



[BILLING CODE: 6750-01S]

FEDERAL TRADE COMMISSION

[File No. 172 3051]

DealerBuilt/LightYear Dealer Technologies; Analysis to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed consent agreement; request for comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order -- embodied in the consent agreement -- that would settle these allegations.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Interested parties may file comments online or on paper, by following the instructions in the Request for Comment part of the **SUPPLEMENTARY**

INFORMATION section below. Write: "DealerBuilt/LightYear Dealer Technologies;

File No. 172 3051" on your comment, and file your comment online at

<https://www.regulations.gov> by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address:

Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Jamie Hine (202-326-2188), Bureau

of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Home Page (for June 12, 2019), on the World Wide Web, at <https://www.ftc.gov/news-events/commission-actions>.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**. Write “DealerBuilt/LightYear Dealer Technologies; File No. 172 3051” on your comment. Your comment - including your name and your state - will be placed on the public record of this proceeding, including, to the extent practicable, on the <https://www.regulations.gov> website.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online through the <https://www.regulations.gov> website.

If you prefer to file your comment on paper, write “DealerBuilt/LightYear Dealer Technologies; File No. 172 3051” on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary,

600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580; or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website at <https://www.regulations.gov>, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential" – as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2) – including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and

must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the public FTC Website – as legally required by FTC Rule 4.9(b) – we cannot redact or remove your comment from the FTC Website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at <http://www.ftc.gov> to read this Notice and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]**. For information on the Commission’s privacy policy, including routine uses permitted by the Privacy Act, see <https://www.ftc.gov/site-information/privacy-policy>.

Analysis of Proposed 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 belonging to 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;
- 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 are 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 practices constitute 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;
- 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.

By direction of the Commission.

April J. Tabor,

Acting Secretary.

[FR Doc. 2019-12768 Filed: 6/14/2019 8:45 am; Publication Date: 6/17/2019]