THE
NATIONAL LAW REVIEW

# Further Expansion of Data Security Requirements in FTC Order with LightYear Dealer Technologies

Friday, June 14, 2019

The FTC has entered into a settlement with LightYear Dealer Technologies, doing business as DealerBuilt, a technology company that develops and sells dealer management system (DMS) software and data processing services to automotive dealerships nationwide. The settlement resolves allegations that DealerBuilt engaged in a number of unreasonable data security practices. The DealerBuilt's DMS software tracks, manages, and stores information related to all aspects of a dealership's business, including sales, finance, inventory, accounting, payroll, and parts and service and collects and maintains personal and competitively sensitive information about consumers and employees.

Drinker Biddle

Article By
Katherine E. Armstrong
Drinker Biddle & Reath LLPDBR on Data

Communications, Media & Internet
All Federal

According to the complaint, the DMS collected and stored personal data of over 14 million consumers, including names, addresses, Social Security numbers, driver's license numbers, credit card numbers, and vehicle information. In addition, the DMS collected and stored the personal data of over 39,000 dealership employees included names, addresses, Social Security numbers, wages, and bank account information. All of this data was stored in clear text, without any access controls or authentication protections. Further, the personal information was transmitted between servers and the dealerships in plain text.

As detailed in the complaint, in April 2015, a DealerBuilt employee bought a storage device and attached it to the network, which created an open connection port that allowed transfers of information for about 18 months. During this time no vulnerability scanning, penetration testing, or other diagnostics were performed. In October 2016, a hacker gained unauthorized access to the backup database through the unsecured storage device and obtained the unencrypted personal information of approximately 12.5 million consumers. DealerBuilt failed to detect the breach. It was not until a security reporter contacted DealerBuilt and a dealership called to complain that its data was publically accessible that the breach was discovered and the vulnerability was identified as the open port on the storage device.

The complaint alleges that DealerBuilt violated both Section 5 of the FTC and the Gramm Leach Bliley Act's Safeguards Rule. DealerBuilt is a financial institution because it is significantly engaged in data processing for its customers, auto dealerships that extend credit to consumers. Specifically, the complaint alleges that DealerBuilt's failure, among other things, to develop, implement, and maintain a written organizational information security policy; to implement reasonably guidance or training for its employees; and to use readily available security measures to monitor its systems or to impose access controls was an unfair practice. The Safeguard's Rule allegations mirror the Section 5 allegations.

The proposed settlement, which has been put out for public comment, includes the standard provisions that will require DealerBuilt to implement and maintain a comprehensive Information Security Program and have biennial assessments performed by a third party for 20 years. It also includes the new provisions announced in the Clixsense and iDressup cases announced in April that require a senior DealerBuilt official to provide the FTC with annual certifications of compliance.

There are noteworthy new provisions in this settlement. The Mandated Information Security Program requirements are tighter and more expansive than those in previous settlements are. For example, previous settlements have mandated that Information Security Programs "be designed to" protect, among other things, the security, confidentiality, and integrity of personal information. The DealerBuilt settlement is tighter and eliminates the words "be designed." This subtle change is significant and will require DealerBuilt to ensure that the Information

Security Program actually protects the security of personal information.

Further, the DealerBuilt settlement includes additional requirements that expand the components of a Data Security Program. For example, the DealerBuilt settlement requires annual reporting to the board of directors or governing body and annual training of employees, and it includes specific requirements with respect to implementing technical measures to monitor networks and systems as well as access controls for all databases that store personal information. It also requires encryption of Social Security numbers and financial account information.

There are a few other refinements of note. DealerBuilt will be required to ensure that all devices on its network with access to personal information are securely installed and inventoried at least once annually, to engage in vulnerability testing every four months and promptly after a covered incident, and to perform penetration testing of the network at least annually and promptly after a covered incident.

The provisions for the third-party assessments are more expansive as well and require, for example, that the specific documents and evidence be available to the Commission for review rather than relying on assertions or attestations by management. In addition, the Commission's Associate Director for Enforcement is to be notified of the person who is selected to conduct each assessment, and is also given authority to approve the assessor.

Chairman Simons described the new requirements as "significant improvements to the FTC's data security orders that will further protect consumers and deter lax security practices."
In addition, this settlement is also an important reminder of the importance of engaging in due diligence before engaging service providers.



**Source URL:** https://www.natlawreview.com/article/further-expansion-data-security-requirements-ftc-order-lightyear-dealer-technologies