UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION

Franklin Toyota/Sdon, a corporation.	Docke N o. C-

COMPLAINT

The Federal Trade Commission ("FTC" or "Commission"), having eason to believe that Franklin's Budget Car Sales, ic., also dbar franklin Toyota/Scion ("Franklin Toyota" or "respondent") has violated Section 5(at) the FTC Act, 15 U.S.C. § 45(a); the optisions of the Commission's Standards for Saguarding 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 Prioracy Sustamer Financial Information Rule ("Privacy Rule"), 16 C.F.R. Part 313, issue/Sion ("Franklin")

Toyota") is a Georgia corporation with its reigntered aldress a P.O. Box 648, Statesboro, Gegia 30459 and its place of business at 500 Comme Boeulevard, Statesboro, Gegia 30458; 400 Northside Dive, Statesboro, Goegia 30458; and 733 Northside Dive East, Statesboro, Gregia 30459.

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

RESPONDENT'S BUSINESS FRACTICES

- automobile parts.nlconnetion with its automobile sales, finklin Toyota provides financing services to individual consumers.
- 4. Since at least 2001, respondent has dsseminated, or caused to be disseminated, to consumers statteents concreting Franklin Toyota's privacy and datasecuity 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.

aset tho

- d. Adequately train employees **b**out information seciting to prevent unauthorized disclosures of presonal information; and
- e. Employreasonable measures to respond to unauthorized access to personnal information on its networks or to conduce curity investigations where unauthorized access to information occurred.
- 9. As a result of the failure set forth in Pagraph 8, astomers' personal information was accessed ad disclosed on peeto-peer ("P2P") networks by a P2P application installed on a computer that was onnected to respondents' computer network.
- 10. Information for approximately 95,000 consumers, including, but not limited to, names, Social Securitynumbers, addesses, does of birth, and divers' license numbers ("customer files")was madeavailableon a P2P network. Such infortion can eaily be misused to committee tity theft and faud.
- 11. Files shaed to a P2P network available for viewing or downloading anyone using a compute that operties a ompatible P2P application. Gealty, a file that has been shared cannot be emoved from P2P networks.

VIOLATIONS OF THE FTC ACT

- 12. Section 5(a)of the FTC Act, 15 U.S.C. § 45(a), **o**hibits unfair or deeptive ats or practices in or affecting commerce
- 13. As set forth in Paggraph 4, espondent hearepesentel, expresslyor by implication, that it implements resonableand appropriate measures to protect consumed personal information from unauthorized access.
- 14. In truth and in fatic respondent did not implement sea able ad appropriate measures to protect onsumers' presonal information from unauthorized acess. Threefore, the representation set forth in Parargph 13 was, and is, flae 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 Safguards Rule, white implements Section 501(b) of the BS Act, 15 U.S.C. § 6801(b), equires financial institutions to protect the secuty, confidentiality, and integrity of customerinformation bydeveloping competensivewritten information security program that ontains reasonable aministrative, technical, and physical safeguards, including(1) designating one or more employees to coordinate the information secrity program; (2) identifying reasonably foreseeable internal and external risks to the secityr, confidentiality, and integrity of customerinformation, and assessing the sufficiency of any safeguards in place to control those sks; (3) designing and implementing information safeguards to control the risks identified through risk

assessment, and gularly testing or otherwise monitoring the efectiveness of the safeguards'key controls, systems, and procdures; (4) overseeing service providers and requiring them by contract to protect the secuty and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring thanges to the business opacion, and other relevant droumstances. 16 C.F.R. §§ 314.3 and 314.4. Violations of the Safeguards Rule are enforced though the FTC Act. 15 U.S.C. § 6805(a)).

- 16. Respondent is a iffancial institution" as that term is definition Section 509(3)(A) for 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 proædures, and has the by engaged in violations of the Sagrands Rule, by, among other things:
 - a. Failing to identify reasonably for esee ble internal and external risks to the security, confidentiality, and integrity of custome information;
 - b. Failing to design and implement information segulards to contrible 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 corepensive written information searity program; and
 - e. Failing to designate an employee to coordinate the companys information security program.

VIOLATION OF THE PRIVACY RULE