102 3094

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
J. Thomas Rosch
Edith Ramirez
Julie Brill
Maureen K. Ohlhausen

In the Matter of **Franklin's Budget Car Sales, Inc., also dba Franklin Toyota/Scion,** **a corporation.**	**DOCKET NO. C-4371**

COMPLAINT

The Federal Trade Commission ("FTC" or "Commission"), having reason to believe that Franklin's Budget Car Sales, Inc., also dba Franklin Toyota/Scion ("Franklin Toyota" or "respondent") has violated Section 5(a) of the FTC Act, 15 U.S.C. § 45(a); the provisions of the Commission's Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Title V, Subtitle A of the Gramm-Leach-Bliley Act ("GLB Act") (codified at 15 U.S.C. §§ 6801-6809); and the Commission's Privacy of Customer Financial Information Rule ("Privacy Rule"), 16 C.F.R. Part 313, issued pursuant to the GLB Act; and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Franklin's Budget Car Sales, Inc., also dba Franklin Toyota/Scion ("Franklin Toyota") is a Georgia corporation with its registered address as P.O. Box 648, Statesboro, Georgia 30459 and its places of business at 500 Commerce Boulevard, Statesboro, Georgia 30458; 400 Northside Drive, Statesboro, Georgia 30458; and 733 Northside Drive East, Statesboro, Georgia 30459.

2. The acts and practices of respondent as alleged in this complaint are in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. Respondent Franklin Toyota is a franchise automobile dealership that sells both new and used automobiles, leases automobiles, provides repair services for automobiles, and sells automobile parts. In connection with its automobile sales, Franklin Toyota provides financing services to individual consumers.

4. Since at least 2001, respondent has disseminated, or caused to be disseminated, to consumers statements concerning Franklin Toyota's privacy and data security policies and practices, including, but not limited to the following:

> We restrict access to non public personal information about you to only those employees who need to know that information to provide products and services to you. We maintain physical, electronic, and procedural safe guards that comply with federal regulations to guard non public personal information.

Franklin Toyota Privacy Policy, attached as Exhibit A.

5. In conducting business, respondent routinely collects personal information from or about its customers, including, but not limited to names, Social Security numbers, addresses, telephone numbers, dates of birth, and drivers' license numbers (collectively, "personal information").

6. Respondent uses computer networks to conduct its business and collect consumer information. Among other things, it uses the networks to obtain an online credit application from consumers; obtain outside lead information; maintain customer automobile and payment records; and manage customer car sales records, finance, and insurance records.

7. Respondent did not provide its customers with annual privacy notices and did not provide a clear and conspicuous opt-out notice that accurately explains to its customers their rights to opt out of any sharing of nonpublic information with unaffiliated third parties.

RESPONDENT'S SECURITY PRACTICES

8. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computers and networks. Among other things, respondent failed to:

   a. Assess risks to the consumer personal information it collected and stored online;

   b. Adopt policies, such as an incident response plan, to prevent, or limit the extent of, unauthorized disclosure of personal information;

   c. Use reasonable methods to prevent, detect, and investigate unauthorized access to personal information on its networks, such as inspecting outgoing transmissions to the internet to identify unauthorized disclosures of personal information;

   d. Adequately train employees about information security to prevent unauthorized disclosures of personal information; and

e. Employ reasonable measures to respond to unauthorized access to personal information on its networks or to conduct security investigations where unauthorized access to information occurred.

9. As a result of the failures set forth in Paragraph 8, customers' personal information was accessed and disclosed on peer-to-peer ("P2P") networks by a P2P application installed on a computer that was connected to respondent's computer network.

10. Information for approximately 95,000 consumers, including, but not limited to, names, Social Security numbers, addresses, dates of birth, and drivers' license numbers ("customer files") was made available on a P2P network. Such information can easily be misused to commit identity theft and fraud.

11. Files shared to a P2P network are available for viewing or downloading by anyone using a computer that operates a compatible P2P application. Generally, a file that has been shared cannot be removed from P2P networks.

VIOLATIONS OF THE FTC ACT

12. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits unfair or deceptive acts or practices in or affecting commerce.

13. As set forth in Paragraph 4, respondent has represented, expressly or by implication, that it implements reasonable and appropriate measures to protect consumers' personal information from unauthorized access.

14. In truth and in fact, respondent did not implement reasonable and appropriate measures to protect consumers' personal information from unauthorized access. Therefore, the representation set forth in Paragraph 13 was, and is, false or misleading, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE SAFEGUARDS RULE

15. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) 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; (3) 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; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer

information; and (5) 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).

16. Respondent is a "financial institution" as that term is defined in Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A).

17. As set forth in Paragraph 8, respondent has failed to implement reasonable security policies and procedures, and has thereby engaged in violations of the Safeguards Rule, by, among other things:

    a. Failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information;

    b. Failing to design and implement information safeguards to control the risks to customer information and failing to regularly test and monitor them;

    c. Failing to investigate, evaluate, and adjust the information security program in light of known or identified risks;

    d. Failing to develop, implement, and maintain a comprehensive written information security program; and

    e. Failing to designate an employee to coordinate the company's information security program.

VIOLATION OF THE PRIVACY RULE

18. The Privacy Rule, which implements Section 503 of the GLB Act, 15 U.S.C. § 6803, requires financial institutions to provide customers, no later than when a customer relationship arises and annually for the duration of that relationship, "a clear and conspicuous notice that accurately reflects [the financial institution's] privacy policies and practices," including its security policies and practices. 16 C.F.R. § 313.4(a), 313.5(a)(1), 313.6(a)(8). In addition, the Privacy Rule requires financial institutions to provide reasonable means for its customers to opt out of the institution's sharing of nonpublic customer information to nonaffiliated third parties and provide opt-out notices to consumers. 16 C.F.R. § 313.7. Violations of the Privacy Rule are enforced through the FTC Act. 15 U.S.C. § 6805(a)(7).

19. As set forth in Paragraph 7, respondent failed to send consumers annual privacy notices and did not provide a mechanism by which consumers could opt out of information sharing with nonaffiliated third parties in violation of the Privacy Rule.

20. 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 FTC Act.

THEREFORE, the Federal Trade Commission this third day of October, 2012, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary