



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:

The Consumer Data Industry Association (“CDIA”) respectfully comments on the Federal Trade Commission’s (“Commission”) proposed Identity Theft Rule. This rule would define certain new key terms in the Fair Credit Reporting Act (“FCRA”), as amended by the Fair and Accurate Credit Transactions Act (“FACT Act”). These terms are “identity theft,” “identity theft report,” and “appropriate proof of identity.” The rule would also determine the duration of an “active duty alert.”

CDIA is an international trade association representing the consumer reporting industry. CDIA’s members include the nationwide consumer reporting agencies as defined in section 603(p) of the Fair Credit Reporting Act (“FCRA”).¹ As amended by the FACT Act, the FCRA imposes significant obligations upon consumer reporting agencies, particularly the nationwide consumer reporting agencies, with respect to consumers who may be victims of identity theft. These obligations are triggered when a consumer who is concerned about “identity theft” provides “appropriate proof of identity” and produces an “identity theft report.” In addition, the FCRA, as also amended by the FACT Act, requires consumer reporting agencies to place an “active duty alert” in the file upon the request of a member of the armed services who qualifies for such an alert. Therefore, the terms that define the circumstances giving rise to these obligations will have a considerable impact on consumer reporting agencies.

¹ These agencies are identified as Equifax Information Services, LLC, Experian Information Solutions, Inc. and Trans Union, LLC.

Summary

CDIA concurs in the Commission's observations as to the importance of these definitions in protecting bona fide victims of actual or potential identity theft and the need to assure that the definitions will not enable the misuse of these protections to undermine the accuracy and integrity of consumer report information. In most respects the proposed rule's definitions appropriately balance the protection of victims with the need to prevent abuse of the system. CDIA believes, however, that in some important respects, the proposed rule and its illustrative examples create unnecessary ambiguity as to the definition of an identity theft report. This definition must include all the statutory elements of the definition of an identity theft, and it must allow consumer reporting agencies and information furnishers to rely upon authentic law enforcement reports and to validate these reports.

Comments

Identity theft significantly harms consumers, creditors and the integrity of consumer report information. CDIA and its members have implemented measures to address this crime and to help victims restore accurate credit information. CDIA worked with the FTC to develop the current voluntary fraud alert initiative, including automatic referral of fraud alert requests to other nationwide consumer reporting agencies. CDIA members regularly assist consumers who believe that information in their files is the result of identity theft. Through the E-OSCAR dispute resolution system, the nationwide consumer reporting agencies help consumers quickly remove or correct fraudulent trade-line information in their files.

In many respects, the FACT Act identity theft provisions reflect current industry practices to address identity theft, as well as those suggested by the FTC at its website: www.ftc.gov/idtheft. The FTC advises victims of identity theft to do the following:

1. Contact the fraud departments of any one of the nationwide consumer reporting agencies to place a fraud alert in the consumer's credit file (which will result in a referral of the fraud alert to the other two nationwide consumer reporting agencies).
2. Close credit accounts that the consumer knows or believes have been tampered with or opened fraudulently. Use the FTC's Identity Theft Affidavit when disputing new unauthorized accounts.
3. File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.
4. File a complaint with the FTC, which maintains a database of identity theft cases used by law enforcement agencies for investigations.

CDIA believes that the FACT Act identity theft requirements are intended to compliment existing industry and government measures designed to help identity theft victims. As the Commission observed, the statutory and regulatory definitions of “identity theft” and “identity theft report” are key to the implementation of the legal protections for these victims. The final rule’s definitions must cover the circumstances that protect bona fide victims. At the same time, experience shows that some unscrupulous consumers will make false allegations to consumer reporting agencies in an attempt to remove accurate information from their files or to interfere with the rights of true victims of identity theft. The definitions must be broad enough to provide convenient relief to the victims, while not facilitating fraud or perpetuating identity theft.

A consumer’s good faith suspicion that he or she has been or is about to become a victim of fraud or related crime, including identity theft, entitles the consumer to an initial fraud alert on his or her file at each of the nationwide consumer reporting agencies, as well as free access to the consumer’s file at each of the nationwide agencies.² Upon presenting an identity theft report and providing reasonable cause to believe that an identity theft has occurred, the consumer may request an extended alert in his or her file at a nationwide consumer reporting agency, and may obtain two free credit reports within a twelve-month period.³ In addition, the consumer’s name will be omitted from any prescreened lists by the consumer reporting agency for five years.⁴ Finally, with an identity theft report evidencing the consumer’s identity theft claim, a consumer may identify information in his or her file that is the result of identity theft and may direct that the information be removed.⁵

The consumer’s rights to fraud alerts and extended alerts apply only to the nationwide consumer reporting agencies. In addition to placing the appropriate alert in the consumer’s file, a nationwide consumer reporting agency must refer the alert to the other nationwide agencies, and the consumer is entitled to free file disclosures at those agencies as well. The consumer’s right to direct that the reporting of specified file information be “blocked” applies to all consumer reporting agencies, but only the nationwide consumer reporting agencies must refer the block request to the other nationwide agencies.

Although fraud alerts, extended alerts and file information blocks are each designed to help identity theft victims, each has different consequences with respect to the consumer’s file at the consumer reporting agency. In the case of fraud alerts and extended alerts, the principal effect is to require creditors to undertake additional measures to verify the identity of the person requesting credit in the consumer’s name.⁶

² FCRA § 605A; 15 U.S.C. § 1681c-1.

³ FCRA § 605A(b)(1); 15 U.S.C. § 1681c-1(b)(1).

⁴ FCRA § 605A(b)(1)(B); 15 U.S.C. § 1681c-1(b)(1)(B).

⁵ FCRA § 605B(a); 15 U.S.C. § 1681c-2(a).

⁶ Creditors may not open new credit accounts, issue new credit cards for an existing account or increase a credit limit unless the creditor uses “reasonable procedures to form a reasonable belief that the user knows the identity of the person” requesting the credit, new card, etc. In addition, the creditor must call a telephone number if it is provided by the consumer or take “reasonable

While this effect creates some difficulty for creditors, it may also interfere with consumers' ability to obtain credit and may significantly inconvenience the consumer. Because of the potential disadvantages to consumers from these file alerts, the additional benefit of free reports that accompany them may not provide sufficient incentive for unscrupulous consumers to falsely allege that they may be identity theft victims, or in the case of extended alerts, to provide a falsified identity theft report.

The same is not true in the case of an information block under section 605B. CDIA's members' experience with consumer report file information disputes shows that dishonest consumers will falsely claim that they have been identity theft victims and will provide falsified documents in support of those claims in order to have accurate, negative information removed from their files.

The FTC's supplementary information accompanying the proposed rule recognizes that the purpose for which the consumer provides the identity theft report (i.e., extended alerts or file information blocks) may determine how much information and detail a consumer reporting agency or a creditor may require when accepting an identity theft report. Because of the significant difference in the effect of an extended alert versus a file information block, CDIA fully supports this distinction and urges that it be reflected in the final rule.

CDIA offers the following specific comments on the proposed rule.

1. Definition of Identity Theft -- Proposed Rule § 603.2(a)

The proposed rule defines "identity theft" as "a fraud committed or attempted using the identifying information of another person without lawful authority." CDIA agrees with the Commission that, in order to trigger the important FCRA rights of potential identity theft victims and to enable them to avoid being actual identity theft victims, the definition should cover an attempted fraud, as well as the actual offense. CDIA notes, however, that an essential element of the offense is fraud or attempted fraud. The mere loss or theft of consumer's identifying information does not constitute identity theft. It may engender a good faith suspicion that the consumer could become a victim of identity theft and thus entitle a consumer to an initial fraud alert, but it does not provide the basis for an identity theft report.

The proposed definition of "identifying information" means "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," "including any telecommunication identifying information or access device as defined in 18 U.S.C. 1029(e)." The cited United States Code provision defines "access device" to include credit card and account numbers, mobile identification numbers, and personal identification numbers, that can be used alone or in conjunction

steps to verify the consumer's identity and to confirm" that the credit application is not the result of identity theft. In the case of an extended alert, the creditor *must* contact the consumer requesting the credit extension, etc. either in person, at the telephone number provided by the consumer or other reasonable contact method designated by the consumer.

with another access device to obtain money, goods, services or other thing of value. As a result of incorporating the US Code definition into the proposed rule, the rule's definition of identity theft could include the authorized use of a credit card, PIN or similar access device. CDIA understands that the Commission intends this result. However, affected industry members may not associate the crime of *identity* theft with the fraudulent use of a credit card number without identifying information. For that reason, in order to facilitate compliance, CDIA suggests that the final rule's definition of identifying information incorporate the current US Code definition of "any telecommunication identifying information or access device" The final rule could also provide that the definition would include the US Code definition as it may be amended, to reflect changes in technology. The portion of the definition of identifying information in Section 603.2(b)(4) of the final rule could read: "Credit card and other account numbers, mobile identification numbers and personal identification numbers, that can be used alone or in conjunction with another access device to obtain money, goods, services or other thing of value, and including any other telecommunication identifying information or access device as defined in 18 U.S.C. 1029(e)." Alternatively, the final rule could give current examples of what are included in "telecommunication identifying information or access device as defined in 18 U.S.C. 1029(e)."

CDIA agrees that an important element of the definition of identity theft is that the person's identifying information is used without lawful authority. As the Commission observes, individuals, such as guardians and attorneys-in-fact, may have lawful authority to use another's identifying information and may misuse that information to commit fraud. CDIA's members have experienced situations where consumers appear to have colluded with family members or friends to perpetrate a fraud or attempted fraud using their own identifying information. In those instances, the consumer refuses to prosecute the perpetrator of the fraud or attempted fraud. For that reason, CDIA believes that the final rule should provide that a consumer's refusal to prosecute the perpetrator of an identity theft is *prima facie* evidence that the consumer's identifying information was used with the consumer's lawful authority and thus does not involve identity theft.

2. **Definition of Identity Theft Report -- Proposed Rule § 603.3(a)**

The proposed rule defines "identity theft report" as 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 States 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."⁷

⁷ 69 Fed. Reg. 23377.

Although CDIA generally supports this definition, CDIA believes that additional clarification is necessary and strongly disagrees with the definition to the extent that it is predicated on the interpretation that an “official, valid” law enforcement report includes a complaint filed with the Commission’s Identity Theft Clearinghouse.

a. Specificity Requirement and Examples of Specificity

The proposed definition requires that the report allege identity theft with as much specificity as the consumer can provide. CDIA supports this element of the definition, and suggests that the final rule and its examples make clear that the report must specify all the elements of the offense of identity theft.

The first example provides for “[s]pecific dates relating to the identity theft such as when the loss or theft of personal information occurred *or* when the fraud(s) using the personal information occurred, and how the consumer discovered or otherwise learned of the theft.” 69 Fed. Reg. 23378 (emphasis added.). This example could be interpreted to mean that the loss or theft of personal information constitutes identity theft; however, the definition requires that the personal identifying information be used without lawful authority to commit a fraud or an attempted fraud. For that reason, we suggest that the definition of identity theft report require the consumer to provide as much specificity as possible as to each element of the offense: (i) the commission of a fraud or an attempted fraud, (ii) using the identifying information of another person, (iii) in an unlawful manner.

b. Requirement for an Official, Valid Law Enforcement Report

The Commission’s Supplementary Information states that, under the FACT Act definition of identity theft report, which the proposed rule would expand upon, “a consumer could opt to use a copy of a complaint filed with the Commission’s Clearinghouse as an “identity theft report” because such a copy would technically meet the statutory definition: it alleges identity theft, is filed with a federal law enforcement agency (i.e., the Commission), and, like all documents filed with federal agencies, is subject to criminal penalties for false filing (see 18 U.S.C. 1001).”⁸

CDIA respectfully disagrees with this observation. As the Commission also notes, its complaint system “is not designed to vouch for the truth of each individual complaint. It is simply designed to provide a central collection point for identity theft data. Victims who have filed complaints with the Clearinghouse have done so voluntarily, with no guarantee of obtaining any immediate, direct benefit such as the investigation of their cases.”⁹ There is nothing about the FTC’s Identity Theft Clearinghouse that would elevate a complaint filed electronically to the status of an “official” report. While FTC staff may consider the information for the purposes of evaluating identity theft trends and may, under certain circumstances, refer the information to law enforcement officials, there appear to be no established procedures for

⁸ 69 Fed. Reg. 23372, n. 9.

⁹ Id.

any FTC official to authenticate the information submitted in such a complaint. In fact, the consumer is given complete discretion in terms of how much information, including identifying information, the consumer wishes to provide. Nothing on the FTC's website alerts the consumer to the FTC's interpretation the complaint would subject the submitter to criminal penalties for filing false information. Indeed, because the consumer need not provide complete identifying information, such a representation would be an empty threat if it were made at all.

Moreover, the FTC's interpretation ignores the legislative history that Congress clearly intended the "valid, official" report to be a police report or similar law enforcement report. CDIA appreciates that only a minority of consumers who have self-identified themselves as victims of identity theft bothered to report the crime to the police. CDIA also recognizes that some consumers report difficulty in having the police accept a report of an identity theft crime.¹⁰ For that reason, the statute defines an "identity theft report" to include a copy of "an official, valid report" filed with "a Federal, State or local law enforcement agency, including the United States Postal Inspection Service, or such other government agency deemed appropriate by the Commission," and the filing of which subjects the person filing the report to criminal penalties for false information in the report.¹¹ The fact that the identity theft report may be filed with law enforcement agencies other than a local police department does not alter the statutory requirement that the report be "valid" and "official."

The FTC's interpretation that the a consumer's complaint filed with the Commission's Clearinghouse would technically meet the statutory definition of an "identity theft report" is also at odds with the instructions to consumers at the FTC's website. As noted above, there the Commission recommends that consumers file *both* a police report *and* a complaint with the Commission's Clearinghouse. CDIA agrees that consumers should file both a police report (or comparable law enforcement report) and a complaint with the Commission, and CDIA agrees that the Commission's website appropriately distinguishes between the two submissions.

CDIA understands that the FTC's observation about a complaint submitted to its Identity Theft Clearinghouse was intended as a basis for providing that data furnishers and consumer reporting agencies may request additional information for the purpose of verifying the identity theft report. Nonetheless, under the FTC's interpretation, if a data furnisher or a consumer reporting agency receives a copy of a complaint that purports to be one submitted on its Identity Theft Clearinghouse, the rule would require that the additional information or documentation be "reasonably" requested for the purpose of determining the validity of the alleged identity theft. CDIA submits that, if the only "report" that the consumer presents is a copy of an on-line complaint submitted to the

¹⁰ It is possible that some consumers who experience difficulty in this regard have experienced the loss or theft of identifying information, such as a wallet. While these circumstances may give rise to a good faith belief that the consumer could be a victim of identity theft and thus support a fraud alert, they do not constitute the elements of identity theft because no fraud or similar criminal offense has occurred. In that case, the police may not accept an identity theft report.

¹¹ FACT Act § 111; codified at FCRA § 603(q)(4); 15 U.S.C. § 1681a(q)(4).

