

Complaint

IN THE MATTER OF

**PREMIER CAPITAL LENDING, INC.,
AND
DEBRA STILES**CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS
OF SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT*Docket C-4241; File No. 072 3004**Complaint, December 10, 2008 – Decision, December 10, 2008*

This consent order addresses failures by Premier Capital Lending, Inc. (PLC) and Debra Stiles to provide reasonable and appropriate safeguards to protect personal information, as well as false or misleading representations respondents made about the security provided for such information. The order prohibits the respondents from misrepresenting the extent to which PLC maintains and protects the privacy, confidentiality, or security of personal information from or about consumers. The order requires the respondents to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to respondents' size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. The respondents are required not to violate any provision of the Gramm-Leach-Bliley Act Safeguards Rule and Privacy Rule. The order requires that the respondents obtain periodic assessments and reports from a qualified, objective, independent third-party professional, certifying, among other things, that PCL has in place a security program that provides protections that meet or exceed the protections required by the order and that PCL's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information is protected. Other provisions require the respondents to retain documents relating to their compliance with the order and to disseminate the order to persons with responsibilities relating to the subject matter of the order. The order requires Stiles to notify the Commission of changes in her business or employment in connection with providing financial products and services. The respondents must also notify the FTC of changes in PCL's corporate status and submit periodic compliance reports.

Complaint

Participants

For the *Commission*: *Laura Berger, Kandi Parsons, Jessica Rich, and Joel Winston.*

For the *Respondents*: *Not represented by counsel.*

COMPLAINT

The Federal Trade Commission (“FTC” or “Commission”), having reason to believe that Premier Capital Lending, Inc. and Debra Stiles have violated 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”), 15 U.S.C. § 6801-6809; the Commission’s Privacy of Consumer Financial Information Rule (“Privacy Rule”), 16 C.F.R. Part 313, issued pursuant to the GLB Act; and Section 5 of the FTC Act, 15 U.S.C. § 45(a), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Premier Capital Lending, Inc. (“PCL”), is a Texas corporation with its principal place of business at 901 W. Bardin Road, Suite 200, Arlington, Texas 76017.

2. Respondent Debra Stiles (“Stiles”) is a co-owner of PCL, Secretary of the company, and Manager of PCL’s headquarters office in Arlington, Texas. Individually, or in concert with others, she formulates, directs, or controls the policies, acts, or practices of PCL, including the acts or practices alleged in this complaint. Her principal office or place of business is the same as PCL’s.

3. PCL is a mortgage lender that specializes in loans to fund the combined purchase by consumers of real estate and manufactured homes. As a lender, PCL routinely obtains sensitive personal information related to its customers and potential

Complaint

customers, including the credit histories or consumer reports for these consumers.

RESPONDENTS' COURSE OF CONDUCT

4. As part of its process for evaluating consumer applicants for mortgage loans, PCL routinely obtains consumer reports from a consumer reporting agency ("CRA"). Under its agreement with the CRA, PCL obtains the consumer reports using an online portal through which authorized PCL employees can request the reports; PCL, in turn, issues each such employee a set of credentials, composed of a user name and password (together, a "CRA login"), with which the employee can log into a personal user portal within PCL's account. Stiles is an administrator of PCL's account, who enables and disables PCL's CRA logins.

5. Once logged into a user portal, a PCL employee requests a consumer report by entering a consumer name, address, and Social Security number ("SSN") into an online form that is transmitted to the CRA. New consumer reports are delivered to an "inbox" within the employee's user portal and, once they are opened, remain accessible to the employee for a period of at least 90 days, via links found in a "Report List" within the user portal. Each employee's Report List includes the name, address, and full SSN used to request the consumer report, as well as a link to the report that was obtained.

6. Stiles, as an administrator of PCL's account with the CRA, is able to review various management reports summarizing consumer report requests made through PCL's account. Among other things, Stiles can review: a chronological list of all consumer report requests made by PCL employees within the preceding 90 days, including the name of the employee who requested the report and the name, address, and SSN used to make the request (a "request list"); a request list limited to requests made using the CRA login of a particular PCL employee; and a request list showing requests made using a particular CRA login

Complaint

during a limited time period, *e.g.*, “Today,” “Yesterday,” “Week to Date,” “Month to Date,” “Last Week,” and “Last Month.” Each of these reports also permits review of the actual consumer reports requested (via a link next to the consumers’ names). PCL incurs no charge for accessing any of these management reports.

7. PCL receives monthly invoices from the CRA that list the requests for which PCL is being billed and include the user name of the employee who made each request, as well as the name of the consumer and the final four digits of the SSN that were used to make the request.

8. In March 2006, Stiles activated a CRA login under PCL’s credentials for the principal of a seller of manufactured homes based elsewhere in the state. The purpose of this arrangement was to enable the seller to access consumer reports from his own workplace for prospective home purchasers that could be referred to PCL for loans. Neither Stiles nor any agent nor employee of PCL visited the seller’s workspace or audited the computer network on which he used the PCL-issued CRA login, in order to assess that network’s vulnerability to attack by a hacker or other unauthorized user. Further, PCL failed to take reasonable steps to assess the seller’s procedures to handle, store, or dispose of personal information. In addition, in the five months that the CRA login issued to the seller was operational, PCL never conducted, or directed the seller to conduct, an inventory of the seller’s computer to determine what personal information related to PCL’s customers was stored there.

9. Working from a computer located in his office, the seller used the CRA login issued to him by Stiles from March through late July 2006. During those five months, he requested and obtained consumer reports on 83 consumers.

Complaint

THE BREACH

10. In or around July 2006, an unauthorized person hacked into the seller's computer and obtained his PCL-issued CRA login. Over the course of about eight days, the hacker used such CRA login to request and obtain 317 new consumer reports on individuals who were not customers of PCL nor the seller. The hacker's requests combined consumers' accurate names and addresses with a suspect series of SSNs, the vast majority of which consisted largely of sequential and repeated numbers, with the final four digits identical (*e.g.*, 866-66-6666).

11. By using the CRA login issued to the seller by PCL, the hacker also gained unrestricted access to all of the 83 consumer reports that had been obtained by the seller for his customers, links to which were stored in his user-portal Report List, together with a list of the name, address, and 9-digit SSN for each of those 83 consumers.

RESPONDENTS' RESPONSE TO THE BREACH

12. PCL learned of the breach on July 25, 2006, after two consumers contacted PCL to ask why their consumer reports had been requested by PCL, a company with which the consumers had no relationship. After confirming that the requests were unauthorized, PCL terminated the seller's CRA login and notified law enforcement authorities and the CRA, which in turn notified the three nationwide CRAs. In August 2006, PCL mailed breach notification letters to the 317 noncustomers whose reports the hacker had obtained.

13. Due to the format of the user portal provided to PCL's users, the "Report List" showing (and providing a link to) the 83 consumer reports requested by the seller was clearly visible to the hacker. However, PCL failed to recognize that the hacker had access to those 83 consumer reports until August 2007, more than

Complaint

a year after the breach. In September 2007, PCL mailed breach notification letters to these additional 83 consumers.

RESPONDENTS' SECURITY PRACTICES

14. From at least March 2006 until August 2007, respondents have engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumers' personal information. Among other things, respondents have failed to:

- a. assess the risks of allowing a third party to access consumer reports through PCL's account;
- b. implement reasonable steps to address these risks by, for example, evaluating the security of the third party's computer network and taking steps to ensure that appropriate data security measures were present;
- c. conduct reasonable reviews of consumer report requests made on PCL's account, using readily available information (such as management reports or invoices) for signs of unauthorized activity, such as spikes in the number of requests made on the account or made by particular PCL users or blatant irregularities in the information used to make the requests; and
- d. assess the full scope of consumer report information stored and accessible through PCL's account and, thus, compromised by the hacker.

15. The acts and practices of respondents as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

Complaint

VIOLATIONS OF SAFEGUARDS RULE

16. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), was promulgated by the Commission on May 23, 2002, and took effect on May 23, 2003. The Rule 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, 314.4.

17. PCL is a "financial institution," as that term is defined in Section 509(3)(A) of the GLB Act, and is therefore subject to the requirements of the Safeguards Rule.

18. As set forth in **paragraphs 8-11** and **13-14**, respondents have failed to implement reasonable and appropriate security policies and procedures and thereby have 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, and

Complaint

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

VIOLATION OF THE FTC ACT

19. Since at least 2006, respondents have disseminated or caused to be disseminated to consumers privacy policies and statements, including but not limited to the following statement from PCL's Privacy Policy:

We take our responsibility to protect the privacy and confidentiality of customer information very seriously. We maintain physical, electronic, and procedural safeguards that comply with federal standards to store and secure information about you from unauthorized access, alteration and destruction. Our control policies, for example, authorize access to customer information only by individuals who need access to do their work.

20. Through the means described in **paragraph 19**, respondents have represented, expressly or by implication, that they implement reasonable and appropriate measures to protect consumers' personal information from unauthorized access.

21. In truth and in fact, as set forth in **paragraphs 8-11** and **13-14**, respondents have not implemented reasonable and appropriate measures to protect consumers' personal information from unauthorized access. Therefore the representation set forth in **paragraph 20** was, and is, false or misleading, in violation of Section 5(a) of the FTC Act.

Complaint

VIOLATION OF THE PRIVACY RULE

22. The Privacy Rule, which implements Section 503(a) of the GLB Act, 15 U.S.C. § 6803(a), requires a financial institution to “provide a clear and conspicuous notice that accurately reflects [its] privacy policies and practices” to its customers. 16 C.F.R. § 313.4.

23. As set forth in **paragraphs 19-20**, respondents disseminated a privacy policy that has contained false or misleading statements regarding the measures it implemented to protect customers’ personal information. Therefore, respondents have disseminated a privacy policy that does not reflect accurately its privacy policies and practices, including its security policies and practices, in violation of the Privacy Rule.

24. The acts and practices of respondents 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 tenth day of December, 2008, has issued this complaint against respondents.

By the Commission.

Decision and Order

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the respondents named in the caption hereof, and the respondents having been furnished thereafter with a copy of a draft Complaint, which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the respondents with violation of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* and the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.*; and

The respondents and counsel for the Commission, having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), including an admission by the respondents 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 respondents 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 respondents have violated the said Acts, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comment, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings, and enters the following Order:

Decision and Order

1. Respondent Premier Capital Lending, Inc. (“PCL”) is a Texas Corporation with its principal place of business at 901 W. Bardin Road, Suite 200, Arlington, Texas 76017.

2. Respondent Debra Stiles (“Stiles”) is a co-owner of PCL, Secretary of the company, and Manager of its headquarters office in Arlington, Texas. Individually or in concert with others, she formulates, directs, or controls the policies, acts, or practices of respondent PCL. Her principal place of business is the same as PCL’s.

ORDER**DEFINITIONS**

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

1. “Personally identifiable information” or “personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an 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; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and security code; (g) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any information that is combined with any of (a) through (g) above.
2. “Gramm-Leach-Bliley Act” or “GLB Act” refers to 15 U.S.C. §§ 6801-6809, as amended, the “Safeguards Rule”

Decision and Order

or the “Standards for Safeguarding Customer Information Rule” refers to 16 C.F.R. Part 314, issued pursuant to Title V, Subtitle A of the GLB Act, 15 U.S.C. §§ 6801-6809, and the “Privacy Rule” or the “Commission’s Privacy of Consumer Financial Information Rule” refers to 16 C.F.R. Part 313, issued pursuant to the GLB Act.

3. “Financial institution” shall mean as defined in Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A).
4. Unless otherwise specified, “respondents” shall mean Premier Capital Lending, Inc. and its subsidiaries, divisions, affiliates, successors and assigns (“PCL”), and Debra Stiles.
5. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondents, and their officers, agents, representatives, and employees, shall not directly 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, misrepresent in any manner, expressly or by implication, the extent to which respondents maintain and protect the privacy, confidentiality, or security of any personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that respondents, and their officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device, no later than the date of service of this order, shall

Decision and Order

establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of consumers' personal information. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent PCL'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 failure;
- 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

Decision and Order

respondents and requiring service providers by contract to implement and maintain appropriate safeguards; and

- E. the evaluation and adjustment of respondents' information security program in light of the results of the testing and monitoring required by subpart C, any material changes to respondents' operations or business arrangements, or any other circumstances that respondents know or have reason to know may have a material impact on the effectiveness of their information security program.

III.

IT IS FURTHER ORDERED that respondents, and their officers, agents, representatives, and employees, shall not, directly or through any corporation, subsidiary, division, website, or other device, violate any provision of:

- A. the Safeguards Rule, 16 C.F.R. Part 314; or
- B. the Privacy Rule, 16 C.F.R. Part 313.

In the event that either of these Rules is hereafter amended or modified, respondents' compliance with that Rule as so amended or modified shall not be a violation of this order.

IV.

IT IS FURTHER ORDERED that, in connection with their compliance with Parts II and III.A. of this order, respondents, and their officers, agents, representatives, and employees, shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional using procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (A) the first one hundred and eighty (180) days after service of the order for

Decision and Order

the initial Assessment; and (B) 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 PCL has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent PCL's size and complexity, the nature and scope of respondent PCL's 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 Safeguards Rule; and
- D. certify that respondent PCL's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biennial reports, 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 by: 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.

Respondents shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection,

Decision and Order

Federal Trade Commission, Washington, D.C. 20580, within ten (10) business days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondents until three years after completion of the final Assessment and provided to the Associate Director of Enforcement upon request within ten (10) business days after respondents receives such request.

V.

IT IS FURTHER ORDERED that respondents shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including by not limited to:

- A. for a period of five (5) years:
 - 1. any documents, whether prepared by or on behalf of either respondent, that contradict, qualify, or call into question respondents' compliance with this order;
 - 2. consumer complaints (whether received in written or electronic form, directly, indirectly or through any third party), and any responses to those complaints, whether in written or electronic form, that relate to respondents' activities as alleged in the draft Complaint and respondents' compliance with the provisions of this order;
 - 3. copies of all subpoenas and other communications with law enforcement entities or personnel, whether in written or electronic form, if such documents bear in any respect on respondents' collection, maintenance, or furnishing of consumer reports or other personal information of consumers; and

Decision and Order

4. all records and documents necessary to demonstrate full compliance with each provision of 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 Assessment, whether prepared by or on behalf of either 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 respondents' compliance with Parts II and III.A. of this order, for the compliance period covered by such Assessment. Respondents shall provide such documents to the Associate Director of Enforcement within ten (10) days of request.

VI.

IT IS FURTHER ORDERED that respondents shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondents shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

IT IS FURTHER ORDERED that respondent Stiles, for a period of ten (10) years after the date of issuance of the order, shall notify the Commission of the discontinuance of her current business or employment or of her affiliation with any new business or employment that provides financial products or services. The notice shall include respondent Stiles' new business address and telephone number and a description of the nature of the business or employment and her duties or responsibilities. All

Decision and Order

notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VIII.

IT IS FURTHER ORDERED that respondents shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) 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 corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation(s) about which respondents learn fewer than thirty (30) days prior to the date such action is to take place, respondents shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

IX.

IT IS FURTHER ORDERED that respondents shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which they have complied with this order.

Decision and Order

X.

This order will terminate on December 10, 2028, or twenty (20) years from the most recent date that the United States or the 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 fewer 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(s) did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent(s) 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 to Aid Public Comment

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

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Premier Capital Lending, Inc., and Debra Stiles (collectively, “respondents”).

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.

According to the Commission’s proposed complaint, Premier Capital Lending, Inc. (“PCL”) is a mortgage lender headquartered in Arlington, Texas that specializes in loans to fund the combined purchase by consumers of real estate and manufactured homes. Debra Stiles (“Stiles”) is a co-owner of PCL and has authority to control its policies, acts, or practices, including those acts or practices alleged in the proposed complaint. As a lender, PCL routinely obtains sensitive personal information pertaining to its customers and potential customers (hereinafter “personal information”), including the credit histories or consumer reports for these consumers. This matter concerns alleged failures by respondents to provide reasonable and appropriate safeguards to protect personal information, as well as false or misleading representations respondents made about the security provided for such information.

According to the proposed complaint, PCL obtains consumer reports from a consumer reporting agency (“CRA”) via an online portal, which each authorized PCL employee logs into using personalized credentials (hereinafter, a “CRA login”). Once logged into the portal, PCL employees request a consumer report by

Analysis to Aid Public Comment

entering a consumer's name, address, and Social Security number ("SSN") into an online form that is transmitted to the CRA. Consumer reports are delivered to an "inbox" within the employee's portal and, once opened, remain accessible to the employee for at least 90 days. Stiles enables and disables PCL's CRA logins, and can review, at no cost, all consumer reports received by PCL employees, as well as various management reports that summarize consumer report requests made on PCL's account. PCL also receives monthly invoices from the CRA that list the requests for which PCL is being billed, including the user name of the employee who made the request, as well as the consumer name and final four digits of the SSN that were used to make the request.

In March 2006, Stiles activated a CRA login under PCL's credentials for the principal of a seller of manufactured homes based elsewhere in the state. The purpose of this arrangement was to enable this seller to access consumer reports from his own workplace for prospective home buyers who could be referred to PCL for loans. Neither Stiles nor any agent or employee of PCL visited this seller's workplace or audited the computer network on which he used the PCL-issued CRA login, in order to assess that network's vulnerability to attack by an unauthorized person.

In or around July 2006, an unauthorized person hacked into the seller's computer and obtained his PCL-issued CRA login. Using the CRA login, the hacker requested and obtained 317 new consumer reports, submitting requests composed of actual consumer names and addresses, combined with a suspect series of SSNs, the vast majority of which consisted largely of sequential and repeated numbers, with the final four digits identical (*e.g.*, 866-66-6666). Using this CRA login, the hacker also gained access to 83 additional consumer reports that had been requested and obtained by the seller. PCL discovered the hacker's 317 unauthorized requests after two consumers whose reports the hacker had obtained contacted PCL to ask why their consumer reports had been requested by PCL, a company with which the

Analysis to Aid Public Comment

consumers had no relationship. PCL then terminated the seller's CRA login; notified law enforcement and the CRA; and, in August 2006, mailed breach notification letters to these 317 consumers. In August 2007, more than a year later, PCL recognized for the first time that the hacker also had access to the 83 consumer reports requested by the seller whose credentials the hacker used. PCL mailed breach notification letters to these additional 83 consumers in September 2007.

The Commission's proposed complaint alleges that respondents engaged in a number of practices that, taken together, failed to employ reasonable and appropriate security to protect consumers' personal information. In particular, the proposed complaint alleges that respondents failed to: (1) assess the risks of allowing a third party to access consumer reports through PCL's account; (2) implement reasonable steps to address these risks by, for example, evaluating the security of the third party's computer network and taking steps to ensure that appropriate data security measures were present; (3) conduct reasonable reviews of consumer report requests made on PCL's account, using readily available information (such as management reports and invoices) for signs of unauthorized activity, such as spikes in the number of requests made on the account or made by particular PCL users or blatant irregularities in the information used to make the requests; and (4) assess the full scope of consumer report information stored and accessible through PCL's account and thus compromised by the hacker.

According to the complaint, respondents' practices violated the Gramm-Leach-Bliley ("GLB") Safeguards Rule by, among other things (1) failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and (2) failing to design and implement information safeguards to control the risks to customer information and to regularly test or monitor them. In addition, the proposed complaint alleges that respondents misrepresented that

Analysis to Aid Public Comment

they implemented reasonable and appropriate measures to protect consumers' personal information from unauthorized access, in violation of Section 5 of the Federal Trade Commission Act. Further, the proposed complaint alleges that respondents disseminated a privacy policy that does not accurately reflect PCL's privacy policies and practices, in violation of the GLB Privacy Rule.

The proposed order applies to personal information that respondents collect from or about consumers. It contains provisions designed to prevent respondents from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits respondents, in connection with the collection of personal information from or about consumers, in or affecting commerce, from misrepresenting the extent to which it maintains and protects the privacy, confidentiality, or security of such information.

Part II of the proposed order requires respondents to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to respondents' size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the order requires respondents to:

1. Designate an employee or employees to coordinate and be accountable for the information security program.
2. Identify 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

Analysis to Aid Public Comment

information, and assess the sufficiency of any safeguards in place to control these risks.

3. Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.
4. Develop and use reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from respondents, and require service providers by contract to implement and maintain appropriate safeguards.
5. Evaluate and adjust PCL's information security program in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on the effectiveness of their information security program.

Part III of the proposed order requires that respondents not violate any provision of the GLB Safeguards Rule and Privacy Rule.

Part IV of the proposed order requires that respondents obtain, covering the first 180 days after the order is served, and on a biennial basis thereafter for twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that (1) PCL has in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) PCL's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information is protected.

Analysis to Aid Public Comment

Parts V through VIII of the proposed order are reporting and compliance provisions. Part V requires respondents to retain documents relating to their 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, respondents 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 requires Stiles to notify the Commission of changes in her business or employment in connection with providing financial products and services. Part VIII requires respondents to notify the FTC of changes in PCL's corporate status. Part IX mandates that respondents submit an initial compliance report to the FTC, and make available to the FTC subsequent reports. Part X 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.

INTERLOCUTORY, MODIFYING,
VACATING, AND MISCELLANEOUS
ORDERS
