1723051

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

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,ton descm-1 (cl a)6 x.(on 2 (,tr)6 (hme)6 (dl a)6 e)6 (dl a)6 leittel a.4 (f)-a.4 (ac

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

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