Analysis of Proposed Consent Order to Aid Public Comment
Premier Capital Lending, Inc., and Debra Stiles, File No. 072 3004

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 (herinafter, a "CRA login"). Once logged into the portal, PCL employees request a consumer report by 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 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 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 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.

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.