

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 with its automob

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 information stored on 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 on 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 t

