1723051

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. Simons, Chairman**
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of **LIGHTYEAR DEALER TECHNOLOGIES, LLC, a limited liability company, d/b/a DEALERBUILT.**	**DOCKET NO. C-4687**

COMPLAINT

The Federal Trade Commission, having reason to believe that LightYear Dealer Technologies, LLC, a limited liability company ("Respondent"), has violated the provisions of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), and the Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Title I of the Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. § 6801 *et seq.*; and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent LightYear Dealer Technologies, LLC, also doing business as DealerBuilt ("DealerBuilt"), is a Missouri limited liability company with its principal office or place of business at 2570 4th Street, SW, Suite A, Mason City, Iowa 50401.

2. The acts and practices of Respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

Respondent's Dealer Management Software

3. Respondent is a technology company with approximately 80 employees located in offices in Iowa and Texas and working remotely from locations around the country. Respondent develops and sells dealer management system ("DMS") software and data processing services to automotive dealerships nationwide. A DMS is a suite of electronic applications that track, manage, and store information related to all aspects of a dealership's business: sales, finance, inventory, accounting, payroll, consumer resource management, and parts and service. A DMS

is designed to collect and maintain large quantities of personal and competitively sensitive information relating to both consumers and employees.

4. Since 1996, Respondent has licensed its LightYear Dealer Management System ("LightYear") to automotive dealerships across the United States. Respondent has approximately 180 customers, which comprise nearly 320 dealership locations. Among Respondent's customers are large dealerships with multiple storefronts and hundreds of employees. Respondent advertises that its clients include the world's largest Ford dealership and one of the nation's largest Honda dealerships. Also among Respondent's customers are dozens of small businesses with only a handful of employees.

5. Respondent's customers can either license the LightYear DMS and have Respondent host their data, or they can license the LightYear DMS and host their data locally (*i.e.*, on their own servers) and use Respondent's backup service. Customers that choose the latter option regularly back up their databases onto Respondent's network, which is then stored on Respondent's servers and accessed only in case of a catastrophic event, such as recovery from a corrupt local database.

6. Respondent's LightYear DMS software is designed to collect large quantities of personal information about dealership consumers and employees. Specifically, Respondent's dealership customers upload personal information about consumers who visit their dealerships or purchase their automobiles, including, but not limited to: (1) name; (2) gender; (3) physical and mailing address; (4) phone number; (5) email address; (6) date of birth; (7) Social Security number ("SSN"); (8) driver's license number; (9) vehicles owned, identified by license plate number, vehicle identification number, and key code; and (10) credit card numbers. Respondent stores or has stored at least some personal information about more than 14 million individual consumers.

7. In addition, Respondent's customers upload payroll data about dealership employees, including, but not limited to: (1) name; (2) gender; (3) physical and mailing address; (4) phone number; (5) email address; (6) date of birth; (7) Social Security number; (8) wages; and (9) bank account information. Respondent stores or has stored personal information about approximately 39,000 dealership employees.

8. Respondent stored all of the information described in paragraphs 6-7 in clear text, without any access controls or authentication protections, such as passwords or tokens. Respondent also transmitted this information between servers at the dealerships and Respondent's back up database in clear text.

9. In approximately April 2015, to increase available backup storage, Respondent directed a company employee to purchase a storage device and attach it to Respondent's backup network. At no time did any manager provide the employee guidance or take any steps to ensure the new storage device was securely configured.

10. The storage device that the employee attached to Respondent's network created an open connection port that allowed transfers of information for approximately 18 months (from approximately April 2015 through November 7, 2016). During this time, Respondent did not

perform any vulnerability scanning, penetration testing, or other diagnostics to detect the open port, nor did Respondent maintain a device inventory or employ procedures that would have enabled Respondent to prevent exposure of the open port. To the contrary, throughout this 18-month period, the device remained undetected until it was exploited in the breach of personal information described below.

Respondent's Data Security Practices

11. Until at least June 2017, Respondent engaged in a number of practices that, taken together, failed to provide reasonable security for the personal information stored on its network. Among other things, Respondent:

a. Failed to develop, implement, or maintain a written organizational information security policy;

b. Failed to implement reasonable guidance or training for employees or third-party contractors, regarding data security and safeguarding consumers' personal information;

c. Failed to assess the risks to the personal information stored on its network, such as by conducting periodic risk assessments or performing vulnerability and penetration testing of the network;

d. Failed to use readily available security measures to monitor its systems and assets at discrete intervals to identify data security events (*e.g.*, unauthorized attempts to exfiltrate consumers' personal information across the company's network) and verify the effectiveness of protective measures;

e. Failed to impose reasonable data access controls, such as restricting inbound connections to known IP addresses, and requiring authentication to access backup databases;

f. Stored consumers' personal information on Respondent's computer network in clear text; and

g. Failed to have a reasonable process to select, install, secure, and inventory devices with access to personal information.

Breach of Personal Information

12. Respondent's failures led to a breach of its backup database. Beginning in late October 2016 and lasting at least ten days, a hacker gained unauthorized access to Respondent's backup database through the unsecured storage device, including the unencrypted personal information of approximately 12.5 million consumers, stored by 130 of Respondent's customers.

13. The hacker attacked Respondent's system multiple times, downloading the personal information of 69,283 consumers, the entire backup directories of five customers. The

information stolen included full names and addresses, telephone numbers, SSNs, driver's license numbers, and dates of birth about dealership customers as well as wage and financial account information about dealership employees.

14. Respondent failed to detect the breach. Respondent only became aware of the breach on November 7, 2016, when a customer called Respondent's Chief Technology Officer and demanded to know why customer data was publicly accessible on the Internet. Further, only after a security reporter provided Respondent information regarding the security vulnerability did Respondent discover the source of the vulnerability (*i.e.*, the open port on the storage device).

15. Respondent notified its dealership customers of the breach and then notified affected consumers. Respondent's dealership customers spent hours attempting to match pieces of breached personal information to their customer pool, in order to notify the appropriate consumers. The dealerships received numerous consumer complaints.

Injury to Consumers and Businesses

16. Breached personal information, such as that stored in Respondent's backup database, is often used to commit identity theft and fraud. For example, identity thieves use stolen names, addresses, and SSNs to apply for credit cards in the victim's name. When the identity thief fails to pay credit card bills, the victim's credit suffers. Identity thieves also use stolen personal information, such as the wage and bank account information that Respondent holds, to obtain tax refunds fraudulently. As a result, victims of identity theft often experience long delays before receiving their tax refunds.

17. Similarly, stolen financial information, such as the credit card numbers, expiration dates, and security codes that Respondent holds, can be used to commit fraud. Specifically, a thief could make unauthorized purchases using stolen credit card information.

18. Even if identity theft and fraud do not occur immediately after a breach, a breach of personal information, such as that stored in Respondent's system, makes identity theft and fraud likely. Respondent's backup database was vulnerable for 18 months and its insecure settings were indexed on Shodan, a publicly accessible website that hackers use to locate insecure Internet-connected devices. Respondent was aware that at least one hacker downloaded consumer data from the breached database.

19. The breach of Respondent's database imposed costs on its dealership customers. Specifically, these businesses spent many hours handling breach response communications, identifying affected consumers, and responding to consumer complaints. Some dealerships retained legal counsel to respond to the breach.

20. Respondent's failures to provide reasonable security for the sensitive personal information about dealership consumers and employees, and business financial information, has caused or is likely to cause substantial injury to consumers and small businesses in the form of fraud, identity theft, monetary loss, and time spent remedying the problem.

21. Dealership customers and consumers had no way of independently knowing about Respondent's security failures and could not reasonably have avoided possible harms from such failures.

22. Respondent could have prevented or mitigated these failures through readily available and relatively low-cost measures.

Gramm-Leach-Bliley Act

23. Respondent is a financial institution, as that term is defined by Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A), and is subject to the GLB Act, because, among other things, Respondent is significantly engaged in data processing for its customers, auto dealerships that extend credit to consumers. 12 C.F.R. § 225.28(b)(14). Respondent collects nonpublic personal information, as defined by 16 C.F.R. § 313.3(n), and is subject to the requirements of the GLB Safeguards Rule, 16 C.F.R. Part 314.

Safeguards Rule

24. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), was promulgated by the Commission on May 23, 2002, and became effective on May 23, 2003. The Rule requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing, implementing, and maintaining a comprehensive information security program that is written in one or more readily accessible parts, and that contains administrative, technical, and physical safeguards that are appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue, including:

a. Designating one or more employees to coordinate the information security program;

b. Identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks;

c. Designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures;

d. Overseeing service providers by requiring them by contract to protect the security and confidentiality of customer information; and

e. Evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

16 C.F.R. §§ 314.3 and 314.4. Violations of the Safeguards Rule are enforced through the FTC Act. 15 U.S.C. § 6805(a)(7).

25. Until at least June 2017, Respondent violated the Safeguards Rule. For example:

a. Respondent failed to develop, implement, and maintain a written information security program;

b. Respondent failed to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and failed to assess the sufficiency of any safeguards in place to control those risks; and

c. Respondent failed to design and implement basic safeguards and to regularly test or otherwise monitor the effectiveness of such safeguards' key controls, systems, and procedures.

VIOLATION OF THE FTC ACT

Count 1
Unfair Data Security Practices

26. As described in Paragraphs 11 to 22, Respondent's failure to employ reasonable measures to protect personal information caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

VIOLATION OF THE GLB SAFEGUARDS RULE

Count 2
Violation of the Safeguards Rule

27. Respondent is a financial institution, as defined in Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A).

28. As set forth in Paragraph 25a, Respondent failed to develop, implement, and maintain a written information security program.

29. As set forth in Paragraph 25b, Respondent failed to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and failed to assess the sufficiency of any safeguards in place to control those risks.

30. As set forth in Paragraph 25c, Respondent failed to design and implement basic safeguards and to regularly test or otherwise monitor the effectiveness of such safeguards' key controls, systems, and procedures.

31. Therefore, the conduct set forth in Paragraphs 28-30 is a violation of the Safeguards Rule, 16 C.F.R. Part 314.

32. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this third day of September 2019, has issued this complaint against Respondent.

By the Commission.

April J. Tabor
Acting Secretary

SEAL: