June 15, 2004

Donald S. Clark
Secretary
Federal Trade Commission
Office of the Secretary
Room H-159 (Annex J)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20850

Re: FACTA Identity Theft Rule, Matter No. R411011

Dear Mr. Clark:

On behalf of the National Business Coalition on Privacy and E-Commerce, we are pleased to have the opportunity to submit comments on the Federal Trade Commission's ("Commission") proposed rule that would further define the terms "identity theft" and "identity theft report" in section 603(q) of the Fair Credit Reporting Act ("FCRA").[1] These terms are critical to the implementation of extended fraud alerts and the blocking of consumer information under sections 605A and 605B of the FCRA,[2] as well as to the duties of a business entity to provide information to a consumer under section 609(e) of the FCRA[3] or to discontinue furnishing data pursuant to section 623(a)(6).[4]

The Coalition is comprised of nationally recognized companies from diverse economic sectors dedicated to the pursuit of a balanced and uniform national policy pertaining to electronic commerce and privacy. Our member companies are top competitors in the e-commerce marketplace, and are strongly committed to ensuring the privacy and security of our customers, both on-line and off-line.

We commend the Commission for its serious effort to balance several important considerations: the ability of consumers to mitigate the effects of threatened or actual identity theft with the duty of consumer reporting agencies ("CRAs") to maintain and protect accurate information about consumers. We are concerned, however, that portions of the proposed rule suggest that some of the statutory prerequisites to an identity theft report may be omitted, which would allow the system for protecting and correcting consumer information to be abused. Accordingly, we recommend that the Commission clarify the rule in certain respects.

---

[1] *See* 15 U.S.C. § 1681a(q)(3), (4). These definitions were added by section 111 of the Fair and Accurate Credit Transactions Act, 2003 ("FACTA"), Pub. L. No. 108-159, 117 Stat. 1952 (Dec. 4, 2003).
[2] *See* 15 U.S.C. §§ 1681c-1, 1681c-2. These sections were added by sections 112 and 152 of FACTA.
[3] *See* 15 U.S.C. § 1681g(e). This section was added by section 151(a)(1) of FACTA.
[4] *See* 15 U.S.C. § 1681s-2(a)(6). This section was added by section 154(a) of FACTA.

1. Alerts and Blocks

Before turning to comments on specific provisions, we believe it is helpful to review the statutory structure of fraud alerts and information blocking under sections 605A and 605B and the role of an identity theft report in that process. The provisions in FACTA on identity theft envision three different levels of consumer protection in instances in which an identity theft may occur, has occurred, or has contaminated a consumer's file.[5]

- First, under FCRA section 605A(a), if a consumer "asserts in good faith a suspicion that [he or she] has been or is about to become a victim of fraud or a related crime," such as identity theft, the consumer may request a CRA to place an initial, or one-call, alert in the consumer's file.[6] This alert has a duration of 90 days.

  The purpose of the initial alert is to prevent the misuse of a consumer's identity when there may be some reason to believe this could occur, such as through the theft of a wallet or purse. Because the foundation for the initial alert is simply the "suspicion" that an identity theft may occur in the future, a consumer is not required to demonstrate an actual identity theft, and the only documentation that a CRA may require before entering the initial alert is "appropriate proof" of the consumer's identity. In keeping with the preventive purpose of the initial alert, a CRA's duties are limited to placement of the alert, referring the alert to other CRAs, and providing to the consumer certain free access to his or her consumer file. Meanwhile, the duty of a user of a consumer report containing an initial or active duty alert is to contact the consumer by telephone, if a telephone number is included in the initial alert, or to take reasonable steps to verify the identity of the applicant before extending new credit. The 90-day time limit serves two functions: it covers the period in which an actual identity theft is most likely to occur, and it limits the time during which an alert may remain in a file without substantiation of an actual identity theft.

- Second, under section 605A(b), a longer term alert involving greater protections is warranted when a consumer contacts a CRA "to report details of an identity theft and [to] submit evidence that provides the [CRA] with reasonable cause to believe *that such identity theft has occurred*."[7] In other words, when a thief has taken an identity (or information about an identity) and has then used the information to obtain goods or services fraudulently, then the CRA must place in the file an extended identity fraud alert. This alert has a duration of seven years. In addition to placing the alert in the file and referring it to other CRAs, a CRA must exclude the consumer from any pre-screened lists for a period of five years

---

[5] Section 605A also provides for an active duty alert, which addresses a specific need of the nation's armed forces and which we discuss further below, but it is not tied to an identity theft report.
[6] 15 U.S.C. § 1681c-1(a); *see* H.R. Rep. No. 263, 108th Cong., 1st Sess. 39 (Sept. 4, 2003).
[7] H.R. Rep. No. 263, *supra* n. 4, at 39 (emphasis added).

and must give the consumer greater access to his or her file than is required in the case of an initial alert. The duty of a user of a consumer report with an extended alert is to contact the consumer by telephone or other method before extending new credit.

The extended alert differs in two principal ways from the initial alert. First, because of the potential harm from an actual identity theft, an extended alert will remain in place for several years so as to prevent the harm, and it entails more elaborate duties on the part of a CRA. Second, because of the lasting effect of an extended alert and the need to avoid frivolous identity theft claims that may be intended only to counter accurate but negative information in a consumer file, a consumer is required to provide substantial evidence of an actual identity theft in what amounts to a sworn statement. The legislative history explains that an acceptable identity theft report is one (a) that is filed with a law enforcement agency and (b) that subjects the individual filing the report to criminal penalties for any false statement.

The Coalition believes that the proposed rule generally reflects the appropriate evidentiary threshold for an extended alert. Put another way, the extended alert provides a necessary baseline of consumer protection for which the identity theft report was contemplated by the statute and described in the proposed rule. For the milder form of protection offered by an initial alert, a formal report is not necessary, and the proposed rule does not require one. However, for the more extensive protection of the actual blocking of information, as described below, we believe that CRAs should have the discretion to require additional verification of the identity theft alleged and of the consumer's identity.

- Third, under section 605B, if a consumer can identify in his or her file information that resulted from an identity theft – e.g., non-payment on a credit card account fraudulently opened in the consumer's name – then a CRA must block the reporting of this information. The affected consumer must provide to the CRA appropriate proof of identity, a copy of an identity theft report, an identification of the information on the consumer credit report that arises out of the alleged identity theft, and confirmation that the information is not information relating to any transaction by the consumer."[8]

  The blocking action is the most stringent action that can be taken with respect to a consumer file, and accordingly it has the highest evidentiary threshold. In addition to proof of identity and an identity theft report, a consumer seeking to block allegedly tainted information must identify that information and must confirm that it does not relate to any transaction in which the consumer in fact engaged.

---

[8] *See* 15 U.S.C. § 1681c-2(a).

Because of the impact of tradeline blocking on the substance of a consumer report, the Coalition recommends that this aspect of the rule be clarified to enable the CRAs to require additional verification of a theft or of the consumer's identity. Additionally, we note that under section 609(e), a retailer or other business is entitled to obtain both a law enforcement report and an affidavit before taking action. A tradeline block is at least equivalent in effect to the 609(e) duty to provide information, and, as a matter of policy, the FTC should allow the CRAs to seek a supporting affidavit when appropriate.

Because the extended alert and tradeline blocking protections are triggered by an actual identity theft and the filing of an identity theft report, the definitions of the two terms have critical importance. An "identity theft" is defined as a "fraud" committed using the identifying information of another person.[9] The Commission is authorized to define the term further.

An "identity theft report" has three "minimum" requirements: a qualifying report must (i) allege an identity theft, (ii) be a copy of "an official, valid report" filed with a law enforcement agency or such other agency deemed appropriate by the Commission, and (iii) subject the person filing the report to criminal penalties for any false information in the report.[10] The statutory definition is consistent with the commonly understood meaning of the term.[11] According to Chairman Oxley, an identity theft report is "typically a police report."[12] The Commission has authority to go beyond these minimums.

This structure of consumer protections and the statutory definitions of identity theft and identity theft report are based on three principles that should underlie the Commission's regulations:

1. An identity theft report must allege the elements of an identity theft: the commission of a fraud involving the unauthorized use of information about a consumer.

2. Because of the significance of a tradeline block and the risks associated with an unwarranted block, an identity theft report must have the attributes of reliability: a report made to a law enforcement agency and one that is subject to criminal penalties for any false statements.

---

[9] 15 U.S.C. § 1681a(q)(3).
[10] *See* 15 U.S.C. § 1681a(q)(4).
[11] The Commission's website, for example, states that an identity theft "occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes." *See* http://www.consumer.gov/idtheft/.
[12] *See* 149 Cong. Rec. E2513 (Nov. 21, 2003).

3. The prerequisite common to all of the alerts or blocks is "appropriate proof of identity." If someone other than the affected consumer were able to use any of the alert or blocking mechanisms to gain access to a consumer file, then the accuracy and confidentiality of consumer information is at risk. This prerequisite acknowledges the responsibility of the CRAs to maintain the security of consumer data.

With this background, we turn to specific provisions of the proposed rule as follows:

2. Definition of "Identity Theft"

A. Definition of Identity Theft (section 603.2(a)). The Coalition supports this definition. Identity theft is the unauthorized and fraudulent use of information about another person that otherwise is kept confidential. The definition captures the appropriate elements; it includes (a) a fraud that is attempted or committed, (b) using "identifying information" of another, and (c) without lawful authority. The Coalition's concern in other parts of the proposed rule, as discussed below, is that there are suggestions that non-fraudulent acts may constitute identity theft such as, for example, the theft of a credit card.

B. Definition of Identifying Information (section 603.2(a)(1)). The Coalition supports this definition as well; it encompasses the different kinds of information that could be used to commit an identity theft.

3. Definition of "Identity Theft Report"

The Coalition has several comments relating to the three elements of the definition that the Commission has proposed – the requirement for allegations of specific fact, the requirement for "an official, valid" law enforcement report, and the ability of a CRA to request additional verification.

A. Specificity Requirement (section 603.(a)(1), (b)). The proposed rule generally would require that a consumer allege an identity theft "with as much specificity as the consumer can provide." Proposed section 603.3(b) provides three examples of specificity. We agree with the concepts embodied in the proposal – that an identity theft must be alleged and that it must be alleged with appropriate specificity – but we are concerned that the articulation of the concepts, particularly in the examples, suggest or imply that a consumer may not actually have to meet the statutory prerequisites for an identity theft report. We believe the guidance should be unambiguous and, accordingly, we would make two specific recommendations.

First, section 603.3(a)(1) should be amended to clarify that a qualifying identity theft report is one "that alleges *each element of an* identity theft with as much specificity as the consumer can provide." (Emphasis added.) This addition would conform the definition of an identity theft report to the definition of an identity theft. As the statute

makes clear, an identity theft exists where there are three elements: (i) the commission of a fraud, (ii) using information of another on (iii) an unauthorized basis. If a CRA is to be obligated to place a seven-year alert on a file or to block information as unreliable, then it it is our view that any predicate identity theft report should include reliable statements of fact with respect to each element.

Second, the examples in section 603.3(b) seem to follow each of these three elements of identity theft, but, again, it would be helpful to make this point explicit. In addition, the example in 603.3(b)(1) seems to suggest that "a loss or theft of personal information" is, by itself, an identity theft. If so, the suggestion is inconsistent with the statute and the policies that underlie the statute, and the language of that provision should be removed. The Coalition, therefore, recommends that 603.3(b) be revised to state as follows (changes from proposed language are in italics):

> Examples of the specificity referenced in paragraph (a)(1) are provided for illustrative purposes only, as follows:
>
> (1) *With respect to the commission of a fraud,* specific dates relating to the identity theft such as *[phrase omitted]* when the fraud(s) using the personal information occurred, and how the consumer discovered or otherwise learned of the theft.
>
> (2) *With respect to the third party that committed the fraud,* identification information or any information about the perpetrator, if known.
>
> (3) *With respect to information used without authorization,* name(s) of information furnisher(s), account numbers, or other relevant account information related to the identity theft.
>
> (4) Any other information known to the consumer about the identity theft.

B. Report Requirement (section 603.3(a)(2)). We support this element of the definition; it accurately tracks the definition in the statute. We note in particular the reference to "an official, valid report."

We are opposed, however, to the Commission's suggestion in the preamble to the proposed rule that a complaint filed with the Identity Theft Data Clearinghouse may constitute an "official, valid" report.[13] The Commission appropriately observes that the

[13] *See* 69 Fed. Reg. 23370, at 23372 & n. 9.

Clearinghouse "is not designed to vouch for the truth of each individual complaint" but goes on to say that the specificity and verification provisions would give the Clearinghouse complaints the necessary elements of reliability. The Commission's view is contrary to the statute. An "official, valid" report is one that on its face demonstrates that the complainant is subject to criminal penalties for any false statements in the report. A CRA should not be required to accept other, unsworn reports because there may be some other indicia of reliability. Additionally, the specificity and verification requirements are themselves subject to a variety of conditions and thus may not in all cases perform the reliability function that the Commission assigns to them. Furthermore, as a matter of policy, it will be far easier for both consumers and the CRAs if it is clear at the outset that a sworn statement, as the "official, valid" modification requires, is required, rather than leave the acceptability of a complaint up to a range of factors dealing with specificity and verification that must be applied on a case by case basis.

B. Verification (section 603.3(a)(3), (c)). Section 603.3(a)(3) would permit a CRA to request additional information in order to determine "the validity of the alleged identity theft." We support this element of the definition of identity theft report. Before taking action that calls into question information in a consumer file, we believe a CRA should have the ability to confirm the validity of an alleged theft. Two of the illustrative examples, however, suggest a very limited ability on the part of a CRA to seek verification even in situations that call for it.

The first such example would preclude a CRA from requesting additional information even if the identity theft report took the form of a law enforcement report, accompanied only by details surrounding the identity of the officer taking the report. The only exception would require that there exists "an indication that the report was obtained fraudulently" or another identifiable concern. CRAs already receive and respond to a variety of law enforcement reports, and, regrettably, a significant percentage of these reports prove to be false or fraudulent, including situations where a consumer has made false assertions to a law enforcement officer. For instance, some reports contain the same police report number and thus appear to be merely photocopies of the same police report. Other forms submitted appear to have been torn from coupon books and are not police reports at all.

The fifth example is ambiguous and should be clarified to permit a CRA to request that allegations in a law enforcement report be sworn to. The example cited would prevent a CRA from requesting that a consumer fill out a different form if the same information appeared on a law enforcement report. To the extent that the example is simply designed to address one form versus another, we have no objection. However, particularly where a tradeline block is involved, CRAs need the discretion to require another "form" if the law enforcement report did not carry with it a criminal penalty for a

false statement. Since it is the goal of the legislation to encourage accuracy in consumer files, the Coalition believes that the example should be clarified on this point.[14]

The Coalition supports the remaining examples. The second illustrative example would allow it to request missing information in a law enforcement report, such as a birth date or a Social Security number.

The third and fourth examples present an appropriate contrast between an law enforcement theft report for the different purposes of a tradeline block and an extended fraud alert. In the example, a CRA may require that a report generated by an automated system – that is, without an officer present to hear the allegations – be supplemented by an affidavit and some form of identification if the report is submitted for a tradeline block. The CRA is not permitted to seek the same verification for an extended fraud alert. We believe that this distinction appropriately authorizes the CRAs to seek additional verification of identity theft where the requested protective measure is the stringent tradeline block.

With respect to all verification requests by a CRA, the proposed rule would require that the request be made within five business days of receipt of an identity theft report. We recommend that this time period be revised to ten business days as CRAs need a reasonable period of time in which to review an identity theft report and determine whether additional verification is necessary, and five business days will not allow for a meaningful review. With a shorter period, CRAs are likely to send out more requests for verification to ensure that it has not overlooked an issue on an identity theft report.

4. Other Comments

(A) Active Duty Alert (section 613.1). We strongly support the twelve-month duration for active duty alerts and would observe that this alert should be renewable for so long as a serviceman or servicewoman is on active duty. The active duty alert serves an important protective function. Soldiers and sailors on active duty are unlikely to be in a position to open new accounts or to incur new credit charges. The active duty alert will help prevent them from becoming identity theft victims, since the alert will notify merchants and others that use consumer reports that new entries to a consumer file or an application for credit from a consumer on active duty may warrant additional investigation.

The twelve-month period for the active-duty alert is the appropriate length. The term of active duty may vary from soldier to soldier, and the Commission observes that an active duty assignment typically does not last more than twelve months and for some

[14] It is also worth noting that a tradeline block is at least as significant an event as a business entity's duty to provide information to a victim of identity theft, and in the latter circumstance, the business entity is required to act only after both a police report and an affidavit are provided. The CRAs should have the discretion to seek an affidavit where circumstances indicate that an identity theft report alone may not be reliable.

service members, an active duty assignment is for a shorter period. The twelve-month period thus provides a sufficient period of protection. If active duty extends beyond twelve months, a serviceman or servicewoman can simply renew the alert. Requiring them to do so on an annual basis is comparable to other housekeeping tasks that must be completed on an annual basis and would not present a material burden.

(B) Proof of Identity (section 614.1). We generally support this section of the proposed rule. We would suggest that the Commission clarify that a CRA has discretion to seek some or all of the consumer file match information listed in section 614.1(b)(1). We believe this to be the meaning of the phrase "and/or." In some cases, a CRA finds it necessary to use all of the information listed in section 614.1(b)(1) to confirm the identity of a consumer. The "and/or" conjunction should be read to allow a CRA to require all of the listed information, if necessary, in order to confirm an identity before taking action with respect to a consumer file. Given the strong policy embodied in FACTA and the FCRA to prevent unauthorized access to a consumer file, we believe it is important that CRAs have the ability to seek, if necessary, the full range of information about a consumer's identity. In many cases, such information will not be required on the list, but it is important for the reliability of the consumer reporting process that CRAs have the ability to request it.

The proposed rule will have a substantial impact on the national CRAs, other CRAS, and the businesses that furnish consumer information to the CRAs. Accuracy and reliability are critical to the consumer reporting process, and to that end many national CRAs already have in place procedures intended to guard against and remedy identity theft. The concerns expressed above are intended to allow the Commission to take advantage of the work that has already been done in deterring and protecting against identity theft.

If you have any questions or would like a further elaboration of our views, feel free to call our Coalition counsel, Mr. Tom Boyd, at (202) 756-3372. We look forward to continuing to work with you as you seek to develop the regulatory structure pursuant to the I.D Theft issue or any other matters related to FACTA.

Sincerely,

Susan Pinder
Coalition Chair