staff further estimates that associated annual labor costs for new entrants would be $801,000 [(5,100 hours × $150 per hour for legal) + (1,000 hours × $36 per hour for computer programmers)] and $15,000 for safe harbor applicants (100 hours per year × $150 per hour), for a total labor cost of approximately $816,000.

2. *Capital or other non-labor costs:* Because Web sites will already be equipped with the computer equipment and software necessary to comply with the Rule's notice requirements, the predominant costs incurred by the Web sites are the aforementioned estimated labor costs. Similarly, industry members should already have in place the means to retain and store the records that must be kept under the Rule's safe harbor recordkeeping provisions, because they are likely to have been keeping these records independent of the Rule. Capital and start-up costs associated with the Rule are minimal.

Willard K. Tom,

General Counsel.

[FR Doc. 2011–2904 Filed 2–8–11; 8:45 am]

BILLING CODE 6750–01–P

FEDERAL TRADE COMMISSION

[File Nos. 092 3088, 082 3208, 092 3089]

ACRAnet, Inc.; SettlementOne Credit Corporation, and Sackett National Holdings, Inc.; Fajilan and Associates, Inc., d/b/a Statewide Credit Services, and Robert Fajilan; Analysis of Proposed Consent Orders To Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed Consent Agreement.

SUMMARY: The consent agreements in these three matters settle alleged violations of federal law prohibiting unfair or deceptive acts or practices or unfair methods of competition. The attached Analysis To Aid Public Comment describes both the allegations in each draft complaint and the terms of the consent order—embodied in each consent agreement—that would settle these allegations.

DATES: Comments must be received on or before March 7, 2011.

ADDRESSES: Interested parties are invited to submit written comments electronically or in paper form. Comments should refer to "ACRAnet, Inc., File No. 092 3088, and/or SettlementOne Credit Corporation, File No. 082 3208, and/or Statewide Credit Services, File No. 092 3089" to facilitate the organization of comments. Please note that your comment—including your name and your state—will be placed on the public record of this proceeding, including on the publicly accessible FTC Web site, at *http://www.ftc.gov/os/publiccomments.shtm.*

Because comments will be made public, they should not include any sensitive personal information, such as an individual's Social Security Number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. Comments also should not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, comments should not include any "[t]rade secret or any commercial or financial information which is obtained from any person and which is privileged or confidential. * * *," as provided in Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and Commission Rule 4.10(a)(2), 16 CFR 4.10(a)(2). Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c), 16 CFR 4.9(c).[1]

Because paper mail addressed to the FTC is subject to delay due to heightened security screening, please consider submitting your comments in electronic form. Comments filed in electronic form should be submitted by using one of the following weblinks: *https://ftcpublic.commentworks.com/ftc/acranet; https://ftcpublic.commentworks.com/ftc/settlementone; https://ftcpublic.commentworks.com/ftc/statewide,* and following the instructions on the web-based form. To ensure that the Commission considers an electronic comment, you must file it on the Web-based form at one of the following weblinks: *https://ftcpublic.commentworks.com/ftc/acranet; https://ftcpublic.commentworks.com/ftc/settlementone; https://ftcpublic.commentworks.com/ftc/statewide.* If this Notice appears at *http://www.regulations.gov/search/index.jsp,* you may also file an electronic comment through that Web site. The Commission will consider all comments that regulations.gov forwards to it. You may also visit the FTC Web site at *http://www.ftc.gov/* to read the Notice and the news release describing it.

A comment filed in paper form should include the "to ACRAnet, Inc., File No. 092 3088, and/or SettlementOne Credit Corporation, File No. 082 3208, and/or Statewide Credit Services, File No. 092 3089" reference both in the text and on the envelope, and should be mailed or delivered to the following address: Federal Trade Commission, Office of the Secretary, Room H–135 (Annex D), 600 Pennsylvania Avenue, NW., Washington, DC 20580. The FTC is requesting that any comment filed in paper form be sent by courier or overnight service, if possible, because U.S. postal mail in the Washington area and at the Commission is subject to delay due to heightened security precautions.

The Federal Trade Commission Act ("FTC Act") and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives, whether filed in paper or electronic form. Comments received will be available to the public on the FTC Web site, to the extent practicable, at *http://www.ftc.gov/os/publiccomments.shtm.* As a matter of discretion, the Commission makes every effort to remove home contact information for individuals from the public comments it receives before placing those comments on the FTC Web site. More information, including routine uses permitted by the Privacy Act, may be found in the FTC's privacy policy, at *http://www.ftc.gov/ftc/privacy.shtm.*

FOR FURTHER INFORMATION CONTACT: Katherine White (202–326–2252), Bureau of Consumer Protection, 600 Pennsylvania Avenue, NW., Washington, D.C. 20580.

SUPPLEMENTARY INFORMATION: Pursuant to section 6(f) of the Federal Trade Commission Act, 38 Stat. 721, 15 U.S.C. 46(f), and § 2.34 the Commission Rules of Practice, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreements containing consent orders to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, have been placed on the public record for a period of thirty (30) days. The following

available at http://www.bls.gov/ncs/ocs/sp/nctb1346.pdf.

[1] The comment must be accompanied by an explicit request for confidential treatment, including the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. The request will be granted or denied by the Commission's General Counsel, consistent with applicable law and the public interest. *See* FTC Rule 4.9(c), 16 CFR 4.9(c).

Analysis To Aid Public Comment describes the terms of the consent agreements, and the allegations in the draft complaints. An electronic copy of the full text of each consent agreement package can be obtained from the FTC Home Page (for February 3, 2011), on the World Wide Web, at *http://www.ftc.gov/os/actions.shtm.* Paper copies can be obtained from the FTC Public Reference Room, Room 130–H, 600 Pennsylvania Avenue, NW., Washington, DC 20580, either in person or by calling (202) 326–2222.

Public comments are invited, and may be filed with the Commission in either paper or electronic form. All comments should be filed as prescribed in the **ADDRESSES** section above, and must be received on or before the date specified in the **DATES** section.

Analysis of Agreement Containing 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 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.[2] 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, 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.

[2] 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.

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.[3]

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 mandate 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.

By direction of the Commission.

Donald S. Clark

Secretary.

[3] 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 e-mail address; a telephone number; or publicly available information regarding property ownership and appraised home value.

Statement of Commissioner Brill, In Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join

In the Matter of SettlementOne Credit Corporation, et al., In the Matter of ACRAnet, Inc., In the Matter of Fajilan and Associates, et al.

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 reports in both 2003[2] 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 of 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 FCRA[5] to make the protection of consumer data a top priority for those who profit from its collection and dissemination.

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

[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).

[FR Doc. 2011–2790 Filed 2–8–11; 8:45 am]

BILLING CODE 6750–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health Statement of Organization, Functions, and Delegations of Authority

Part N, National Institutes of Health, of the Statement of Organization, Functions, and Delegations of Authority for the Department of Health and Human Services (40 FR 22859, May 27, 1975, as amended most recently at 66 FR 6617, January 22, 2001, and redesignated from Part HN as Part N at 60 FR 56605, November 9, 1995), is amended as set forth below to establish the Office of Portfolio Analysis (OPA) and Office of Program Evaluation and Performance (OPEP) within the Division of Program Coordination, Planning and Strategic Initiative (DPCPSI) within the Office of the Director.

Section N–AW, Organization and Functions, is amended as follows: Immediately after the paragraph headed "Office of Portfolio Analysis and Strategic Initiatives" (N AW6, formerly HN AW6), insert the following:

Office of Portfolio Analysis (N AW7, formerly N AW7) (1) Prepare and analyze data on NIH sponsored biomedical research to inform trans-NIH planning and coordination; (2) serve as a resource for portfolio management at the programmatic level; (3) employ databases, analytic tools, methodologies and other resources to conduct assessments in support of portfolio analyses and priority setting in scientific areas of interest across NIH; (4) research and develop new analytic tools, support systems, and specifications for new resources in coordination with other NIH organizations to enhance the management of the NIH's scientific portfolio; and (5) provide, in coordination with other NIH organizations, training on portfolio analysis tools, procedures, and methodology.

Office of Program Evaluation and Performance (N AW8, formerly N AW8) (1) Plan, conduct, coordinate, and support program evaluations, including IC-specific program and project evaluations and trans-NIH evaluations; (2) manage and administer NIH's Evaluation Set-Aside Program; (3) coordinate and direct the preparation of plans and reports required by the Government Performance and Results Act (GPRA), including the development of required performance measures; (4) identify and advise on emerging national issues within program evaluation and performance, including NIH's response to legislative, regulatory, and policy requirements of the GPRA and administration of the NIH-wide evaluation program.

Delegations of Authority Statement: All delegations and redelegations of authority to officers and employees of NIH that were in effect immediately prior to the effective date of this reorganization and are consistent with this reorganization shall continue in effect, pending further redelegation.

Dated: January 21, 2011.

LaVerene Stringfield,

Associate Director for Management, OD, ES, NIH.

[FR Doc. 2011–2848 Filed 2–8–11; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

[30 Day–11–10BG]

Agency Forms Undergoing Paperwork Reduction Act Review

The Centers for Disease Control and Prevention (CDC) publishes a list of information collection requests under review by the Office of Management and Budget (OMB) in compliance with the Paperwork Reduction Act (44 U.S.C. Chapter 35). To request a copy of these requests, call the CDC Reports Clearance Officer at (404) 639–5960 or send an e-mail to *omb@cdc.gov.* Send written comments to CDC Desk Officer, Office of Management and Budget, Washington, DC 20503 or by fax to (202) 395–5806. Written comments should be received within 30 days of this notice.

Proposed Project

National Voluntary Environmental Assessment Information System (NVEAIS)—New—National Center for Environmental Health (NCEH), Centers for Disease Control and Prevention (CDC).

Background and Brief Description

The CDC is requesting OMB approval for a National Voluntary Environmental Assessment Information System to collect data from foodborne illness outbreak environmental assessments routinely conducted by local, state, territorial, or tribal food safety programs during outbreak investigations. Environmental assessment data are not currently collected at the national level. The data reported through this information system will provide timely data on the causes of outbreaks, including environmental factors associated with outbreaks, and are essential to environmental public health regulators' efforts to respond more effectively to outbreaks and prevent future, similar outbreaks.

The information system was developed by the Environmental Health Specialists Network (EHS–Net), a collaborative project of federal and state public health agencies. The EHS–Net has developed a standardized instrument for reporting data relevant to foodborne illness outbreak environmental assessments.

State, local, tribal, and territorial food safety programs are the respondents for this data collection. Although it is not possible to determine how many programs will choose to participate, as NVEAIS is voluntary, the maximum potential number of program respondents is approximately 3,000.

However, these programs will be reporting data on outbreaks, not their programs or personnel. It is not possible to determine exactly how many outbreaks will occur in the future, nor where they will occur. However, we can estimate, based on existing data that a maximum of 1,400 foodborne illness outbreaks will occur annually. Only programs in the jurisdictions in which these outbreaks occur would report to NVEAIS. Consequently, we have based our respondent burden estimate on the number of outbreaks likely to occur each year. Assuming each outbreak occurs in a different jurisdiction, there will be one respondent per outbreak. Each respondent will respond only once per outbreak investigated.

There are two activities for which we need to estimate burden for these programs. The first is entering all requested environmental assessment data into NVEAIS. This will be done once for each outbreak. This will take approximately 120 minutes per outbreak.

The second activity requiring a burden estimate is the manager interview that will be conducted at each establishment associated with an