

Complaint

IN THE MATTER OF
SETTLEMENTONE CREDIT CORPORATION
AND
SACKETT NATIONAL HOLDINGS, INC.

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT, SECS. 604
AND 607(A) OF THE FAIR CREDIT REPORTING ACT, AND THE
GRAMM-LEACH-BLILEY SAFEGUARDS RULE

Docket No. C-4330; File No. 082 3208
Filed, August 17, 2011 — Decision, August 17, 2011

This consent order addresses allegations that SettlementOne Credit Corporation and its parent corporation Sackett National Holdings, Inc. (“Respondents”) failed to provide reasonable and appropriate security for consumers’ personal information. According to the complaint, Respondents obtained sensitive consumer information, much of which is not publicly available, from the three nationwide consumer reporting agencies, Equifax, Experian, and TransUnion. Respondents then used this information to create “trimerge reports,” which it sold to mortgage brokers and others to determine consumers’ eligibility for credit. The complaint alleges that Respondents, among other things, failed to develop comprehensive written information security policies; to implement reasonable steps to maintain an effective system of monitoring access to consumer reports by end users; and take appropriate action to correct existing vulnerabilities or threats to personal information in light of known risks. As a result, hackers were able to exploit vulnerabilities and access hundreds of consumer reports. The order requires Respondents to establish and maintain a comprehensive information security program reasonably designed to protect consumer information. The order further requires Respondents to maintain procedures to ensure that its consumer reports are given only to those persons or entities that will use it for a permissible purpose under the Fair Credit Reporting Act. The order further requires Respondents to obtain an independent, third-party assessment of its security procedures on a biennial basis for the next 20 years.

Participants

For the *Commission*: *Anthony Rodriguez and Katherine White.*

For the *Respondents*: *Patrice A. Ficklin, Relman, Dane & Colfax, PLLC.*

Complaint

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

Complaint

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;

Complaint

- 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.

Complaint

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;

Complaint

- 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).

Decision and Order

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 through 12, 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 seventeenth day of August, 2011, has issued this complaint against respondents.

By the Commission.

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 that 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 Federal Trade Commission Act, 15 U.S.C. § 45 *et seq*; the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*; and the

Decision and Order

Commission's Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314, issued pursuant to Title V, Subtitle A of the Gramm-Leach-Bliley Act , 15 U.S.C. §§ 6801-6809.

The Respondents, their attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), an admission by the Respondents of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondents that the law has been violated as alleged in such Complaint, or that 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 has reason to believe that the Respondents have violated the Federal Trade Commission Act, the Fair Credit Reporting Act, and the Gramm-Leach-Bliley Act's Safeguards Rule, 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 comments, and having duly considered the comments received from interested persons, now in further conformity with the procedure described in Section 2.34 of its Rules, 16 C.F.R. § 2.34, the Commission hereby issues its Complaint, makes the following jurisdictional findings, and enters the following Order:

- 1a. Respondent SettlementOne is a California corporation with its principal office or place of business at 2605 Camino Del Rio South, Suite 400, San Diego, CA 92108. SettlementOne is a wholly-owned subsidiary of Sackett National Holdings, Inc.
- 1b. Respondent Sackett National Holdings, Inc. is a corporation with its principal office or place of business at 2605 Camino Del Rio South, San Diego, CA 92108. SNH conducts business through its ten wholly-owned subsidiaries, including SettlementOne.

Decision and Order

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondents, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

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

1. “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; (d) a telephone number; (e) a Social Security number; (f) a credit card or debit card account number; (g) checking account information, (h) a driver’s license, military or state identification number; (i) a persistent identifier, such as a customer number, that is combined with other available data that identifies an individual consumer; or (j) any information that is combined with any of (a) through (i) above.
2. “Gramm-Leach-Bliley Act” or “GLB Act” refers to 15 U.S.C. §§ 6801-6809, as amended, the “Safeguards Rule” 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.
3. “Financial institution” shall mean as defined in Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A).
4. “The Fair Credit Reporting Act” or “FCRA” refers to 15 U.S.C. § 1681 *et seq.*

Decision and Order

5. “Consumer report” shall mean as defined in Section 603(d)(1) of the FCRA, 15 U.S.C. § 1681a(d)(1).
6. Unless otherwise specified, “respondents” shall mean Sackett National Holdings and SettlementOne Credit Corporation, and their subsidiaries, divisions, affiliates, successors and assigns.
7. “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 shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers, including the security, confidentiality, and integrity of personal information accessible to end users. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to the respondents’ size and complexity, the nature and scope of the respondents’ activities, and the sensitivity of the personal information collected from or about consumers. The information security program must include:

- 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

Decision and Order

limited to: (1) employee training and management; (2) information systems, including network and software design, access, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

- 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 the respondents, and requiring service providers by contract to implement and maintain appropriate safeguards; and
- E. the evaluation and adjustment of the respondents' information security program in light of the results of the testing and monitoring required by sub-Part 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.

II.

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 the Safeguards Rule, 16 C.F.R. Part 314. In the event that this Rule is hereafter amended or modified, respondents' compliance with that Rule as so amended or modified shall not be a violation of this order.

Decision and Order

III.

IT IS FURTHER ORDERED that respondents, in connection with the compilation, creation, sale, or dissemination of any consumer report shall:

- A. Furnish such consumer report only to those persons which it has reason to believe have a permissible purpose as described in Section 604(a)(3) of the Fair Credit Reporting Act, 15 U.S.C. § 1681b(a)(3), or under such other circumstances as set forth in Section 604 of the Fair Credit Reporting Act, 15 U.S.C. § 1681b;
- B. Maintain reasonable procedures to limit the furnishing of such consumer report to those with a permissible purpose and ensure that no consumer report is furnished to any person when there are reasonable grounds to believe that the consumer report will not be used for a permissible purpose, as required by Section 607(a) of the Fair Credit Reporting Act, 15 U.S.C. § 1681e(a).

IV.

IT IS FURTHER ORDERED that respondents shall, in connection with their compliance with Part I of this order, obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession, provided however, that except for SettlementOne Credit Corporation for which such Assessments are always required, Sackett National Holdings, Inc. shall not be required to obtain such Assessments for any subsidiary, division, affiliate, successor or assign if the personal information such entities collect, maintain, or store from or about consumers is limited to a first and last name; a home or other physical address, including street name and name of city or town; an email address; a telephone number; or publicly available information regarding property ownership and appraised home value. Each Assessment shall be prepared and completed within sixty (60) days after the

Decision and Order

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, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) 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 respondents have implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondents' size and complexity, the nature and scope of respondents' 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 respondents' security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Respondents shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial

Decision and Order

Assessments shall be retained by respondents until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days after respondents receive 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. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including but not limited to documents, prepared by or on behalf of respondents, that contradict, qualify, or call into question respondents' compliance with this order;
- B. for a period of five (5) years, 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
- C. for a period of three (3) years after the date of preparation of each Assessment required under Part IV of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondents, 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 I and II of this order, for the compliance period covered by such Assessment.

VI.

IT IS FURTHER ORDERED, that for a period of five (5) years from the date of entry of this Order, respondents shall deliver copies of the Order as directed below:

Decision and Order

- A. Respondents must deliver a copy of this order to (1) all current and future principals, officers, directors and managers, (2) all employees, agents and representatives who engage in conduct related to the subject matter of the order, and (3) any business entity resulting from any change in structure set forth in Part VII. For current personnel, delivery shall be within five (5) days of service of this Order. For new personnel, delivery shall occur prior to them assuming their responsibilities. For any business entity resulting from any change in structure set forth in Part VII, delivery shall be at least ten (10) days prior to the change in structure.
- B. Respondents must secure a signed and dated statement acknowledging receipt of this Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this section.

VII.

IT IS FURTHER ORDERED that respondents shall notify the Commission at least thirty (30) days prior to any change in the corporations 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 corporations about which respondents learns less 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. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line FTC v. SettlementOne Credit Corporation, and Sackett National

Decision and Order

Holdings, Inc. *Provided, however,* that, in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of such notices is contemporaneously sent to the Commission at DEbrief@ftc.gov.

VIII.

IT IS FURTHER ORDERED that respondents and their successors and assigns, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their own compliance with this order. Within ten (10) day of receipt of written notice from a representative of the Commission, they shall submit additional true and accurate written reports.

IX.

This order will terminate on August 17, 2031, or twenty (20) years from the most recent date that the United States or the Federal Trade 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 less 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 respondents did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order 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

Analysis to Aid Public Comment

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 OF CONSENT ORDER TO AID PUBLIC
COMMENT**

The Federal Trade Commission has accepted, subject to final approval, three agreements containing consent orders from ACRAnet, Inc. (“ACRAnet”); SettlementOne, Inc. (“SettlementOne”), and its parent corporation Sackett National Holdings, Inc.; and Fajilan and Associates, Inc. d/b/a Statewide Credit Services (“Statewide”) and its principal Robert Fajilan (collectively “respondents”).

The proposed consent orders have 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 agreements and the comments received, and will decide whether it should withdraw from the agreements and take appropriate action or make final the agreements’ proposed orders.

According to the Commission’s proposed complaints, respondents contract with the three nationwide consumer reporting agencies, Experian, Equifax, and TransUnion to obtain consumer reports that they assemble and merge 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 account numbers. Respondents provides the trimerge reports to end user clients through an online portal. Respondents issue credentials to their clients, which consist of a user name and password. The end user

Analysis to Aid Public Comment

clients use these credentials to access respondents' online portals and receive trimerged reports.

The Commission's complaints allege that respondents engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumers' personal information. Among other things, they failed to: (a) develop and disseminate comprehensive written information security policies; (b) assess the risks of allowing end users with unverified or inadequate security to access consumer reports through their online portals; (c) implement reasonable steps to address these risks by, for example, evaluating the security of end users' 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 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.

The complaints further allege that hackers were able to exploit vulnerabilities in the computer networks of multiple end user clients, putting all consumer reports in those networks at risk. In multiple breaches, hackers accessed hundreds of consumer reports.

According to the proposed complaints, respondents' practices violated the Gramm-Leach-Bliley ("GLB") Safeguards Rule by, among other things: (1) failing to design and implement information safeguards to control the risks to customer information; (2) failing to regularly test or monitor the effectiveness of existing controls and procedures; (3) failing to evaluate and adjust the information security programs in light of known or identified risks; and (4) failing to develop, implement, and maintain comprehensive information security programs. In addition, the proposed complaints allege that respondents' conduct violated sections 604 and 607(e) of the Fair Credit Reporting Act ("FCRA"). Further, the proposed complaints allege that respondents' failure to employ reasonable and appropriate measures to secure the personal information they maintain and sell is an unfair practice in violation of Section 5 of the Federal Trade Commission Act.

Analysis to Aid Public Comment

The proposed orders contain provisions designed to prevent respondents from engaging in similar practices in the future. They also apply to personal information respondents collect from or about consumers. The orders name the resellers themselves, ACRAnet, SettlementOne, and Statewide; in the case of SettlementOne, its parent corporation Sackett National Holdings; and in the case of Statewide, its principal Robert Fajilan.

Part I of the proposed orders requires respondents to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers, including the security, confidentiality, and integrity of personal information accessible to end users.¹ The security program must contain administrative, technical, and physical safeguards appropriate to each respondent's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. Specifically, the orders require respondents to:

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

¹ The proposed order against Statewide includes an individual respondent, Robert Fajilan. Parts I-VI of this order apply to any business entity that Mr. Fajilan controls.

Analysis to Aid Public Comment

- Develop and use reasonable steps to select and 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.
- Evaluate and adjust the information security program in light of the results of the testing and monitoring, any material changes to the company's operations or business arrangements, or any other circumstances that they know or have reason to know may have a material impact on the effectiveness of their information security program.

Part II of the proposed orders prohibits respondents from violating any provision of the GLB Safeguards Rule.

Part III of the proposed orders requires that respondents, in connection with the compilation, creation, sale or dissemination of any consumer report shall: (1) furnish such consumer report only to those persons it has reason to believe have a permissible purpose as described in Section 604(a)(3) of the FCRA, or under such other circumstances as set forth in Section 604 of the FCRA; and (2) maintain reasonable procedures to limit the furnishing of such consumer reports to those with a permissible purpose and ensure that no consumer report is furnished to any person when there are reasonable grounds to believe that the consumer report will not be used for a permissible purpose.

Part IV of the proposed orders requires that respondents obtain within 180 days, 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 they have in place a security program that provides protections that meet or exceed the protections required by Part I of the proposed order; and their security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information is protected.²

² The proposed order against SettlementOne and Sackett National Holdings does not require Sackett National Holdings to obtain an assessment for any subsidiary, division, affiliate, successor or assign if the personal

Analysis to Aid Public Comment

Parts V through IX of the proposed orders are reporting and compliance provisions. Part V requires respondents to retain documents relating to their compliance with the orders. For most records, the orders require 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 orders now and in the future to principals, officers, directors, and managers, and all employees, agents and representatives who engage in conduct related to the subject matter of the order. In the ACRAnet and SettlementOne orders, Part VII ensures notification to the FTC of changes in corporate status. In the Statewide order, Part VII requires the individual respondent to notify the FTC of changes in contact information, business or employment status, and Part VIII requires the corporate respondent to notify the FTC of changes in corporate status. Part VIII of the ACRAnet and SettlementOne orders and Part XI of the Statewide order mandates that respondents submit an initial compliance report to the FTC, and make available to the FTC subsequent reports. The last provision of the orders is a provision “sunsetting” the orders after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid public comment on the proposed orders. It is not intended to constitute an official interpretation of the proposed orders or to modify their terms in any way.

information such entities collect, maintain, or store from or about consumers is limited to a first and last name; a home or other physical address, including street name and name of city or town; an email address; a telephone number; or publicly available information regarding property ownership and appraised home value.

Concurring Statement

**STATEMENT OF COMMISSIONER BRILL, IN WHICH
CHAIRMAN LEIBOWITZ AND COMMISSIONERS
ROSCH AND RAMIREZ JOIN**

The respondents in these three matters are resellers of consumer reports who failed to take reasonable measures to protect sensitive consumer credit information. We fully support staff's work on these matters. We write separately to emphasize that in the future we will call for imposition of civil penalties against resellers of consumer reports who do not take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the Fair Credit Reporting Act ("FCRA").

The respondents in these three matters treated their legal obligations to protect consumer information as a paper exercise. Respondents provided only a cursory review of security measures. Thereafter, respondents took no further action to ensure that their customers' security measures adequately protected the information in the consumer reports. Nor did they provide training on security measures to end users. Even after discovering security breaches that should have alerted them to problems with the data security of some customers, respondents failed to implement measures to check the security practices of other clients.

The FCRA requires respondents to take reasonable measures to ensure that consumer reports are given only to entities using the reports for purposes authorized by the statute.¹ As a result of respondents' failure to comply with the FCRA, nearly 2,000 credit reports were improperly accessed. There is not doubt that such unauthorized access can result in grave consumer harm through identity theft.

The significant impact and cost of identity theft are well documented. Although reports regarding the impact of identity theft do not always agree on specific figures, they do reveal tremendous economic and non-economic consequences for both consumers and the economy. The Commission itself issued

¹ 15 U.S.C. § 1681b; 15 U.S.C. § 1681e(a).

Concurring Statement

reports in both 2003² and 2007.³ Our 2007 report estimated that in 2005 alone 8.3 million consumers fell victim to identity theft. We found that 1.8 million of those victims had new accounts opened in their names. One-quarter of the “new account victims” incurred more than \$1,000 in out-of-pocket expenses and five percent spent 1,200 hours in dealing with the consequences of the theft. The report concluded that total losses from identity theft in 2006 totaled \$15.6 billion. Beyond these financial impacts, we also identified non-economic harm to victims in many forms: denial of new credit or loans, harassment from collection agencies, the loss the time involved in resolving the problems, and being subjected to criminal investigation. In view of the hardships and costs brought on by identity theft, measures to prevent it must be rigorously enforced.

While we view the breaches in these cases with alarm, we are also cognizant of the fact that these are the first cases in which the Commission has held resellers responsible for downstream data protection failures.⁴ Looking forward, the actions we announce today should put resellers — indeed, all of those in the chain of handling consumer data — on notice of the seriousness with which we view their legal obligations to proactively protect consumers’ data. The Commission should use all of the tools at its disposal to protect consumers from the enormous risks posed by security breaches that may lead to identity theft. In the future, we should not hesitate to use our authority to seek civil penalties under the FCRA⁵ to make the protection of consumer data a top priority for those who profit from its collection and dissemination.

² Fed. Trade Comm’n. *Identity Theft Survey Report* (2003), available at <http://www.ftc.gov/os/2003/09/synovatereport.pdf>.

³ Fed. Trade Comm’n, *2006 Identity Theft Survey Report* (2007), available at <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.

⁴ The Commission has previously taken action where the credit reporting agency failed to adequately screen purchasers of consumer credit information. For instance, in *United States v. ChoicePoint, Inc.*, 09-CV-0198 (N.D. Ga. Oct. 19, 2009), the Commission alleged that the failure to screen customers led to the sale of 160,000 credit reports to identity thieves posing as customers of ChoicePoint.

⁵ The Fair Credit Reporting Act authorizes the Commission to seek civil penalties for violations of the Act. 15 U.S.C. § 1681s(a)(2)(A).

Complaint

IN THE MATTER OF

ACRANET, INC.

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT, SECS. 604
AND 607(A) OF THE FAIR CREDIT REPORTING ACT, AND THE
GRAMM-LEACH-BLILEY SAFEGUARDS RULE

Docket No. C-4331; File No. 092 3088
Filed, August 17, 2011 — Decision, August 17, 2011

This consent order addresses allegations that ACRANet, Inc. (“Respondent”) failed to provide reasonable and appropriate security for consumers’ personal information. According to the complaint, Respondent obtained sensitive consumer information, much of which is not publicly available, from the three nationwide consumer reporting agencies, Equifax, Experian, and TransUnion. Respondent then used this information to create “trimerge reports,” which it sold to mortgage brokers and others to determine consumers’ eligibility for credit. The complaint alleges that Respondent, among other things, failed to develop comprehensive written information security policies; to implement reasonable steps to maintain an effective system of monitoring access to consumer reports by end users; and take appropriate action to correct existing vulnerabilities or threats to personal information in light of known risks. As a result, hackers were able to exploit vulnerabilities and access hundreds of consumer reports. The order requires Respondent to establish and maintain a comprehensive information security program reasonably designed to protect consumer information. The order further requires Respondent to maintain procedures to ensure that its consumer reports are given only to those persons or entities that will use it for a permissible purpose under the Fair Credit Reporting Act. The order further requires Respondent to obtain an independent, third-party assessment of its security procedures on a biennial basis for the next 20 years.

Participants

For the *Commission*: *Anthony Rodriguez and Katherine White.*

For the *Respondent*: *Jed W. Morris, Lukins & Annis.*