082 3208

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Jon Leibowitz, Chairman**
William E. Kovacic
J. Thomas Rosch
Edith Ramirez
Julie Brill

In the Matter of	)	
SETTLEMENTONE CREDIT CORPORATION, a corporation,	)	
and	)	
SACKETT NATIONAL HOLDINGS, INC., a corporation.	)	**DOCKET NO.**

COMPLAINT

The Federal Trade Commission ("FTC" or "Commission"), having reason to believe that SettlementOne Credit Corporation and Sackett National Holdings, Inc. 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 Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 et seq.; and Section 5 of the Federal Trade Commission Act ("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 SettlementOne Credit Corporation ("SettlementOne") is a California corporation with its principal office or place of business at 2605 Camino Del Rio South, San Diego, California 92108. Respondent SettlementOne is a wholly-owned subsidiary of respondent Sackett National Holdings, Inc.

2. Respondent Sackett National Holdings, Inc. ("SNH") is a corporation with its principal office or place of business at 2605 Camino Del Rio South, San Diego, California 92108. SNH conducts business through its ten wholly-owned

subsidiaries, including SettlementOne. During all times material to this complaint, SNH controlled the practices alleged in this complaint.

3. 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.

4. SettlementOne contracts with the three nationwide consumer reporting agencies, Equifax, Experian, and TransUnion ("nationwide CRAs") to obtain consumer reports that it assembles and merges into a single "trimerge report." The trimerge reports contain sensitive consumer information such as full name, current and former addresses, Social Security number, date of birth, employer history, credit account histories and information, and even account numbers. Much of this sensitive information is not publicly available. These "trimerge reports" are "consumer reports" as defined in Section 603(d) of the FCRA, 15 U.S.C. § 1681a(d).

5. Respondents sell these trimerge reports to mortgage brokers and others to determine consumers' eligibility for credit. In creating and selling the trimerge reports to end user clients, respondent SettlementOne is a consumer reporting agency as that term is defined in Section 603(f) of the FCRA, 15 U.S.C. § 1681(f).

6. Respondent SettlementOne is a "financial institution" as that term is defined by Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A), and is therefore subject to the requirements of the Safeguards Rule.

RESPONDENTS' COURSE OF CONDUCT

7. SettlementOne furnishes its end user clients with trimerge reports through an online portal. It issues credentials to its clients, which consist of a user name and password. The end user clients use these credentials to access SettlementOne's online portal and receive trimerged reports.

8. From at least February 2008, 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 failed to:

   a. develop and disseminate information security policies for SettlementOne and its end user clients;

   b. assess the risks of allowing end users with unverified or inadequate security to access consumer reports through SettlementOne's portal;

c. implement reasonable steps to address these risks by, for example, evaluating the security of end user's computer networks, requiring appropriate information security measures, and training end user clients;

d. implement reasonable steps to maintain an effective system of monitoring access to consumer reports by SettlementOne's end users, including by monitoring to detect anomalies and other suspicious activity; and

e. take appropriate action to correct existing vulnerabilities or threats to personal information in light of known risks.

9. Because of SettlementOne's lack of information security policies and procedures, respondents allow clients without basic security measures in place, such as firewalls and updated antivirus software, to have access to their trimerge reports. The lack of such security measures directly caused highly-sensitive consumer reports to be available to hackers, as explained below.

THE BREACHES

10. As a direct result of these failures, between February and June 2008, hackers were able to exploit vulnerabilities in the computer networks of multiple SettlementOne end user clients, putting consumer reports in those networks at risk. In multiple breaches, hackers accessed at least 784 consumer reports without authorization. Additionally, the hackers had the ability to view any consumer report that the end user client had pulled in the previous 90 days.

11. Following each of the breaches, respondents did not make reasonable efforts to determine the cause(s) of the breaches and protect against future breaches. Although respondents did terminate some of the affected end users after learning of the security breaches, in other cases respondents did nothing. Respondents, for example, did not require end user clients to submit any documentation demonstrating that the clients' computer systems were virus free and otherwise properly protected. In one instance, despite the lack of documentation, the respondents restored access to an end user whose credentials had been stolen.

12. In addition, respondents have made no effort to warn their other end users of a known threat, or to suggest they make any efforts to ensure their systems were adequately secured. Respondents continue to give access to consumer reports to end user clients whose information security has not been adequately verified.

VIOLATIONS OF THE SAFEGUARDS RULE

13. 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 became effective 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 that include: (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.

14. As described in Paragraphs 7 through 12, respondents failed to implement reasonable security policies and procedures to protect sensitive consumer information, and have thereby engaged in violations of the Safeguards Rule by, among other things:

    a. failing to design and implement information safeguards to control the risks to customer information;

    b. failing to regularly test or monitor the effectiveness of its existing controls and procedures;

    c. failing to evaluate and adjust the information security program in light of known or identified risks; and

    d. failing to develop, implement, and maintain a comprehensive information security program.

VIOLATIONS OF THE FCRA

15. Section 604 of the FCRA, 15 U.S.C. § 1681b, prohibits a consumer reporting agency from furnishing a consumer report except for specified "permissible purposes." As described in Paragraph 10, in multiple instances, respondents furnished consumer reports to hackers that did not have a permissible purpose to obtain a consumer report. By and through the acts and practices described in Paragraphs 7 through 12, respondents have violated Section 604 of the FCRA, 15 U.S.C. § 1681b.

16. Section 607(a) of the FCRA, 15 U.S.C. § 1681e(a), requires every consumer

reporting agency to maintain reasonable procedures to limit the furnishing of consumer reports to the purposes listed under Section 604 of the FCRA, 15 U.S.C. § 1681b. As described in Paragraphs 7 through 12, respondents failed to maintain reasonable procedures to limit the furnishing of consumer reports to the purposes listed under Section 604 of the FCRA. By and through the acts and practices described in Paragraphs 7 through 12, respondents have violated Section 607(a) of the FCRA, 15 U.S.C. § 1681e(a).

17. Section 607(a) of the FCRA, 15 U.S.C. § 1681e(a), prohibits a consumer reporting agency from furnishing a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a permissible purpose. As described in Paragraphs 10 through 12, in numerous instances, respondents furnished consumer reports under circumstances in which they had reasonable grounds for believing that the reports would not be used for a permissible purpose. By and through the acts and practices described in Paragraphs 10 through 12, respondents have violated Section 607(a) of the FCRA, 15 U.S.C. § 1681e(a).

18. By their violations of Sections 604 and 607(a) of the FCRA, and pursuant to Section 621(a) thereof, 15 U.S.C. § 1681s, respondents have engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE FTC ACT

19. As described in Paragraphs 7 through12, respondents have not employed reasonable and appropriate measures to secure the personal information they maintain and sell. Respondents' failure to employ reasonable and appropriate security measures to protect consumers' personal information has 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. This practice was, and is, an unfair act or practice in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this __ day of _____, _____, has issued this complaint against respondents.

By the Commission.

Donald S. Clark
Secretary