News Update on FTC's Application of Safeguards Rule to Software Company

News Update 7.17.19

FTC Puts Software Companies and Service Providers on Notice of Broad Enforcement Powers Under Gramm-Leach-Bliley Act Safeguards Rule

The Federal Trade Commission ("FTC") has put software companies and software service providers on notice it intends to interpret the Gramm-Leach-Bliley Act's Safeguards Rule broadly to apply to businesses which make available software or services that serve financial, payroll, and accounting purposes and collect sensitive data on consumers and their employees.

The FTC recently announced its settlement of a complaint filed against LightYear Dealer Technologies, LLC which does business as Dealerbuilt, which required Dealerbuilt as condition of the settlement to develop, implement and maintain an information security program that incorporates the minimum requirements specified by the FTC and submit to third party compliance assessments and annual certifications over a period of the

next 20 years.

The FTC's specified minimum requirements for Dealerbuilt's information security program included the following:

- Develop, implement, maintain and record in writing an Information Security Program;
- Make available the written program, evaluations of the program, and updates on the program, to the company's board of directors or governing body, or if none exists, the senior officer responsible for the program at least once per annual period and after any data breach;
- Identify an employee or employees responsible for the coordination of the program;
- Provide written assessment annually and after any data breach of any potential data breach risks;
- Develop written safeguards to ensure data security including the following:
    - Training of all employees at least once every annual period on how to protect personal information;
    - Technical measures monitoring networks, systems to identify attempted data breaches;
    - Access controls on databases containing personal information, which (a) restrict the ability to connect to only approved IP addresses; (b) require authentication to access the databases; and (c) limit the access of employees to only those databases as necessary to perform their duties;
    - Encrypt all social security numbers and financial account information;
    - Implement policies and procedures for secure installation and inventory on an annual basis
- Perform assessment annually and after any data breach of the sufficiency of safeguards and modify the program as necessary;
- Conduct test annually and after any data breach of

effectiveness of safeguards, which shall include vulnerability testing every four months and after a data breach, and annual penetration testing, as well as after any data breach;

- Ensuring that contracts with any service providers ensure compliance with safeguards; and
- Evaluate and make adjustments to program upon any changes to operations or business or in event of any data breach. or on an annual basis.

The FTC Order also mandates that an information security assessment be conducted initially and biennially by a third party professional approved by the Associate Director for Enforcement for the Bureau of Consumer Protection at the FTC, and that the assessor will be required to provide the documents relevant to the assessment to the FTC for review within 10 days following the completion of the initial review and then on demand. Furthermore, the Order requires the senior corporate manager or senior officer of Dealerbuilt to submit annual written certifications to the FTC, and that within a reasonable time following any discovery of a data breach, or at least 10 days following the provision of first notice of any data breach, Dealerbuilt must send a report to the FTC of any data breach, which meets certain specified requirements. Also, the Order permanently enjoins all individuals affiliated with Dealerbuilt from violating any provisions of the Safeguards Rule, and makes the Order applicable to all businesses connected to Dealerbuilt, which Dealerbuilt is to be broadly interpreted and Dealerbuilt is required to identify in detail via compliance reports, accompanied by sworn affidavits.

The FTC also imposes broad recordkeeping requirements on Dealerbuilt through the Order, requiring Dealerbuilt to create and retain for the next 20 years accounting records of all revenues collected, personnel records, consumer complaint records and responses to those records, and any documents

relied upon to prepare mandate assessments and to demonstrate full compliance with the order.

Finally, within 10 days of any request by the FTC, Dealerbuilt is required to furnish compliance reports to the FTC or other requested information accompanied by sworn affidavits.

The FTC announcement is attached **here** and the Order attached **here**.

What prompted this broad enforcement action by the FTC against DealerBuilt? According to the **FTC Complaint**, a series of security failures resulted in the breach of a backup database through a storage device beginning in late October 2016, which resulted in the breach of personal information of nearly Seventy Thousand consumers, which included full names and addresses, telephone numbers, social security numbers, drivers license numbers, and birthdates of consumers as well as wage and financial account information of dealership employees. The **FTC Complaint** further alleges that Dealerbuilt failed to detect the breach and only learned of it after a customer called its chief technology officer demanding to know why customer data was publicly available on the Internet.

The **FTC Complaint** alleged that Dealerbuilt was a financial institution as defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act, 15 U.S.C. Section 6809(3)(A) as a result of being "significantly engaged in data processing for its customers, auto dealerships that extend credit to customers." **The Complaint** alleged that the "failure to employ measures to protect personal information" constituted an "unfair act or practice" and that the failures to (a) "develop, implement, and maintain a written information security program"; (b) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information" and "assess the sufficiency of any safeguards in place to control those risks"; and (c) to design and implement basic safeguards and to regularly test or otherwise monitor

the effectiveness of such safeguards" constituted a violation of the Safeguards Rule and an unfair or deceptive act or practice in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

What should software companies and service providers take away from this FTC enforcement action? First and foremost, the FTC is making a definitive statement that if you are in the business of providing software or software services that have any sort of financial or accounting function to them, you are a financial institution for purposes of Gramm-Leach-Bliley and the Safeguards Rule is going to be deemed to apply to your business. Second, the FTC considers service providers accountable for the protection of any personal data they collect or store. Third, the FTC expects businesses using third party software or providers to have contracts in place with those software companies or service providers imposing security requirements, monitoring requirements, and explicitly requiring them to follow websites reporting on known vulnerabilities. Fourth, the FTC expects businesses to train and supervise employees on how to ensure the security of the company. The FTC specifically points businesses in its announcement to comply with its publication, **Start with Security: Lessons Learned from FTC Cases**.FTC Puts Software Companies and Service Providers on Notice of Broad Enforcement Powers Under Gramm-Leach-Bliley Act Safeguards Rule