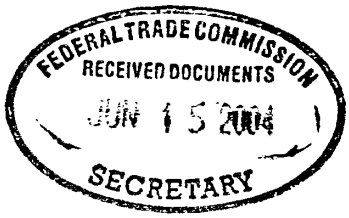

June 15, 2004

Federal Trade Commission
Office of the Secretary
Matter Number: R411011
Room H-159 (Annex J)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: FACTA Identity Theft Rule
69 FR 23370 (April 28, 2004)

Dear Sir or Madam:

America's Community Bankers ("ACB")[1] welcomes the opportunity to comment on the Federal Trade Commission's ("Commission") proposed regulation[2] to implement those provisions of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA")[3] designed to combat identity theft and provide a period for the effectiveness of "active duty alerts."

ACB Position

Protecting consumers from identity theft and fraud is a major priority for community banks. ACB supports the reasonable implementation of the strong identity theft provisions of the FACTA. ACB commends the Commission for its efforts to provide additional guidance on the implementation of the act by proposing definitions for "identity theft" and "identity theft report." However, ACB is concerned that the implementing regulations may dilute the effectiveness of these provisions by expanding their coverage to non-identity theft frauds for which consumers already have effective remedies. Existing remedies for check fraud, unauthorized use of credit cards, ACH fraud and other payments related frauds are adequate and effective. Moreover, a plain reading of the FACTA's identity theft provisions does not support the inclusion of other types of fraud within the definition of "identity theft."

While community banks do not believe that the real victims of identity theft should be burdened with unnecessary restrictions on their rights, ACB members strongly believe that the implementing regulations must guard against abuse of the FACTA's powerful tools by those who would use them to wipe out negative, but legitimate, credit information. To help insure legitimacy of complaints filed, ACB urges the Commission to require that an identity theft report be filed with an appropriate law enforcement agency with legal authority to investigate or prosecute an alleged identity theft. ACB believes that in the context of blocks of negative information, consumer reporting agencies and furnishers of information should have the option

[1] America's Community Bankers represents the nation's community banks of all charter types and sizes. ACB members pursue progressive, entrepreneurial and service-oriented strategies in providing financial services to benefit their customers and communities.
[2] 69 Fed. Reg. 23370 (April 28, 2004).
[3] Pub. L. No. 108-159 (December 4, 2003).

900 Nineteenth Street, NW ★ Suite 400 ★ Washington, DC 20006
Phone: (202) 857-3100 ★ Fax: (202) 296-8716 ★ www.AmericasCommunityBankers.com

of requiring a consumer to file a face-to-face complaint with a law enforcement official in addition to a previously filed electronic, telephonic or other automated system complaint. Additionally, ACB believes that the final "identity theft report" definition should give furnishers at least ten business days within which to request additional information from consumers who wish to block negative credit history.

ACB is concerned that the proposed 12-month period for active duty alerts may be inadequate to protect deployed armed forces personnel. ACB requests that the Commission consider extending the period to two years.

Proposed Definitions

Identity Theft. As proposed, the Commission would define "identity theft" to mean, "a fraud committed or attempted using the identifying information of another person without lawful authority." The Commission proposes to define "identifying information" (using the definition found in 18 U.S.C. 1028(d)(4))[4] to mean, "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any: (A) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, employer or taxpayer identification number; (B) Unique biometric data such as a fingerprint, voice print, retina or iris image, or other unique physical representation; (C) Unique electronic identification number, address or routing code; or (D) Telecommunication identifying information or access device" (Emphasis added)

In enacting Title I of FACTA, Congress sought to focus private and public sector resources on combating identity theft, or the assumption of a person's identity to commit financial fraud. ACB is concerned that the proposed definition of "identity theft" expands the definition beyond what was intended by Congress. We urge the Commission to limit the scope of the implementing regulations of the FACTA's powerful tools to identity theft and not dilute their effectiveness by diverting their use to other types of fraud – for which consumers already have effective remedies.

For example, the definition of "identifying information" is broad enough to include account numbers and credit card numbers. As a consequence, the definition of "identity theft" can be read to include types of financial fraud other than identity theft, such as check fraud and credit card fraud. These are serious crimes against consumers, but they do not constitute identity theft. Consumers can more easily detect these crimes through inspections of statements and notices from financial institutions. However, in an identity theft, the criminal assumes the identity of the victim to open a new account or enter into a new extension of credit and uses artifices to prevent detection of the crime by the victim.

The distinction between true identity theft crimes and more conventional payments related fraud is important. Conventional payments fraud includes: check fraud, unauthorized credit card use, ACH fraud, and other payments related fraud.

---

[4] Section 1028 of title 18, among other matters, makes unlawful the use or transfer of the identifying information of another person to commit, or to aid and abet, a violation of a Federal law or a felony under State or local law. 18 U.S.C. 1028(a)(7).

Federal and state laws provide the victims of conventional payments fraud with significant consumer protections. For fraud related to the unauthorized use of electronic funds transfer transactions (e.g., debit card, ACH, telephone transfers, etc.), the regulations implementing the Electronic Funds Transfer Act[5] require financial institutions to provisionally reimburse a consumer within 10 business days of the reported fraud. Fraud related to the unauthorized use of a credit card provides consumers with similar protections, and adverse credit reports explicitly are prohibited on any disputed credit transaction[6]. Additionally, the laws governing the payment of checks[7] provide consumers up to one-year to report a fraudulent check and allow a consumer to seek compensatory damages from a financial institution.

Consumers through a cursory review of their monthly statements can easily identify conventional payments related fraud, and once reported to a financial institution, such fraud is rarely reported to the consumer reporting agencies. In the event information relating to a conventional payments related fraud is reported to a consumer reporting agency, long-standing FCRA accuracy dispute requirements[8] allow the consumer to correct easily the mistake.

Moreover, support for not including payments related fraud within the definition of "identity theft" comes from both the plain language of Section 605A(a) of the FCRA[9], and the scheme of rights and remedies under Title I of FACTA. Section 605A(a) of the FCRA provides that a consumer who asserts in good faith that he or she "has been or is about to become a victim of fraud or related crime, including identity theft" has the right to have included in his or her consumer report an "initial fraud alert." The language of 605A(a) evidences the intent of Congress to distinguish between fraud and fraud that is the result of identity theft.

Additionally, Title I of the FACTA provides two different sets of rights and remedies to consumers: one set that applies to victims and potential victims of fraud or related crime, including identity theft; and another set of rights that applies only to consumers who file identity theft reports. As noted above, section 605A(a) entitles the former group of consumers to request an initial fraud alert that lasts for 90 days.[10] Consumers who file identity theft reports have additional rights. These consumers have the right to an "extended alert," which provides the same protections of the initial alert for a period of seven years.[11] They have the right to request that consumer reporting agencies block information on a consumer report that results from an alleged identity theft[12]. Additionally, once an identity theft report has been lodged with a credit reporting agency or a furnisher of information related to identity theft, FACTA prohibits the furnisher from re-furnishing the questionable information.

We urge the Commission to clarify that "identity theft" does not include non-identity theft financial fraud. Otherwise, important private and public resources needed to combat identity theft will be diverted for purposes not anticipated by Congress.

---

[5] 12 CFR 205.
[6] 12 CFR 226.12.
[7] Uniform Commercial Code, Articles 3 and 4.
[8] 15 U.S.C. 1681i.
[9] As amended by section112(a) of the FACTA.
[10] The initial fraud alert imposes on the users of consumer reports a duty to verify the identity of the consumer, prior to establishing a new credit plan or issuing an additional credit card on an existing account. Section 605A(h) of the FCRA, as amended by section 112 of FACTA.
[11] Section 605A(b) of the FCRA, as amended by section 112(b) of the FACTA.
[12] Section 605B of the FCRA, as amended by section 152 of the FACTA.

ACB supports the Commission decision to include, in the definition of "identity theft," the words "without lawful authority" in an effort to prevent individuals from colluding with each other to obtain goods or services without paying for them and then trying to allege that the transaction resulted from identity theft

Identity Theft Report. Proposed section 603.3 (a) would define "identity theft report" to mean a report "(1) That alleges identity theft with as much specificity as the consumer can provide: (2) That is a copy of an official, valid report filed by the consumer with a Federal, State, or local law enforcement agency, including the United State Postal Inspection Service, the filing of which subjects the person filing the report to criminal penalties relating to the filing of false information, if, in fact, the information in the report is false; and (3) That may include additional information or documentation that an information furnisher or consumer reporting agency reasonably requests for the purpose of determining the validity of the alleged identity theft...." [13]

Proposed section 603.3(b) provides illustrative examples of the specificity contemplated for "identity theft reports." Proposed section 603.3(c) provides illustrative examples of the circumstances under which a furnisher of information or credit reporting agency can require additional validation of an allegation of identity theft and the type of validation that could be required under those circumstances.

ACB believes that there is potential for abuse of the powerful consumer remedies under the FACTA. The ability to block negative, but legitimate, credit report information through an allegation of identity theft will tempt not only individuals with poor credit histories, but also "credit repair" firms. The first line of defense against abuse of this important tool is the law enforcement agency that receives the complaint.

Section 603(p)(4) of the FCRA requires that the consumer file the identity theft report with "an appropriate Federal, State or local law enforcement agency." The proposed regulation only requires that the report be filed with a law enforcement agency. It does not require filing with an "appropriate" law enforcement agency. We urge the Commission to require that the identity theft report be filed with an appropriate law enforcement agency that has legal authority to investigate or prosecute the alleged identity theft. A law enforcement agency with jurisdiction over the matter would have a greater interest in insuring the legitimacy of complaints filed with the agency than a law enforcement agency without authority to act on the complaint.

The examples in proposed part 603.3(c) rightfully place more credence on reports filed in person with a law enforcement officer than ones filed electronically. ACB is concerned with the proposal's reliance on automated systems for receiving complaints, particularly in connection with requests for blocks of negative information. In a footnote, the Commission acknowledges that automated systems can be abused.[14] ACB believes that in the context of requests for blocks of negative information, credit reporting agencies and furnishers of information should always have the option of requiring the consumer to file a face-to-face complaint with a law enforcement official in addition to a previously filed electronic, telephonic or other automated system complaint.

---

[13] 69 Fed. Reg. 23377 (April 28, 2004).
[14] 69 Fed. Reg. 23372 (April 28, 2004).

Under the proposal, a credit reporting agency or furnisher of information would have five business days from receipt of an identity theft report or request for service to ask the consumer for additional information to validate the claim of identity theft.[15] ACB believes many furnishers, particularly small ones, will need more than five business days to request additional information from the consumer. The furnisher may need time to receive the report, process it, review its contents, and search its own files before it realizes that it needs additional information. Therefore, we believe it would be more appropriate to allow a request to be made within ten business days.

Active Duty Alerts May Need to Extend Beyond One Year

The Commission has proposed a 12-month active duty alert. An active duty alert, like an initial fraud alert, requires potential creditors to take certain steps to confirm the identity of a credit applicant seeking credit in the name of the consumer who is the subject of the alert.

The active duty alert will help armed forces personnel from falling victim identity theft whenever they are deployed in locations or situations where they will be unlikely to apply for credit or manage their financial accounts. Section 112 of the FACTA requires the Commission to determine the duration of an "active duty alert," which the FACTA sets at a minimum of 12 months. [16] ACB is concerned that the proposed 12-month period does not adequately take into account the possible time active duty personnel are deployed.

For example, on April 15, 2004, the U.S. Secretary of Defense announced that the U.S. military would keep about 21,000 American soldiers, scheduled to end their one-year tour of duty in April, in Iraq beyond April.[17] ACB is concerned that the proposed duration for active duty alerts will not adequately protect fighting men and women who are currently deployed overseas. ACB suggests that the Commission consult with the Office of the U.S. Secretary of Defense to determine whether a more reasonable time period might be two years.

Conclusion

ACB supports the reasonable implementation of the identity theft provisions of the FACTA and commend the efforts of the Commission to implement those provisions through this regulation. ACB urges the Commission to:

(1) clarify that "identity theft" does not include check fraud, unauthorized use of credit cards, ACH fraud and other payments related fraud, for which there are already effective remedies;
(2) require that an identity theft report be filed with an appropriate law enforcement agency with legal authority to investigate or prosecute an alleged identity theft;
(3) allow credit reporting agencies and furnishers of information to require a consumer to file a face-to-face complaint with a law enforcement official in addition to a previously filed electronic, telephonic or other automated system complaint, in the context of requests for blocks of negative information;

---

[15] 69 Fed. Reg. 23378 (April 28, 2004).
[16] Section 605A(c) of the FCRA.
[17] (*Online NewsHour; www.pbs.org/newshour/update)*

(4) allow furnishers of information ten business days within which to request additional information from a consumer who seeks to block negative information; and
(5) consider extending the time period for active duty alerts to two years.

We look forward to working with the Commission on this proposal. Thank you for the opportunity to comment on this important matter. Should you have any questions, please contact the undersigned at 202-857-3121 or via e-mail at cbahin@acbankers.org, or Rob Drozdowski at 202-857-3148 or via e-mail at rdrozdowski@acbankers.org.

Sincerely,

Charlotte M. Bahin

Charlotte M. Bahin
Senior Vice President
Regulatory Affairs