072 3004

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of	)	
PREMIER CAPITAL LENDING, INC., a corporation,	)	**DOCKET NO. C-**
and	)	
DEBRA STILES, individually and as an officer of the corporation.	)	

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 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 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.

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 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.

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

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.

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.

By the Commission.

Donald S. Clark
Secretary