

Complaint

IN THE MATTER OF

FRANKLIN'S BUDGET CAR SALES, INC.
DBA
FRANKLIN TOYOTA/SCION

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT AND THE
GRAMM-LEACH-BLILEY ACT

Docket No. C-4371; File No. 102 3094
Complaint, October 3, 2012 – Decision, October 3, 2012

This consent order addresses Franklin's Budget Car Sales, Inc.'s practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computers and networks. The 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; and violated the Gramm-Leach-Bliley 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 consent order prohibits Franklin Toyota from violating any provision of the Gramm-Leach-Bliley Act's Standards for Safeguarding Consumer Information Rule ("Safeguards Rule") and making misrepresentations about the privacy, security, confidentiality, and integrity of any personal information collected from or about consumers.

Participants

For the *Commission*: Karen Jagielski.

For the *Respondent*: Michael A. Goodman, Hudson Cook, LLP.

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. §§

Complaint

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.

Complaint

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

Complaint

- 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

Complaint

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;

Complaint

- 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.

Complaint

Exhibit A**Notice Applied to**

Franklin Chevrolet Co., Inc. (also as Franklin Chevrolet Cadillac Buick Pontiac GMC and Franklin Toyota, Inc.) Here in referred to as Franklin Auto Group.

Franklin Auto Group is committed to respecting the individual privacy of its customers. In accordance with federal regulations, vehicle financial activity in automobile dealerships leasing, credit sales and insurance product sales would likely be considered financial activities. Therefore because the Gramm, Leach, Bliley Act (GLB Act) requires a privacy notice the following notice is provided:

Privacy Notice

In connection with your transaction Franklin Auto Group may obtain information about you as described in this notice, which we handle as stated in this notice.

1. We collect non public personal information about you from the following sources:
 - a. Information we receive from your application and other forms.
 - b. Information about your transactions with our affiliates and others; and
 - c. Information we receive from credit reporting agencies.
2. We may disclose all the information we collect, as described above to auto manufacturers/ distributors that we have franchises with and companies that perform marketing services or other functions on our behalf or to other financial institutions with whom we have joint marketing agreements. We may make disclosures about you as a consumer, a customer, or a former customer. We do not sell list of our customers or otherwise make that information available to nonaffiliated third parties except as described above.
3. We may also disclose non public personal information about you as a consumer, a customer or a former customer, as provided by law.
4. 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.
5. We do not provide for an opt-out due to agreements made in items 2, 3, & 4 above where the disclosure is necessary to process or service a transaction for you the consumer therefore not required. Any questions may be directed to 1-800-684-6348.

Consumer acknowledgment: I (we) acknowledge that I (we) received a copy of this notice on the date indicated below.

Customer Signature

Date

Customer Name Printed

Co-Customer Signature

Date

Co-Customer Name Printed

Franklin 00134

Decision and Order

DECISION AND ORDER

The Federal Trade Commission (“Commission” or “FTC”), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft of complaint, which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the respondent with violations of Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45, the Standards for Safeguarding Consumer Information Rule (“Safeguards Rule”), 16 C.F.R. Part 314, and the Privacy of Consumer Financial Information Rule (“Privacy Rule”), 16 C.F.R. Part 313;

The respondent, its attorney, and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of the agreement is for settlement purposes only and does not constitute an admission by the respondent that the law has been violated as alleged in such complaint, or that any of the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, the Safeguards Rule, and the Privacy Rule, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comment received from an interested person pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:

1. Respondent Franklin's Budget Car Sales, Inc., also dba Franklin Toyota/Scion is a Georgia corporation with

Decision and Order

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 Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER DEFINITIONS

For purposes of this order, the following definitions shall apply:

- A. Unless otherwise specified, “respondent” shall mean Franklin’s Budget Car Sales, Inc., also dba Franklin Toyota/Scion, its successors and assigns, and each of their successors and assigns.
- B. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) date of birth; (c) home or other physical address, including street name and name of city or town; (d) email address or other online contact information, such as an instant-messaging user identifier or a screen name that reveals an individual’s email address; (e) telephone number; (f) driver’s license number; (g) financial account information; (h) Social Security number; (i) credit or debit card information, including card number, expiration date, and security code; (j) persistent identifier, such as a customer number held in a “cookie” or processor serial number; and (k) any information that is combined with any of (a) through (j) above.
- C. “Commerce” shall mean “commerce” as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

Decision and Order

- D. All other terms are synonymous in meaning and equal in scope to the usage of such terms in the Gramm-Leach-Bliley Act (codified at 15 U.S.C. § 6801 *et seq*) (“GLB Act”).

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or indirectly, or through any corporation, subsidiary, division, website or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, is prohibited from misrepresenting in any manner, expressly or by implication, the extent to which respondent maintains and protects the privacy, confidentiality, or security of any personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that respondent and its officers, agents, representatives, and employees, shall not, directly or indirectly, or through any corporation, subsidiary, division, website, or other device, violate 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.

In the event that the Safeguards Rule or Privacy Rule is hereafter amended or modified, respondent’s compliance with these Rules as so amended or modified shall not be a violation of this order.

III.

IT IS FURTHER ORDERED that respondent, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content

Decision and Order

and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. The designation of an employee or employees to coordinate and be accountable for the information security program;
- B. The identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;
- C. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- D. The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and
- E. The evaluation and adjustment of respondent's information security program in light of the results of

Decision and Order

the testing and monitoring required by sub-part C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

IV.

IT IS FURTHER ORDERED that, in connection with its compliance with the Safeguards Rule and Part III of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. Set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. Explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers;
- C. Explain how the safeguards that have been implemented meet or exceed the protections required by the Part III of this order; and

Decision and Order

- D. Certify that respondent's information security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, initial and biennial Assessments shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line "In re Franklin's Budget Car Sales, Inc., FTC File Number 1023094." *Provided, however*, that, in lieu of overnight courier, Assessments may be sent by first-class mail, but only if an electronic version of such Assessments is contemporaneously sent to the Commission at DEBrief@ftc.gov.

V.

IT IS FURTHER ORDERED that respondent shall maintain and, upon request, make available to the Commission for inspection and copying:

- A. For a period of five (5) years, a print or electronic copy of each document relating to compliance, including but not limited to documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. For a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the

Decision and Order

Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts II and III of this order, for the compliance period covered by such Assessment.

VI.

IT IS FURTHER ORDERED that for a period of five (5) years from the date of entry of this Order, respondent shall deliver copies of the Order as directed below:

- A. Respondent must deliver a copy of this Order to (1) all current and future principals, officers, directors, and managers, (2) all current and future employees, agents and representatives who engage in conduct related to the subject matter of the Order, and (3) any business entity resulting from any change in structure set forth in Part VII. For current personnel, delivery shall be within five (5) days of service of this Order. For new personnel, delivery shall occur prior to them assuming their responsibilities. For any business entity resulting from any change in structure set forth in Part VII, delivery shall be at least ten (10) days prior to the change in structure.
- B. Respondent must secure a signed and dated statement acknowledging receipt of this Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this section.

VII.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to

Decision and Order

this order; the proposed filing of a bankruptcy petition; or a change in respondent's name or address. *Provided, however,* that, with respect to any proposed change in the entity about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line "In re Franklin's Budget Car Sales, Inc., FTC File Number 1023094." *Provided, however,* that, in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of such notices is contemporaneously sent to the Commission at DEBrief@ftc.gov.

VIII.

IT IS FURTHER ORDERED that respondent and its successors and assigns, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, respondent shall submit additional true and accurate written reports. Unless otherwise directed by a representative of the Commission, each report required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line "In re Franklin's Budget Car Sales, Inc., FTC File Number 1023094." *Provided, however,* that, in lieu of overnight courier, reports may be sent by first-class mail, but only if an electronic version of such reports is contemporaneously sent to the Commission at DEBrief@ftc.gov.

Analysis to Aid Public Comment

IX.

This order will terminate on October 3, 2032, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in less than twenty (20) years;
- B. This order's application to any respondent that is not named as a defendant in such complaint; and
- C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

**ANALYSIS OF CONSENT ORDER TO AID PUBLIC
COMMENT**

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").

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

**EPN, INC.
D/B/A
CHECKNET, INC.**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT

*Docket No. C-4370; File No. 112 3143
Complaint, October 3, 2012 – Decision, October 3, 2012*

This consent order addresses EPN, Inc.'s allowing an EPN employee to install a P2P application on her desktop computer, which was connected to EPN's computer network, resulting in two files containing personal information about a client's customers being made available on a P2P network. The complaint alleges that EPN violated of Section 5(a) of the Federal Trade Commission Act by failing to employ reasonable and appropriate measures to prevent unauthorized access to personal information which caused, or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. The consent order prohibits misrepresentations about the privacy, security, confidentiality, and integrity of any personal information collected from or about consumers.

Participants

For the *Commission*: Karen Jagielski, Jessica Lyon, and Manas Mohapatra.

For the *Respondent*: Amy Purcell and Scott Vernick, Fox Rothschild LLP.

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that EPN, Inc., d/b/a Checknet Inc. ("EPN") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent EPN is a Utah corporation with its principal office or place of business at 746 East 1910 South, Suite 3, Provo, UT 84606.