Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of* LightYear Dealer Technologies, LLC d/b/a DealerBuilt**
File No. 1723051

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;

- 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;

- 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.