Analysis of Proposed Consent Orders to Aid Public Comment
In the Matter of ACRAnet, Inc., File No. 092 3088
In the Matter of SettlementOne Credit Corporation, and Sackett National Holdings, Inc., File No. 082 3208
In the Matter of Fajilan and Associates, Inc. d/b/a Statewide Credit Services, and Robert Fajilan, File No. 092 3089

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 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.

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.

- Develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondents,

[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.

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]

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

[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 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.

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 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.