leach-Bliley Act's Safeguards Rule (GLB) against DealerBuilt.

The FTC asserted that DealerBuilt met the definition of a "financial institution" for purposes of the Gramm-Leach-Bliley Act. (Under GLB, any institution engaged in certain "finance activities" may be considered a "financial institution." Sufficient "finance activities" include those that are "financial in nature" or "incidental to financial activity," as these terms are defined in 12 U.S.C. 1843(k) and by regulations promulgated by the Board of Governors of the **Federal Reserve**.) GLB further requires financial institutions to develop, implement and maintain a comprehensive information security program; identify reasonably foreseeable risks to the security, confidentiality, and integrity of customer information; and implement basic safeguards and regularly test their effectiveness, all of which DealerBuilt failed to undertake, according to the FTC.

DealerBuilt's data security practices, which were alleged to be lax at the time the FTC filed its complaint, included:

- Storing information in clear text, without any access controls or authentication protections like passwords or tokens. Data transmitted between dealerships and DealerBuilt's backup database also was in clear text.
- No written information security policy.
- No provision of reasonable data security training for employees or contractors.

- No assessment of risks to the sensitive data on its network by conducting periodic risk assessments or performing vulnerability and penetration testing.
- No use of readily available security measures to monitor – among other things – unauthorized attempts to transfer sensitive information.
- No reasonable data access controls in place – for example, systems to limit inbound connections to known IP addresses or require authentication to access backup databases.
- No reasonable process to select, install and secure devices with access to personal information.

In reporting the outcome of the case's proposed settlement, the FTC noted the following key recommendations for those in possession of consumer personal information:

1) Train and supervise your employees to be security-centric.

2) Exercise care when installing devices with network access.

3) Note that Gramm-Leach-Bliley Act coverage is broad. Consider whether your business (or affiliates or service providers) could be a "financial institution" subject to the GLB Safeguards Rule (16 C.F.R. Part 314). All it takes is for a business to be "significantly engaged" in providing financial products or services.

4) If your company uses third-party software or providers, build security into your contracts with those providers.

5) Remember that service providers also are accountable for protecting the personal data they collect and store.

This article was first published on Auto Finance Excellence, a sister service of Auto Finance News, and is reprinted with permission. McGlinchey Stafford is pleased to serve as the official Compliance partner of Auto Finance Excellence, providing insights and thought leadership through webinars, podcasts, and monthly columns.