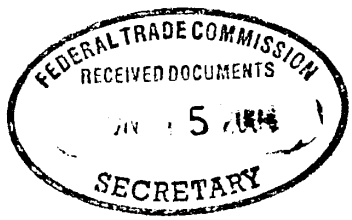
EQUIFAX



Equifax Information Services LLC
1550 Peachtree Street, NW
Atlanta, Georgia 30309
(404) 885-8000

June 15, 2004

Federal Trade Commission
Office of the Secretary
Room H-159 (Annex J)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: FACTA Identity Theft Rule, Matter No. R411011

I. INTRODUCTION

Equifax Information Services LLC is a consumer reporting agency that furnishes consumer reports to its financial institution customers, other businesses that have a permissible purpose as defined in the Fair Credit Reporting Act (FCRA), and consumers. It is a subsidiary of Equifax Inc., a 105-year-old company and member of the Standard & Poor's (S&P) 500® Index, a global leader in turning information into intelligence, serving customers across a wide range of industries and markets, including financial services, retail, telecommunications, utilities, mortgage, brokerage, insurance, automotive, healthcare, direct marketing and transportation. Equifax Inc. is not a consumer reporting agency.

Equifax Information Services LLC (Equifax) appreciates the opportunity to submit formal written comments in the above referenced matter. Because Equifax is a consumer reporting agency, it has a profound interest in the issue of identity theft. We support the provisions of the FACT Act that seek to help prevent the occurrence of this crime and those that seek to help consumers repair the damage to their reputations and credit histories after they have been victimized. Many of the identity theft prevention and credit history restoration obligations contained in the FACT Act impact the operations of Equifax and other consumer reporting agencies. We are committed to helping the Federal Trade Commission (FTC) develop rules that implement the law in the most effective and efficient manner.

We commend the FTC for seeking to balance the rights of identity theft victims with the potential for abuse of the credit reporting system, by prescribing rules and definitions that take into account the practical application of these rights. Given the recognition of the need for this balance, Equifax's comments provide additional suggestions based on its experience in working with voluntary initiatives that it has established, many of which are incorporated by the FACT Act.

II. OVERVIEW OF THE RULE

Under the FACT Act, consumers that have been victimized by identity theft have certain new rights. They have the right to place a fraud alert on their file maintained by a consumer reporting agency in order to notify prospective lenders that the consumer's identity may have been compromised. In addition, the FACT Act creates a new alert that can be placed on consumer reports when the individuals are on active military duty. Consumers also are given the right under the FACT Act to block information from appearing on their consumer reports that is the result of fraudulent activity. Equifax supports these objectives of the FACT Act. In fact Equifax has accepted fraud alerts from consumers and placed them on their files since 1997. Equifax has also blocked information at a fraud victim's request since 1999.

Under the FACT Act, several of these consumer rights depend on the filing of an "Identity Theft Report," which in turn depends on a definition of "identity theft." For these rights to be exercised, it is necessary for a consumer reporting agency to properly identify the individual seeking to exercise them. However, it is also necessary for the identity theft report to be legitimate and valid. The FTC is authorized by the FACT Act to define certain terms and has done so in the proposed rule.

III. COMMENTS

A. The definition of "identity theft".

There is much in the definition of "identity theft" proposed by the FTC to commend it. Since an initial fraud alert may be placed on a consumer's file by a consumer reporting agency when the consumer has a suspicion that he or she "is about to become" a victim of fraud, including "attempt" to commit fraud as part of the definition is a logical and useful extension. Also, adding "without lawful authority" helps address situations where there may be collusion in committing fraud.

However, defining it as "any fraud committed using identifying information" may result in "identity theft" being over broad in light of the purpose of the FACT Act. The FACT Act is designed to help consumers who are fraud victims in relation to their consumer reports and the consumer reporting system rather than unrelated types of financial or other fraud that may be committed against individuals where consumer reports do not play a role. The consumer rights created by the FACT Act help consumers prevent future identity theft by allowing them to place fraud alerts on their files or mitigate damage by blocking fraudulently created accounts from appearing on their reports.[1]

[1] See footnote 1 of the Supplementary Information that accompanies the rule.

Fraud alerts when there has been no identity theft but only another type of fraudulent transaction for which consumer reports are not likely to be used does not help the individual. It may, in fact, hinder the consumer's ability to get credit or another benefit for which the consumer report is used. In fact, users of consumer reports are only required to take action based on a fraud alert on a consumer's report when the consumer applies for new credit or enters into a credit transaction other than using a credit card.[2] Users are not required to take any action when a credit card is used even if they had access to a consumer report at that time, which they typically do not. The rule should recognize that there is a balance between the consumer benefit of using fraud alerts for fraud victims and consumer harm and inconvenience from fraud alerts in the consumer reports of individuals who have not been victims.

Given the need to draw a balance, the rule should carefully define "identity theft" to only include situations where actual identity theft occurred. In the context of the Fair Credit Reporting Act, making unauthorized charges to a stolen or "borrowed" credit card should not be called identity theft for these purposes. Yet the definition covers it.

Fraud alerts on consumer reports make sense because the objective is to alert future credit grantors that the applicant may be a fraud perpetrator. Blocking fraudulently created accounts makes sense when the individual is applying for new credit because the fraudulent account should not be considered by a new creditor in making a credit decision. In the context of the Criminal Code, making it a crime to use a number, such as a credit card number, that may be used to defraud individuals, businesses or the government, makes sense. In the context of the FACT Act, calling the use of a stolen credit card or credit card number identity theft does not. Using a stolen credit card is a crime but does not by itself constitute identity theft. The fact that users are specifically permitted to extend credit on an open ended credit plan even if there is a fraud alert on the consumer's report without a FACT Act requirement to confirm the consumer's identity demonstrates that there is a distinction for purposes of the FACT Act

Consumer reports are used to establish new credit. Consumer reports are not typically used when an individual makes a charge to an existing credit card or credit card number. Placing a fraud alert on a consumer's file when the credit card has been stolen does not prevent the use of the card. Blocking an account that belongs to the consumer from appearing on the consumer's report when the consumer applies for credit does not prevent the stolen card from being used.[3] Placing a fraud alert on a file when the consumer is not an identity theft victim does not help the consumer in this context, but it

---

[2] FCRA §605A(h)(B)(i) – "In general—No prospective user of a consumer report that includes an initial fraud alert or an active duty alert in accordance with this section may establish a new credit plan or extension of credit, **other than an open-end credit plan**... in the name of the consumer, or issue an additional credit card on an existing account requested by a consumer, or grant any increase in credit limit on an existing credit account requested by a consumer ..." (emphasis added)

[3] Blocking the account that belongs to the consumer also prevents the reporting of accurate information that may benefit the consumer. The derogatory rating resulting from the fraudulent transactions should be removed through the normal consumer dispute process, but blocking the account prevents the consumer from getting the benefit of a good payment history. Blocking an account should not be a substitute for correcting information.

does makes it more difficult for the consumer to obtain new credit in the future. In addition, the consumer reporting agencies and creditors evaluating applications can be overburdened if all consumers whose credit cards have been lost, stolen or used without authority place alerts on their files.

Finally, it has been our experience that on occasion, an individual permits another to use his or her credit card to make a purchase, and then later, either intentionally or having forgotten, denies the charge claiming it was the result of identity theft. To address this type of situation, we believe that lack of consent of the individual claiming to be a victim should be an element of the definition of "identity theft."

We, therefore, recommend a clarification to the definition of "identity theft" to more closely track the purpose of the identity theft provision in the FACT Act and add the "consent" element.

We suggest the following revision to the definition:

> **The term "identity theft" means using or attempting to use any means of identification of another person without lawful authority and without the consent or knowledge of that person for the purpose of obtaining a financial product or service, such as a credit card or loan, or other product, service, or benefit in that person's name.**

B. Identity theft report.

The impact of identity theft reports is far reaching. Creditor collection efforts are impacted. Debts may not be transferred if an identity theft report has been filed and an account blocked. The information may not be furnished by the creditor to a consumer reporting agency if an identity theft report is presented to the creditor. The §603(p) consumer reporting agencies must refer to each other consumer complaints alleging identity theft. And creditors must follow additional steps before granting credit to a consumer whose file contains an alert. It is therefore essential that the validity of the identity theft report be properly determined.

Underlying the identity theft report process are two fundamental issues: 1) What constitutes an identity theft report? And 2) Is the identity theft report legitimate?

1. Definition of identity theft reports.

We commend the FTC for recognizing that identity theft reports can be fraudulent and used to make valid negative accounts disappear from consumer reports. Such activity could jeopardize the entire consumer reporting system. As discussed above, we have had experience with such occurrences. Requiring that the identity theft report include some specificity as to the crime can help prevent fraudulent claims and help resolve legitimate disputes. We also believe that the additional information cited in the examples that the consumer reporting agency may request goes a long way toward achieving the goal of specificity.

However, requiring that additional information can only be requested by a consumer reporting agency after the identity theft report is filed delays the process and adds additional costly steps and communications that do not serve the process well and may frustrate legitimate victims. Also, this additional information, by not being part of the actual identity theft report may not be subject to criminal penalties for providing false information. We recommend, therefore, that the FTC prescribe the contents of an identity theft report to specifically include the items cited in the examples in the definition of identity theft report.

At the minimum, an identity theft report should contain the dates relating to the identity theft, such as when the loss of personal information and/or the actual fraud occurred, if known; any information known about the perpetrator; names of creditors; account numbers; any additional information known by the victim and "identifying information" as defined in the rule; and name, contact information, badge number, and other identification information of the law enforcement officer taking the consumer's complaint. The information in the examples that *may* be requested should be put into the definition and be part of the identity theft report. Rather than requiring an exchange of correspondence, the process can be completed much more rapidly if the information is included in the first place.

Finally, as suggested by the FTC in question number 3 and in footnote 9 of the Supplementary Information (also addressed below), we believe that, unfortunately, unscrupulous individuals are unlikely to be deterred from filing false identity theft reports by the remote possibility of criminal penalties. We believe that identity theft reports should not be easily prepared or available. The automated preparation of identity theft reports or the report filed with the FTC's complaint system should not serve as identity theft reports. In fact, we believe that "an **official**, **valid** report filed by a consumer with an **appropriate** federal, state or local law enforcement agency...the filing of which subjects the person filing the report to criminal penalties relating to the filing of false information" means a law enforcement agency that has criminal enforcement responsibility regarding filing false documents.

Also, to be valid, the report must be filed for the purpose of law enforcement with an agency that is charged with investigating the substance of the complaint. We do not believe the FTC's complaint system meets this test. Therefore, at a minimum, we believe the definition of identity theft report should focus on the words "official," "valid" and "appropriate." All these elements need to be present for an identity theft report to be accepted and it should be defined as such. It need not be a defined as report filed with any government agency.

Finally, we believe consumers are more likely to be deterred from filing false identity theft reports and abusing the system if the report involves some face to face encounter with an official. This could be the police, postal inspector or some other law enforcement official. Forms completed anonymously on line or otherwise should not serve as valid or official identity theft reports.

2. Legitimacy of identity theft reports.

The next critical issue is how the consumer reporting agency can determine that the identity theft report is legitimate. As discussed above, requiring that an identity theft report be prepared by an appropriate law enforcement agency and that it be official and valid goes a long way toward minimizing the likelihood of abuse. However, the consumer reporting agency should also be able to take other information into account to determine whether the report is valid—more than merely asking the individual for further information. The rule should make clear that even if the consumer provides proper proof of identity and the report appears to be valid, the consumer reporting agency should be able to reject the identity theft report and not place an alert on the file or block an account if it believes that it is a fraudulent or not valid identity theft report.

The rules by which the validity of an identity theft report can be established are not easily defined in the rule. Rather this is the area where consumer reporting agencies should be allowed to develop and implement reasonable requirements that are flexible and that are based on experience. The report will most likely be received by mail. The consumer reporting agency may require some proof of authenticity; it should be allowed to verify the report with the law enforcement agency; and it should be permitted to take other additional steps that are appropriate given the nature and circumstances of the identity theft report.

C. Appropriate proof of identity.

Underlying the alert process and other new consumer rights is the fundamental issue of whether the consumer or their representative presenting themselves to the consumer reporting agency can be properly identified for the purposes of sections 605A, 605b and 609(a)(1)(A) of FCRA[4]

[4] The rule incorrectly refers 609(a)(1). The latter reference should be to section 609(a)(1)(A).

The individual claiming to be a fraud victim and asking that a fraud alert be placed on his or her file or that accounts be blocked should be properly identified. Consumer reporting agencies have developed procedures to properly identify consumers, particularly when they ask for a copy of their files. However, the rule places a new obligation on consumer reporting agencies relating to identifying the consumer. They are required to "develop and implement reasonable requirements" to determine proof of identity, to "ensure that the information is sufficient" and to "adjust the information to be commensurate with an identifiable risk of harm." In addition to these new requirements, the rule again provides examples. The requirement to establish reasonable procedures to identify individuals based on a risk analyses creates additional exposure and potential liability for consumer reporting agencies that is not warranted by the FACT Act. In addition to properly identifying individuals, they must now develop reasonable requirements and adjust them based on a risk of harm. If they guess wrong as to the risk of harm and make the wrong "adjustment" by denying an account block when it should have been accepted, or accepting one when it should have been denied, they appear to be liable under this rule.

But it is hard to imagine how the FTC envisions this operating in a practical way. A consumer will submit an identity theft report which will contain identification information, and ask that an alert be placed on his or her file, or that an account be blocked, or that an alert or block be removed. Should the consumer reporting agency then ask for additional proof of identity? Or can it search its database for the consumer's file and place the alert or the block? Must additional information be requested if the request is for a block as opposed to an alert or for the removal of either? But if a consumer fraudulently asks for an account to be blocked, isn't it most likely that the consumer is asking that his or her own account be blocked--in which case the consumer will have no problem presenting all the identifying information requested? Must more identifying information be requested when a consumer asks that the alert be removed? What can be requested? It must be remembered that the requests in most situations will not be made in person so any request for additional information will delay the implementation of the consumer's request.

The greatest risk of abuse may very well be a consumer who actually owes an account asking that it be blocked. How is asking for additional identifying information going to prevent the abuse? Won't only legitimate fraud victims be frustrated by additional questions? Given the volume of identity theft cases according to the most recent surveys and studies, we believe consumers are best served if they face the least bureaucracy and the least exchange of correspondence. The consumer reporting agencies should be permitted to accept the identity theft report and follow the consumer's wishes, provided the report contains enough identifying information to locate the credit file in its database, and provided the consumer reporting agency believes the identity of the person submitting the identity theft report and that the identity theft report is legitimate.

The identifiers listed in the example are generally adequate. We believe, however, that the examples should be part of the rule and that if the information listed is received as part of the identity theft report and matched to the database, the consumer reporting agency should be deemed to have complied with the rule and established appropriate identity. If a consumer reporting agency matches name, address, social security number and date of birth provided by the consumer with the information in its database, no requests for further identifying information will likely be needed. However, if the consumer reporting agency has reason to doubt the identity of the consumer, it should be permitted to request a copy of a government issued identification or utility bill or any other proof of identity.

However, in this connection, the examples listed for the file match need to be modified when made part of the rule. It should be clear that requiring an exact match of identifiers may result in fraud victims not getting the rights they are asking for. Identity theft often involves a fraud perpetrator changing the address or varying the name or social security number of a fraud victim. A fraud victim may provide an address that does not match exactly; a social security number may vary slightly from that on the consumer's file; the name may be a nickname or formal name (Bob vs. Robert, etc.) resulting in an inability to match if an exact match is required. Therefore, the rule should permit matching that conforms to the process used by the consumer reporting agency in providing consumer disclosures. It should be sufficient if the consumer reporting agency, using the identifiers listed in the examples, forms a reasonable belief that the individual is who he or she claims to be.

Since the initial, extended and active duty alerts may be placed on a consumer's file upon the request of a personal representative, the FTC should also address what kind of identifying information is required of the personal representative of the consumer. To prevent fraudulent use of the alerts, we believe that any personal representative should be required to present a court order or a certified and notarized power of attorney appointing the individual as a personal representative. Otherwise, anyone can appear as a personal representative asking for an alert or a block or its removal on behalf of another consumer.

Finally, since the alerts must be referred by one nationwide consumer reporting agency to the others, as well as data furnishers, specificity in the identification rule is essential. Allowing adjustments commensurate with the risk of harm allows too much leeway and could result in different standards and risk evaluations by nationwide consumer reporting agencies and data furnishers. One data furnisher or nationwide consumer reporting agency may accept the proof of identity and the others not, resulting in confusion to consumers and the system.

Therefore, we recommend that name, address, social security number and date of birth be the identifiers required as proof of identity and that they be part of the rule, not examples. But, consumer reporting agencies may use reasonable and flexible procedures, as needed, to determine the identity of a consumer if there is a reasonable basis for doubt.

IV. SPECIFIC ANSWERS TO SELECTED QUESTIONS

We believe we have answered the majority of the specific questions raised by the FTC above. However, we will elaborate answers to certain questions below:

Question B. 3. To deter abuse of the credit reporting system, the Act requires that an identity theft report be subject to criminal penalties for false filing and allows consumer reporting agencies and information furnishers to reject a block or continue furnishing information. How likely is it that these safeguards will deter abuse of the credit reporting system? Are these safeguards less likely to deter abuse when automated systems are available to generate reports? If so, why? If not, why not? Are there alternate ways to deter abuse other than what the FTC has proposed? What would be the advantages or disadvantages of these alternate approaches?

Answer: We believe it is appropriate to subject those who file false identity theft reports to criminal penalties. However, as discussed above, even with potential penalties, consumers attempting to block legitimate accounts from their files may not be deterred. Much will depend on the level of enforcement. If fraudulent identity theft reports are prosecuted and the prosecutions publicized, there would be a deterrent effect. If they are not prosecuted, which we fear might happen, there would be no deterrent.

We believe the most effective way of deterring abuse is to require identity theft reports to be filed with law enforcement agencies in an in-person setting. As the FTC noted in footnote 9 to the Supplementary Information, "The FTC complaint system...is not designed to vouch for the truth of each individual claim" even though the complaints are technically identity theft reports since false reports are subject to criminal penalties. For the reasons stated above, we do not believe they are appropriate or valid identity theft reports. Those filing false reports filed on line with the FTC or other agencies are unlikely to be greatly deterred by potential criminal penalties, particularly if the likelihood of enforcement is remote.

Questions C related to Active Duty Alerts.

Comment: There is nothing in the rule that requires someone asking for an active duty alert to show proof that the individual is on active duty. Although the likelihood of abuse may be remote, the possibility of mischief is present. All that is required to place an active duty alert on a file is a request with appropriate proof of identity, and the request can be made by anyone acting on behalf of the consumer. Since the consumer

reporting agency is, according to the rule, to adjust the identifying information requested to be commensurate with the risk of harm, it is likely that any request will be granted. We suggest that the request be accompanied at least by some evidence that the individual is on active duty.

V. CONCLUSION

We appreciate this opportunity to provide comments on the Identity theft rule and look forward to continuing to work with the FTC as we implement practices and procedures to fight identity theft. That battle will be facilitated by appropriate rules that are workable and practical in the credit and consumer reporting industry.

Sincerely,

/s/ Kent E. Mast

KENT E. MAST
General Counsel
Equifax Information Services, LLC
Equifax Inc.