Re: FACTA Identity Theft Rule, Matter No. R411011

June 15, 2004

Background

Subsection 112(b) of the Fair and Accurate Credit Transactions Act of 2003 (FACTA) requires the Federal Trade Commission to determine what constitutes appropriate proof of identity for the purposes of sections 605A, 605B, and 609(a)(1) of the Fair Credit Reporting Act (FCRA), as amended by FACTA. These purposes refer to, respectively, a request by a consumer, or an individual acting on behalf of, or as a personal representative of a consumer, for placing and removing fraud and active duty alerts on consumer credit files; a request by a consumer for blocking fraudulent information on credit files resulting from identity theft; and a request by a consumer for Social Security number truncation on credit file disclosures.

In light of these new requirements, the Commission seeks comments on what should constitute appropriate proof of identity for these purposes. In each of these instances, an individual consumer would provide this proof of identity to a consumer credit reporting agency. The consumer reporting agency then authenticates the consumer's claimed identity on the basis of this information. After the consumer is authenticated, the credit reporting agency performs the requested activities.

Section 605A(h)(1)(B)(i) of the FCRA also restricts the ability of users of consumer credit reports on which an "initial" fraud alert has been placed to grant credit or open new accounts unless "the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request." If a consumer provides a telephone number as part of the fraud alert, the user is required to contact the consumer at that number to verify the application (section 605A(h)(1)(B)(ii)). If, however, the fraud alert is an "extended" alert, meaning that the period of the alert is longer and that the consumer can demonstrate that he/she has been a victim of identity theft by means of an identity theft report, then the user of the credit report is actually required to contact the consumer to verify that the application is legitimate (section 605A(h)(2)(B)).

Although this request for public comments does not specifically seek comments on potential policies and procedures that could form a reasonable belief that the user of a credit report knows the identity of a person seeking to establish a new credit account, Section 615(e) of the FCRA requires the Commission, along with appropriate federal banking regulatory agencies, to establish guidelines pertaining to identity theft, and policies and procedure for implementing those guidelines. These comments will address this issue as well.

The Problem With Asking Consumers To Provide Identifying Information

In all these instances, there is a common theme: a credit reporting agency, or the user of a credit report, must authenticate the identity of an individual consumer prior to carrying out the wishes of that consumer. These wishes range from placing and removing fraud alerts, to actually opening new credit accounts. Since the very purpose of a fraud alert is to ensure that an imposter cannot open a new account or otherwise secure credit in someone else's name, it would seem that the authentication procedure required to actually grant credit or open a new account should be at least as "strong" as that for placing or removing a fraud alert.

The Commission proposes that the authentication method used by credit reporting agencies for placing and removing fraud alerts be based on "reasonable requirements to identify consumers in accordance with the risk of harm that might arise from a misidentification." The examples provided by the Commission include requesting that the consumer provide a sufficient set of information about the consumer, such as name, address, Social Security number, date of birth, etc., so that this information may be matched with information in the consumer's credit report. **The problem with this "knowledge-based" approach is that it's not difficult for an identity thief to acquire this information about his victim**. Recognizing this, the Commission further allows that consumers may, at the discretion of the consumer reporting agency, also be asked to provide physical documentation such as utility bills, government-issued identification documents, etc. **The problem here is that providing such documentation would seem to require an in-person appearance by the consumer at the credit reporting agcncy, which would be cumbersome and inconvenient**. **Such documentation can also be easily faked by identity thieves**.

The authentication problem faced by a credit reporting agency that places or removes fraud alerts on behalf of a consumer is similar to the authentication problem faced by credit grantors that must verify the identity of an applicant for a new credit account that is applied for remotely; i.e., online or over the phone. In both cases, the credit reporting agency, as well as the credit grantor, will have limited means to perform identity authentication. Most of the time, the best they can do is to perform some type of knowledge-based authentication by asking the consumer personal questions whose answers can be verified against information contained in various public and private databases.

However, the assumption that a person's identity can be authenticated on the basis of knowledge of a few items of personal information is faulty, because it rests on the erroneous assumption that this information can be kept secret and out of the hands of imposters. It is widely acknowledged that sensitive personal information about an individual can be acquired without much difficulty by fraudsters. Therefore, **the Commission's rules for "proof of identity" need to rely on methods that are stronger than simple knowledge of personal information**.

Potential Solutions to the Authentication Problem

What might such methods entail? Consider that even though a credit grantor, or a consumer credit reporting agency, may not have a previous relationship with a particular consumer, it is highly likely that the consumer does have other relationships which may be leveraged in order to authenticate that consumer's identity. In particular, most people have some type of bank account, especially those who have credit files and may become the victim of identity fraud. When a person opens a bank account, the bank (in theory) is supposed to take steps to verify the identity of that person. In many instances, this may consist solely of asking the potential customer to provide a government-issued photo ID, which of course can be faked. In other instances, the potential banking customer may be asked to provide some other physical documentation, perhaps in combination with the use of knowledge-based authentication. This would be done in-person at the bank. The methods and criteria by which banks verify the identities of new customers is a separate and important issue, but here it will be assumed that the bank has taken adequate steps to verify these identities.

Once a bank verifies a person's identity and opens an account for that person, a trusted relationship then exists between the bank and the consumer (who is now a customer of the bank). This trusted relationship could potentially be leveraged if the bank will agree to assert the consumer's identity in response to a request by another organization, such as a credit reporting agency or a credit grantor. Such responses would consist of an assertion to the requester that would confirm or deny the identity claimed by someone seeking to place or remove a fraud alert, etc., or to open a new credit account, based upon criteria that would be established by the financial services industry, the Commission, and relevant banking regulatory agencies.

What the Commission Should Do

It is proposed that the Commission, in conjunction with other relevant banking regulatory agencies, undertake to further study and investigate the feasibility of banks acting as "trusted authenticators" whereby they would respond to requests for an identity authentication from entities such as credit reporting agencies or credit grantors.

As the FCRA requires, a fraud alert may be placed by consumers on their credit files to guard against identity theft. The very concept of a fraud alert acknowledges that a powerful method of confirming the identity of those seeking to establish a new credit account is to contact the "true owner" of a claimed identity to verify that this person is indeed seeking to open the account. Yet this method of identity theft prevention, as a long term measure, is reserved by the FCRA only for those who can demonstrate that they have been victims of identity theft, by submission of an identity theft report.

As part of the proposed studies that the Commission and relevant banking regulatory agencies should undertake, the feasibility of allowing any consumer to

request that they be directly contacted via a phone call, secure e-mail, or other method, before credit is granted or extended in their name, should be studied.

The proposed studies should focus on at least two approaches by which banks could authenticate the identities of their customers, in response to a request from a credit reporting agency, or a credit grantor. These two approaches are:

- The bank contacts its customer by secure e-mail, telephone, or some other method, for identity verification.
- The bank authenticates its customer using an authentication method that the bank has already established with the person whose identity is claimed. The authentication method would likely be the same as the bank uses to authenticate its customer for access to online banking services, or telephone banking services.

Robert Pinheiro
Security Consultant

bp@bobpinheiro.com