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

Dear Mr. Clark:

The Credit Bureau of Council Bluffs, Inc appreciates the opportunity to comment on the Federal Trade Commission's ("FTC") proposed settlements in the three above-referenced matters.

Background on Credit Bureau of Council Bluffs, Inc.

Credit Bureau of Council Bluffs, Inc. was founded in 1915, and incorporated in 1969 as a credit reporting agency. We began the automation of the credit data in 1982 first on the Pinger system and eventually on the TransUnion system. Up until 2001 the Credit Bureau of Council Bluffs owned and maintained the credit information for southwestern Iowa and Nebraska. Upon selling our database to TransUnion in 2001 we would be known to you as a "reseller" in Fair Credit Reporting Act ("FCRA") terms, servicing the consumer reporting needs of mortgage lenders, consumer lenders, auto dealers, property managers, and employers. The Credit Bureau of Council Bluffs, Inc. has been in my family since 1947. We employ 16 people and serve customers throughout the Midwest. My company is very similar to the respondents' companies referenced above.

As a "reseller" of consumer reports, we obtain reports from the three nationwide consumer reporting agencies and create combined, or "tri-merge", and other specialty hybrid consumer reports for specific mortgage lending, consumer lending, auto lending, tenant screening and employment screening needs.

I take the duty of being a good steward of the consumers' data within my control very seriously and have never neglected my obligation to safeguard the consumers' information. I agree with the FTC's statements about problems associated with identity theft and for that reason I have devoted significant corporate resources, including investment in sophisticated technology systems, to protect consumer data within my control.

The FTC's Statement about the Respondents

I notice that the respondents in these matters did not admit to any of the complaint allegations. Each company made a business decision to settle on the terms of the negotiated order, rather than incur the significant legal fees and expenses of defending an FTC enforcement action. For that reason, I find troubling FTC's press release and particularly the statement of Commissioner Brill, joined by the Chairman and Commissioners Rosch and Ramirez (the "Commissioners' Statement"). These FTC statements are not a reflection of the efforts that I take in protecting the consumers' data and I find them derogatory and inflammatory in nature. I believe that these types of messages are likely to give the public an inaccurate impression of my industry and our compliance with Federal laws.

Despite the impression created by the FTC's press release and the Commissioners' Statement, each of these three resellers had implemented and maintained an information security program that was reasonably designed to protect the security, confidentiality, and integrity of customer information, as required under the GLBA Safeguards Rule. Each reseller maintained reasonable procedures to limit the provision of consumer reports to end-users who had a permissible purpose for the reports in accordance with the FCRA. Moreover, each reseller required its end-users to agree by written contract that they would implement and maintain adequate information security systems, controls and procedures, including firewalls and other appropriate data security measures. These written agreements provided that an end-user's violation of these contractual obligations could result in suspension of the end-user's access to the reseller's portal or termination of the agreement. By implementing vigorous internal security measures and contractually mandating that end-users act similarly, the resellers met their legal obligations under the FCRA and the GLBA to protect consumer information. The resellers having sold the information after meeting their legal obligations under FCRA and the GLBA placed the obligation of safeguarding the consumer information upon the end-user who had purchased it.

The Missing Parties in the Proposed Orders

None of the unprotected computer systems involved in the data breaches that led to these enforcement actions were within the ownership or control of these resellers. The FTC's complaints allege that the breaches occurred because the end-users lacked adequate firewalls or other security controls. Thus, the alleged failures of these independent third parties, and not the resellers' actions, contributed to the security breaches. These end-users apparently did not meet their own legal obligations under the FCRA and the GLBA, and they appear to have breached their contractual obligations to the resellers. For these reasons, I believe that the Commission's enforcement actions targeted the wrong parties in these matters.

The proposed orders essentially require the respondent resellers to comply with their legal obligations under the GLBA and the FCRA – obligations that the resellers had endeavored to meet even prior to the FTC's enforcement actions. Because the end-users are not subject to these consent orders, the FTC's enforcement actions will not protect consumers with respect to the security and confidentiality of consumer information held by these end-users.

It is important to understand that, as mortgage lenders, consumer lenders, auto dealers, property managers, and employers these end-users receive and maintain consumers' indentifying information and highly confidential financial information from applications, financial institutions, employers and others, in addition to consumer reports from resellers. These end-users are subject to the same GLBA and FCRA laws as the resellers. Yet, the FTC's orders will not require these end-users to implement any measures to comply with these laws. Clearly, the FTC has brought the wrong parties under order.

The Commissioners' Statement

Despite the fact that the FTC's orders apply only to the resellers, the Commissioners' Statement asserts that "these are the first cases in which the Commission has held resellers responsible for downstream data protection failures." This statement is at odds with the terms of the consent orders and, for the most part, even the complaint's allegations. As an owner of a consumer reporting agency, I am deeply troubled by the Commissioners' apparent plan to hold resellers responsible for the potential failures of independent third parties to protect consumer data. There is no basis in the FCRA or even the GLBA Safeguards Rule for this kind of liability.

Further, the Commissioners state that they will seek civil penalties in future cases involving "resellers – indeed, all of those in the chain of handling consumer data" based

on their "legal obligations to proactively protect consumers' data." The FCRA imposes certain legal requirements on resellers in providing reports to end-users with permissible purposes. However, FCRA does not require resellers or others in the chain of handling consumer data to "proactively protect consumers' data." Resellers' data security obligations with respect to consumer information are governed by the GLBA Safeguards Rule, which does not provide for civil penalties for violations of its requirements.

The FTC can best promote the important objective of protecting consumer information by focusing on entities that are best able to provide this protection. The Commission should hold resellers responsible for consumer information and access to that information within their control, but the Commission should also hold end-users responsible for their own data security. In this case, the FTC ignores end-users altogether and instead would require resellers to assume responsibility for third parties' internal data security measures. Not only will this impose an unfair and unworkable burden on firms such as mine, it would also create a system that leaves consumers more vulnerable than they would be if the FTC required each entity to take responsibility for its own data security systems.

Thank you again for the opportunity to comment on these matters.

Sincerely,
Heather Russell-Schroeder
President