Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Franklin Budget Car Sales, Inc., File No. 102 3094

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Franklin's Budget Car Sales, Inc., also doing business as Franklin Toyota/Scion ("Franklin Toyota").

The proposed consent 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.

The Commission's proposed complaint alleges that Franklin Toyota, a Georgia corporation, 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 also provides financing services to individual consumers. The complaint alleges that In the course of its business, Franklin Toyota 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. The complaint alleges that Franklin Toyota is a "financial institution" as defined in the Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. § 6801 et seq.

According to the complaint, Franklin Toyota engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computers and networks. In particular, Franklin Toyota failed to: (1) assess risks to the consumer personal information it collected and stored online; (2) adopt policies, such as an incident response plan, to prevent, or limit the extent of, unauthorized disclosure of personal information; (3) 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; (4) adequately train employees about information security to prevent unauthorized disclosures of personal information; and (5) 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.

The complaint alleges that as a result of these failures, Franklin Toyota customers' personal information was accessed and disclosed on peer-to-peer ("P2P") networks by a P2P application installed on a computer connected to Franklin Toyota's computer network. The complaint alleges that information for approximately 95,000 consumers, including but not limited to consumers' names, Social Security numbers, addresses, dates of birth, and drivers' license numbers, was made available on a P2P network. Such information can easily be used to facilitate identity theft and fraud.

Files shared to a P2P network are available for viewing or downloading by anyone using

a personal computer with access to the network. Generally, a file that has been shared cannot be permanently removed from P2P networks.

In fact, the use of P2P software poses very significant data security risks to consumers. A 2010 FTC examination of P2P-related breaches uncovered a wide range of sensitive consumer data available on P2P networks, including health-related information, financial records, and drivers' license and social security numbers. *See Widespread Data Breaches Uncovered by FTC Probe: FTC Warns of Improper Release of Sensitive Consumer Data on P2P File-Sharing Networks* (Feb. 22, 2010), http://www.ftc.gov/opa/2010/02/p2palert.shtm. Files shared to a P2P network are available for viewing or downloading by any computer user with access to the network. Generally, a file that has been shared cannot be removed permanently from the P2P network. In addition, files can be shared among computers long after they have been deleted from the original source computer.

According to the complaint, Franklin Toyota violated the GLB Safeguards Rule by, among other things, failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; design and implement information safeguards to control the risks to customer information and failing to regularly test and monitor them; investigate, evaluate, and adjust the information security program in light of known or identified risks; develop, implement, and maintain a comprehensive written information security program; and designate an employee to coordinate the company's information security program.

In addition, the proposed complaint alleges that Franklin Toyota misrepresented that it implements reasonable and appropriate measures to protect consumers' personal information from unauthorized access, in violation of Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a). Furthermore, the proposed complaint alleges that Franklin violated the GLB Privacy Rule by failing to send consumers annual privacy notices and by failing to provide a mechanism by which consumers could opt out of information sharing with nonaffiliated third parties.

The proposed order contains provisions designed to prevent Franklin Toyota from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits misrepresentations about the privacy, security, confidentiality, and integrity of any personal information collected from or about consumers. Part II of the proposed order prohibits Franklin Toyota from violating any provision of the GLB Act's Standards for Safeguarding Consumer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, or the GLB Act's Privacy of Consumer Financial Information Rule ("Privacy Rule"), 16 C.F.R. Part 313. Part III requires Franklin Toyota to establish, implement, and thereafter maintain a comprehensive information security program, including the designation of an employee to oversee Franklin Toyota's security program, employee training, and implementation of reasonable safeguards. Part IV of the order requires Franklin Toyota to obtain, for a period of twenty years, biennial assessments of its information security program from an independent third-party professional possessing certain credentials or certifications.

Parts V through IX of the proposed order are reporting and compliance provisions. Part V requires Franklin Toyota to retain documents relating to its compliance with the order. For most records, the order requires that the documents be retained for a five-year period. For the third party assessments and supporting documents, Franklin Toyota must retain the documents for a period of three years after the date that each assessment is prepared. Part VI requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VII ensures notification to the FTC of changes in corporate status. Part VIII mandates that Franklin Toyota submit a compliance report to the FTC within 90 days, and periodically thereafter as requested. Part IX is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.