



March 7, 2011

Hon. Donald S. Clark
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Washington, DC 20580

Via Electronic Filing

Re: In the Matter of SettlementOne Credit Corporation, et al., File No. 082 3208
In the Matter of ACRAnet, Inc., File No. 092 3088
In the Matter of Fajilan and Associates, et al. File No. 092 3089

To Whom It May Concern:

The Consumer Data Industry Association (CDIA) respectfully submits this comment on the Federal Trade Commission's ("FTC" or "Commission") proposed settlements in the three above-referenced matters. CDIA is an international trade association representing consumer reporting agencies, including resellers of consumer reports, and other consumer data companies. CDIA's approximately 200 members include the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening and collection services. These members include resellers of consumer reporting information to end-users in the mortgage industry.

The FTC's complaints in these matters allege that the reseller respondents allowed clients to access their credit reports when the clients lacked basic security measures, such as firewalls and updated antivirus software, and that, as a result, hackers accessed consumers' credit reports via the clients' computer networks. The complaints also allege that the resellers did not make reasonable efforts to protect against future breaches after they became aware of the data breaches.

The proposed consent orders in these cases require each of the respondents to comply with the Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule and the Fair Credit Reporting Act ("FCRA"). Specifically, the consent orders require the respondents to (a) establish, implement and maintain reasonable procedures to safeguard the data provided to end-users and (b) assure that consumer reports are provided only to persons which the consumer reporting agency has reason to believe have a permissible purpose for the consumer reports.

In CDIA's experience, its members take very seriously their privacy, confidentiality, security, and data protection responsibilities with respect to consumer information. The specific obligations of consumer reporting agencies, resellers and end-users with respect to the use and security of consumer information depend upon the respective role of each a participant in the information flow.

CDIA is concerned about the Commission's press release and the statements of Commissioner Brill, joined by Chairman Leibowitz and Commissioners Rosch and Ramirez. CDIA finds particularly inappropriate the Commissioners' statements: "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." As the Commission knows, because the respondents agreed to settle these matters without admitting any of the FTC's complaint allegations, there was no evidentiary finding and thus no basis to support such statements. The Commissioners' statements are inconsistent with CDIA's experience with its reseller members. CDIA believes that resellers do much more than rely on end-users' contractual representations and warranties with respect to data security measures. Moreover, the Commissioners' statements denigrate respondents' reliance on representations and warranties in binding contracts by responsible firms and thus the value of these contractual agreements.

The Commissioners' statements describe some potentially very significant new obligations for firms that provide consumer data to end-users or others. The Commissioners would impose these obligations without any public dialogue or administrative process. Before considering such a major policy shift, the Commission should engage knowledgeable industry participants in a discussion of the import of these obligations.

CDIA also objects to the Commissioners' statement that the FTC holds the resellers "responsible for downstream data protection failures" which by law are the direct and independent responsibility of end-users of consumer reports. This statement is similar to the complaint allegation: "Because of [respondent's] lack of information security policies and procedures, respondent allows end-users 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." These statements imply that resellers should be held responsible for security failures within an end-user and for the consequences of the end-user's failures. CDIA disagrees with such a theory. If an end-user lacks firewalls, anti-virus software or other security measures, the end-user's security failures directly enable hackers' access to the end-user's consumer report information. CDIA agrees that end-users should have effective security procedures in place to protect against the misuse of consumer reports obtained lawfully from consumer reporting agencies, much as our members have their own specific duties under law with regard to consumer reports under their control.

While resellers are responsible for implementing reasonable systems and controls with respect to end-users' access to information through their portals, resellers cannot be held responsible for the failure of end-users' security programs or for the consequences of the end-users' failures. The law does not require resellers to monitor or audit their end-users' information security programs, because the law appropriately imposes these duties on the end-users themselves. In our view, consumer reporting agencies and users of consumer reports have specific and separate duties under the FCRA. Similarly, all financial institutions under the GLBA have separate duties with regard to the safeguarding of nonpublic personal information. Our members do not question the validity of these duties as they apply to them, and they take their responsibilities to comply with the law very seriously. So too should users of consumer reports.

CDIA notes that the Commission did not bring enforcement actions against the end-users whose alleged data security failures led to the breaches. CDIA believes that the appropriate focus would have been on the end-users' failures. Resellers and other consumer reporting agencies should not be held responsible for the actions or failures of independent third parties in their handling of consumer data.

CDIA also notes that the Commissioners' statements differ from the consent order provisions to which the respondents agreed. These provisions reflect the legal requirements for resellers and others who access or hold consumer information. Specifically, the orders require the respondents to

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 respondents are also required to comply with the GLBA Safeguards rule and the FCRA. Thus, in contrast to the Commissioners' statements and the complaint language, these order provisions reflect the respondents' legal requirements with respect to consumer data which they maintain and to which they can reasonably control access.

CDIA is also concerned with the Commissioners' statement that the FTC will seek 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 [FCRA]." CDIA is concerned to the extent that statement might be interpreted to require resellers to protect information in consumer reports accessed or held by an end-user, regardless of the reasonableness of the resellers' procedures to comply with the FCRA. As the Commission knows, the FCRA requires all consumer reporting agencies to maintain reasonable procedures to limit the furnishing of consumer reports for permissible purposes. FCRA sections 604(a) and (c) and 607(a) set forth the requirements for consumer reporting agencies with respect to those procedures. Civil penalties may be an appropriate remedy if a consumer reporting agency engages in a knowing violation of these (or other) FCRA requirements that constitutes a pattern or practice of violations. However, the Commissioners' statement implies that the FTC may seek to exercise its civil penalty authority by interpreting the FCRA to impose requirements on resellers beyond their statutory obligations.

In sum, CDIA is concerned to the extent that the Commissioners' statements may indicate their intention to apply new standards and new liability to resellers and others based on the conduct or failure of independent third parties.

CDIA appreciates the opportunity to submit this comment. We would be glad to discuss the issues addressed in this letter with the Commissioners and the FTC staff.

Sincerely,

Stuart K. Pratt
President & CEO