

Complaint

IN THE MATTER OF

LIGHTYEAR DEALER TECHNOLOGIES, LLCCONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT AND THE STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION
RULE

Docket No. C-4687; File No. 172 3051
Complaint, September 3, 2019 – Decision, September 3, 2019

This consent order addresses LightYear Dealer Technologies, LLC's storage of personal information about more than 14 million consumers. The complaint alleges that Respondent has violated Section 5(a) of the Federal Trade Commission Act and the Standards for Safeguarding Customer Information Rule issued pursuant to Title I of the Gramm-Leach-Bliley Act by engaging in a number of unreasonable security practices that led to a hacker's unauthorized access of personal information about 12.5 million consumers. The consent order prohibits Respondent, and any business that Respondent controls directly, or indirectly, from transferring, selling, sharing, collecting, maintaining, or storing personal information unless it establishes and implements, and thereafter maintains, a comprehensive information security program that protects the security, confidentiality, and integrity of such personal information.

Participants

For the *Commission*: *Jamie Hine* and *Elisa Jillson*.

For the *Respondents*: *Andrew Berg, Greenberg Traurig, LLP* and *Craig A. Harris, Munsch Hardt Kopf & Harr, P.C.*

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.

Complaint

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;

Complaint

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.*,

Complaint

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

Complaint

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

Complaint

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

Complaint

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.

Decision and Order

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

By the Commission.

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), and the Federal Trade Commission’s 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.*

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission’s Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondent is LightYear Dealer Technologies, LLC, a Missouri limited liability company, also doing business as DealerBuilt, with its principal office or place of business at 2570 4th Street, SW, Suite A, Mason City, Iowa 50401.
2. The Commission has jurisdiction over the subject matter of this proceeding and over Respondent, and the proceeding is in the public interest.

Decision and Order

ORDER**Definitions**

For purposes of this Order, the following definitions apply:

- A. “Covered Incident” means any instance in which any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.
- B. “Personal Information” means individually identifiable information from or about an individual consumer, including: (a) a first and last name; (b) a home or other physical address; (c) an email address; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other government issued identification number; (g) a financial account number; (h) credit or debit card information; (i) a date of birth; and (j) a license plate, vehicle identification number, or key code.
- C. “Respondent” means LightYear Dealer Technologies, LLC, a limited liability company, also doing business as DealerBuilt, and its successors and assigns.

Provisions**I. Mandated Information Security Program**

IT IS ORDERED that Respondent, and any business that Respondent controls directly, or indirectly, shall not transfer, sell, share, collect, maintain, or store Personal Information unless it establishes and implements, and thereafter maintains, a comprehensive information security program (“Information Security Program”) that protects the security, confidentiality, and integrity of such Personal Information. To satisfy this requirement, Respondent must, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Information Security Program;
- B. Provide the written program and any evaluations thereof or updates thereto to Respondent’s board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for Respondent’s Information Security Program at least once every twelve (12) months and promptly after a Covered Incident;

Decision and Order

- C. Designate a qualified employee or employees to coordinate and be responsible for the Information Security Program;
- D. Assess and document, at least once every twelve (12) months and promptly following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of such information;
- E. Design, implement, maintain, and document safeguards that control for the internal and external risks Respondent identifies to the security, confidentiality, or integrity of Personal Information identified in response to sub-Provision I.D. Such safeguards shall also include:
 - 1. Training of all of Respondent's employees, at least once every twelve (12) months, on how to safeguard Personal Information;
 - 2. Technical measures to monitor all of Respondent's networks and all systems and assets within those networks to identify data security events, including unauthorized attempts to exfiltrate Personal Information from those networks;
 - 3. Data access controls for all databases storing Personal Information, including by, at a minimum, (a) restricting inbound connections to approved IP addresses, (b) requiring authentication to access them, and (c) limiting employee access to what is needed to perform that employee's job function;
 - 4. Encryption of all Social Security numbers and financial account information on Respondent's computer networks; and
 - 5. Policies and procedures to ensure that all devices on Respondent's network with access to Personal Information are securely installed and inventoried at least once every twelve (12) months.
- F. Assess, at least once every twelve (12) months and promptly following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results.

Decision and Order

- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly following a Covered Incident, and modify the Information Security Program based on the results. Such testing shall include vulnerability testing of Respondent's network once every four months and promptly after a Covered Incident, and penetration testing of Respondent's network at least once every twelve (12) months and promptly after a Covered Incident;
- H. Select and retain service providers capable of safeguarding Personal Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards for Personal Information; and
- I. Evaluate and adjust the Information Security Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Information Security Program. At a minimum, Respondent must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

II. Information Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision I of this Order titled Mandated Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

- A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Information Security Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney client privilege, statutory exemption, or any similar claim.
- B. For each Assessment, Respondent shall provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name and affiliation of the person selected to conduct the Assessment, which the Associate Director shall have the authority to approve in his sole discretion.

Decision and Order

- C. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each 2-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.
- D. Each Assessment must: (1) determine whether Respondent has implemented and maintained the Information Security Program required by Provision I of this Order, titled Mandated Information Security Program; (2) assess the effectiveness of Respondent's implementation and maintenance of sub-Provisions I.A-I; (3) identify any gaps or weaknesses in the Information Security Program; and (4) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by Respondent's management. The Assessment shall be signed by the Assessor and shall state that the Assessor conducted an independent review of the Information Security Program, and did not rely solely on assertions or attestations by Respondent's management.
- E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re LightYear Dealer Technologies, LLC, d/b/a DealerBuilt, FTC File No. 172 3051." All subsequent biennial Assessments shall be retained by Respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

III. Cooperation with Third Party Information Security Assessor

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with any Assessment required by Provision II of this Order titled Information Security Assessments by a Third Party, must disclose all material facts to the Assessor, and must not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Information Security Program required by Provision I of this Order, titled Mandated Information Security

Decision and Order

Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions I.A-I; or (3) identification of any gaps or weaknesses in the Information Security Program.

IV. Annual Certification

IT IS FURTHER ORDERED that, in connection with compliance with Provision I of this Order titled Mandated Information Security Program, Respondent shall:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's Information Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of a Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.
- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re LightYear Dealer Technologies, LLC, d/b/a DealerBuilt, FTC File No. 172 3051."

V. Covered Incident Reports

IT IS FURTHER ORDERED that Respondent, within a reasonable time after the date of Respondent's discovery of a Covered Incident, but in any event no later than ten (10) days after the date Respondent first notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;

Decision and Order

- C. A description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;
- D. The number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;
- E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of each materially different notice required by U.S. federal, state, or local law or regulation and sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, “In re LightYear Dealer Technologies, LLC, d/b/a DealerBuilt, FTC File No. 172 3051.”

VI. GLB Rule Violations

IT IS FURTHER ORDERED that Respondent, and Respondent’s officers, agents, employees and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, are hereby permanently restrained and enjoined from violating any provision of The Standards for Safeguarding Consumer Information Rule, 16 C.F.R. Part 314, appended hereto.

VII. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order.
- B. For twenty (20) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives with responsibilities related to the subject matter of the Order; and (3) any business

Decision and Order

entity resulting from any change in structure as set forth in Provision VIII of this Order titled Compliance Reports and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

- C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

VIII. Compliance Reports and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

- A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (1) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (2) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (4) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes Respondent made to comply with the Order; and (5) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; or (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the

Decision and Order

United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.

- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, “In re LightYear Dealer Technologies, LLC, d/b/a DealerBuilt, FTC File No. 172 3051.”

IX. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. Personnel records showing, for each person providing services, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. Copies or records of all consumer complaints concerning the subject matter of the Order, whether received directly or indirectly, such as through a third party, and any response;
- D. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, confidentiality, security, or integrity of any Personal Information, including any representation concerning a change in any website or other service controlled by Respondent that relates to the privacy, confidentiality, security, or integrity of Personal Information;
- E. For five (5) years after the date of preparation of each Assessment required by this Order, all materials and evidence that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of Respondents, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondents’ compliance with related Provisions of this Order, for the compliance period covered by such Assessment; and

Decision and Order

- F. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

X. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within ten (10) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XI. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate on September 3, 2039, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than twenty (20) years;
- B. This Order's application to any Respondent that is not named as a defendant in such complaint; and
- C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Analysis to Aid Public Comment

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission (“Commission”) has accepted, subject to final approval, an agreement containing a consent order from LightYear Dealer Technologies, LLC, also doing business as DealerBuilt (“Respondent”).

The proposed consent order (“proposed order”) has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement’s proposed order.

This matter involves DealerBuilt (“DealerBuilt”), a technology company that develops and sells dealer management system software and data processing services to automotive dealerships nationwide. Respondent has stored personal information about more than 14 million consumers.

The Commission’s proposed two-count complaint alleges that Respondent has violated Section 5(a) of the Federal Trade Commission Act and the Standards for Safeguarding Customer Information Rule (“Safeguards Rule”), issued pursuant to Title I of the Gramm-Leach-Bliley Act (“GLB”).

First, the proposed complaint alleges that Respondent has engaged in a number of unreasonable security practices that led to a hacker’s unauthorized access of personal information about 12.5 million consumers. During that breach, the hacker also downloaded the personal information of approximately 70,000 consumers, which was contained in the back-up directories of five DealerBuilt customers. The proposed complaint alleges that Respondent:

- failed to develop, implement, or maintain a written organizational information security policy;

Analysis to Aid Public Comment

- failed to implement reasonable guidance or training for employees or third-party contractors, regarding data security and safeguarding consumers' personal information;
- 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;
- 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;
- failed to impose reasonable data access controls, such as restricting inbound connections to known IP addresses, and requiring authentication to access backup databases;
- stored consumers' personal information on Respondent's computer network in clear text; and
- failed to have a reasonable process to select, install, secure, and inventory devices with access to personal information.

The proposed complaint alleges that Respondent could have addressed each of the failures described above by implementing readily available and relatively low-cost security measures.

The proposed complaint alleges that Respondent's failures 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. Such practice constitutes an unfair act or practice under Section 5 of the FTC Act.

Second, the proposed complaint alleges that Respondent violated the Safeguards Rule, which 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. The proposed complaint alleges that Respondent:

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

Analysis to Aid Public Comment

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

The proposed order contains injunctive provisions addressing the alleged unfair conduct in connection with Respondent's sale of dealer management system software and services. Part I of the proposed order prohibits Respondent, and any business that Respondent controls directly, or indirectly, from transferring, selling, sharing, collecting, maintaining, or storing personal information unless it establishes and implements, and thereafter maintains, a comprehensive information security program that protects the security, confidentiality, and integrity of such personal information.

Part II of the proposed order requires Respondent to obtain initial and biennial data security assessments for twenty years.

Part III of the agreement requires Respondent to disclose all material facts to the assessor and prohibits Respondent from misrepresenting any fact material to the assessments required by Part II.

Part IV requires Respondent to submit an annual certification from a senior corporate manager (or senior officer responsible for its information security program) that Respondent has implemented the requirements of the Order, is not aware of any material noncompliance that has not been corrected or disclosed to the Commission, and includes a brief description of any covered incident involving unauthorized access to or acquisition of personal information.

Part V requires Respondent to submit a report to the Commission of its discovery of any covered incident.

Part VI is a prohibition against violating GLB.

Parts VII through X of the proposed order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide information or documents necessary for the Commission to monitor compliance. Part XI states that the proposed order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order's terms.

Complaint

IN THE MATTER OF

**QUAKER CHEMICAL CORPORATION,
GLOBAL HOUGHTON LTD.,
GULF HOUGHTON LUBRICANTS LTD.,
AND
AMAS HOLDINGS SPF**

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT AND SECTIONS 7 AND 11 OF THE CLAYTON ACT

*Docket No. C-4681; File No. 171 0125
Complaint, July 23, 2019 – Decision, September 9, 2019*

This consent order addresses the \$172.5 million acquisition by Quaker Chemical Corporation of certain assets of Global Houghton LTD. The complaint alleges that the Transaction, if consummated, would violate Section 7 of the Clayton Act and that the asset purchase agreement constitutes a violation of Section 5 of the Federal Trade Commission Act by substantially lessening competition in the manufacture and sale of aluminum hot rolling oils (“AHRO”) and steel cold rolling oils (“SCRO”) in North America. The consent order requires Quaker to divest Houghton’s North American AHRO and SCRO product lines to Total S.A.

Participants

For the *Commission*: Steven Couper and Terry Thomas.

For the *Respondents*: Joanne Lewers, Drinker Biddle & Reath LLP; Scott Perlman, Mayer Brown LLP; Karen Kazmerzak and Timothy Muris, Sidley Austin LLP.

COMPLAINT

Pursuant to the provisions of the Federal Trade Commission Act (“FTC Act”), and by virtue of the authority vested in it by said Act, the Federal Trade Commission (“Commission”), having reason to believe that Respondent Quaker Chemical Corporation (“Quaker”) intends to acquire Global Houghton Ltd. (“Houghton”), in violation of Section 5 of the FTC Act, as amended, 15 U.S.C. § 45, and which, if the acquisition is consummated, may substantially lessen competition in violation of Section 7 of the Clayton Act, 15 U.S.C. § 18, and Section 5 of the FTC Act, and it appearing to the Commission that a proceeding by it in respect thereof would be in the public interest, hereby issues its complaint pursuant to Section 5(b) of the FTC Act, 15 U.S.C. § 45(b), and Section 11(b) of the Clayton Act, 15 U.S.C. § 21(b), stating its charges as follows:

I. RESPONDENTS

1. Respondent Quaker is a corporation organized, existing, and doing business under and by virtue of the laws of the Commonwealth of Pennsylvania with its executive offices and