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 Commissi

RESPONDENTS' COURSE OF CONDUCT

4. As part of its process for evalua

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

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