



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:

Affiliated Information Resources, Inc., dba Airfactz appreciates the opportunity to comment on the Federal Trade Commission's ("FTC") proposed settlements in the three above-referenced matters.

Background on Affiliated Information Resources, Inc., dba Airfactz

Airfactz was founded in 1990, as a credit reporting agency (known to you as a "reseller" in Fair Credit Reporting Act ("FCRA") terms, servicing the consumer reporting needs of mostly small business such as Landlords, Property Managers, and small employers in the Spokane, Washington area. Our company, while serving different market segments, is very similar to the respondents' companies referenced above.

As a "reseller" of consumer reports, we generally obtain reports from one of the three nationwide consumer reporting agencies and to create consumer reports for specific rental background check or employers pre-hiring background check 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. For that

reason I have devoted significant corporate resources, including investment in sophisticated technology systems, to protect consumer data within my control.

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 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 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. How will the FTC's orders really protect consumer information in the face of so many additional sources?

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.

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. This will impose an unfair and unworkable burden on firms such as mine, all the while leaving consumers vulnerable by ignoring entities which should be responsible for their own data security systems.

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

Sincerely,

»

Mark R. Millsap
Vice President
Affiliated Information Resources, Inc.

cc: corporate file