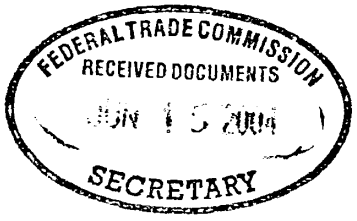
Jodi Golinsky
Vice President &
Senior Regulatory Counsel

MasterCard International
Law Department
2000 Purchase Street
Purchase, NY 10577-2509
914 249-5978
Fax 914 249-3648
E-mail jodi_golinsky@mastercard.com
www.mastercard.com

MasterCard International



June 15, 2004

The Federal Trade Commission
Office of the Secretary
Room 159-H (Annex J)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: FACTA Identity Theft Rule, R-411011

To Whom It May Concern:

MasterCard International Incorporated ("MasterCard")[1] submits this comment letter in response to the Proposed Rule ("Proposal") issued by the Federal Trade Commission ("Commission") regarding the definitions of "identity theft" and "identity theft report," as well as the duration of an "active duty alert" under the Fair Credit Reporting Act ("FCRA") as amended by the Fair and Accurate Credit Transactions Act ("FACT Act"). MasterCard appreciates the opportunity to comment on the Proposal.

Definition of "Identity Theft"

Section 111 of the FACT Act amends the FCRA to include a definition for the term "identity theft." Specifically, the statute defines "identity theft" to mean "a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation." The definition of "identity theft" is central to several provisions in the FCRA as amended by the FACT Act. For example, an identity theft report is a report that must allege an identity theft.[2] Section 615(e) of the FCRA directs the Commission and other agencies to establish certain guidelines "regarding identity theft." Under Section 609(d) of the FCRA, any consumer who "expresses a belief that [he or she] is a victim of fraud or identity theft" is entitled to a summary of various rights. Under Section 609(e) of the FCRA, a consumer can obtain certain information from a business entity resulting from an alleged identity theft.

[1] MasterCard is a SEC-registered private share corporation that licenses financial institutions to use the MasterCard service marks in connection with a variety of payments systems.
[2] Issues related to identity theft reports will be discussed under a separate heading.

The Proposal defines identity theft to be "a fraud committed or attempted using the identifying information of another person without lawful authority." Although the Commission has improved the definition of "identity theft" in some respects, we strongly urge the Commission to amend the definition further to reflect the scope of activities intended by Congress. "Identity theft" is commonly understood to be an actual fraud committed involving an assumption of another's identity, and is therefore distinct from an attempted identity theft. This distinction is critical because we believe Congress intended to have law enforcement, consumer reporting agencies, creditors, data furnishers, and business entities focus their limited resources (*e.g.*, pursuant to Sections 609(e) or 615(e) of the FCRA) on actual instances of identity theft—*not those that have been prevented already.*

We believe that a broad definition of identity theft will dilute resources dedicated to assisting actual victims of identity theft, thereby not providing benefits to consumers. The Commission suggests that a broader definition is justified because consumers may have inquiries included in their consumer report that do not belong as a result of an attempted identity theft and that "victims should be entitled to take advantage of the [FACT] Act to have these inquiries removed." We note that consumers who are victims of attempted identity theft have the ability to correct their consumer reports using the dispute process already provided for in the FCRA. Thus, an expanded definition of "identity theft" is not necessary to provide victims a remedy to correct data on a consumer report.[3] The Commission also suggests that a broad definition is necessary because "victims who have learned of attempts by an identity thief and want to reduce the likelihood that the identity thief will succeed in opening new accounts may want to place an 'initial fraud alert' on their consumer reports." We respectfully note that the statute does not require a consumer to be a victim of "identity theft" in order to place an initial alert in the consumer's file. All that is necessary to place an initial alert in the file is for the consumer to assert "in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime." We believe that a consumer who has been a victim of attempted identity theft could make such an assertion regardless of whether "identity theft" were to also mean "attempted identity theft."

If the Final Rule includes "attempted" identity theft in the definition of "identity theft," we ask the Commission to provide for a clear definition of what "attempted" identity theft means. MasterCard believes that the scope of "attempted" identity theft should coincide with the Commission's stated policy purposes for including it in the definition of "identity theft." In particular, it should be the type of attempt that would result in an inquiry on the consumer's consumer report. Therefore, a fraudulent application for a credit card that is denied after a consumer report is obtained could be included as "attempted" identity theft. However, a foiled pretext call would likely not rise to the same level.

---

[3] Congress gave victims of identity theft a more powerful tool to correct consumer reports that have been damaged by identity theft. We do not believe that the presence of a false inquiry on a consumer report warrants the dilution of resources to help actual victims of identity theft, especially because other effective remedies are available to those who have experienced attempted identity theft.

Under the Proposal, an identity theft would involve the misuse of someone's "identifying information." This term is defined quite broadly to include any name or number that can be used, alone or with other information, to identify an individual. We urge the Commission to refine this definition to encompass only the types of information that can be used to assume an individual's identity. For example, misuse of a credit card number, while a serious crime, is not necessarily "identity theft"—it is account fraud. However, misuse of a consumer's name and Social Security number would likely rise to an "identity theft." We also note that the examples of "identifying information" in the Proposal would appear to be broader than the definition itself. Specifically, "identifying information" is defined to be a name or a number, but the examples include a fingerprint and other information that would not appear to be a name or a number. We ask the Commission to clarify this point in the Final Rule.

The Commission has also proposed that for there to be an identity theft, the person's identifying information must be used to commit the fraud "without lawful authority." The Supplementary Information explains that "[a]dding 'without lawful authority' [to the definition] prevents individuals from colluding with each other to obtain goods or services without paying for them, and then availing themselves of the rights conferred" by the FCRA. We applaud the Commission for adding this concept to the definition of "identity theft." Indeed, we urge the Commission to include such an example in the text of the Final Rule as an example of activities that would be *per se* "without lawful authority." We also ask the Commission to clarify that "identity theft" does not include circumstances in which the "victim" obtained any benefit from the alleged fraud or where the "victim" voluntarily allowed the perpetrator to use the account in question.

Definition of "Identity Theft Report"

The FACT Act provides victims of identity theft with a powerful tool to rectify consumer files that have been damaged by identity theft. For example, an identity theft victim can block a consumer reporting agency from reporting data resulting from an identity theft if the consumer provides the agency, among other things, a copy of an identity theft report. And the consumer reporting agency can only in very limited circumstances decline to block, or rescind a block. Similarly, a victim can block a data furnisher from furnishing data resulting from identity theft to a consumer reporting agency if the victim provides the furnisher with an identity theft report. The statute does not allow furnishers to "unblock" such information unless the furnisher "knows or is informed by the [victim] that the information is correct."

By enacting the tradeline blocking provisions, Congress provided identity theft victims with useful tools to eliminate incorrect data resulting from identity theft. However, Congress also recognized that these blocking provisions could be devastating if misused by unscrupulous credit repair clinics and others seeking to eliminate accurate (but negative) data from credit files. Therefore, Congress required that a victim file an identity theft report as an indicator of legitimacy of the claim of identity theft before he or she could block the furnishing or reporting of information. Said differently, the identity theft report was intended to be of the type that could not be abused by credit repair clinics or fraudsters to suppress accurate information in a consumer's file. The Commission recognizes this

fact, stating in the Supplementary Information that an identity theft report "could provide a powerful tool for misuse, allowing persons to engage in illegal activities in an effort to remove or block accurate, but negative, information in their consumer reports."

The FACT Act defines an "identity theft report" to have "the meaning given that term by the Commission" but to mean "at a minimum" a report: (i) that alleges an identity theft; (ii) that is a copy of an official, valid report filed by a consumer with an appropriate federal, state, or local law enforcement agency, including the U.S. Postal Inspection Service, or such other government agency deemed appropriate by the Commission; and (iii) 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. The Commission has proposed to define the term to mean a report: (i) that alleges identity theft with as much specificity as the consumer can provide; (ii) that is a copy of an official, valid report filed by the consumer with a federal, state, or local law enforcement agency, including the U.S. Postal Inspection Service; (iii) the filing of which subjects the person filing the report to criminal penalties relating to the filing of false information if the information in the report is false; and (iv) that may include additional information or documentation that an information furnisher or consumer reporting agency reasonably requests under certain circumstances.

MasterCard appreciates that the Commission has attempted to craft a definition of an "identity theft report" that will allow the reports to be accessible to legitimate victims of identity theft without creating the potential for abuse. However, we believe the definition of "identity theft report" in the Proposal should be amended to enhance the integrity of such reports without making them too difficult for consumers to obtain.

Alleging Identity Theft With Specificity

According to the Supplementary Information, the Commission has added two protections to the statutory definition of identity theft report "to prevent abuses of the credit reporting system, without creating road blocks to a victim's recovery process." One of the protections involves requiring that a consumer allege identity theft "with as much specificity as the consumer can provide" as part of the identity theft report. The Proposal then provides illustrative examples of the "specificity" envisioned by the Commission, including specific dates relating to the identity theft, the perpetrator's identity, account information, and "any other information known to the consumer about the identity theft." The Commission states that the requirement to allege an identity theft "with as much specificity as the consumer can provide" will help provide sufficient safeguards against abuse. Although MasterCard believes that such information could assist furnishers and consumer reporting agencies in blocking the appropriate information, and that this provision therefore should be retained, we do not believe that the requirement will significantly deter abuse with respect to filing false identity theft reports. In this regard, a person seeking to abuse the system could provide the bare minimum of information necessary to qualify as alleging identity theft and claim that he or she is unable to provide any more specificity. Alternatively, we do not believe that it would be very difficult for a fraudster to lie with specificity.

Requesting Additional Information

The Proposal would allow furnishers or consumer reporting agencies to request additional documentation to help them determine the validity of the alleged identity theft request. According to the Commission, "the request for additional information is intended to compensate for a report which does not rise to the level of the ideal law enforcement report (*i.e.*, a detailed report taken by a law enforcement officer face-to-face with the consumer which contains identifying or other contact information for the officer.)" The additional information must be "reasonably" requested not later than five business days after the later of: (i) the date of receipt of the copy of the report filed with a law enforcement agency; or (ii) the date of the request by the consumer for the blocking. Furthermore, the request must be "for the purpose of determining the validity of the alleged identity theft."

MasterCard believes that it is critical that data furnishers and consumer reporting agencies be permitted to request the information they may need in connection with the consumer's filing of an identity theft report. Thus, we believe this concept should be retained with some modifications. In particular, we believe that a recipient of an identity theft report should be permitted to request any additional information it deems necessary for reasons other than simply to assess the validity of the consumer's claim. For example, a furnisher or consumer reporting agency may need additional information to carry out the service the consumer has requested, or to investigate the alleged crime. We also believe that the Commission should delete the five-business-day requirement with respect to the furnisher's or consumer reporting agency's request. The recipient of the report may need more than five business days to review whether a further request to the consumer is necessary. This will be particularly true if credit repair clinics attempt to flood furnishers or consumer reporting agencies with thousands of bogus identity theft reports in an effort to overwhelm the entity and run out the clock.

In addition to amending the Proposal with respect to how a furnisher or consumer reporting agency can request additional information, we urge the Commission to clarify that a furnisher or a consumer reporting agency is not required to perform the service requested by the consumer until the recipient of the report has: (i) had sufficient time to review the report's contents; and (ii) received any additional information requested in connection with the report. MasterCard believes this clarification is consistent with the Commission's intent and we therefore urge the Commission to provide explicit guidance in this regard.

Although the ability of a furnisher or consumer reporting agency to seek additional information should be retained for the reasons described above, it is worth noting that we do not believe that the requirement to provide specific information is a particular deterrent to those seeking to abuse the system. A fraudulent actor who is willing to lie to the furnisher or the consumer reporting agency by filing a false report is unlikely to be deterred by a requirement to lie with specificity when asked for more details.

Filing The Report With An "Appropriate" Law Enforcement Agency

As described above, we share the Commission's concern that the definition of an "identity theft report" be sufficient to deter those seeking to abuse the system while preserving the benefits of the FCRA for true victims of identity theft. Although we believe the Commission's provisions with respect to alleging an identity theft with specificity, and allowing furnishers/consumer reporting agencies to request additional information, are generally useful, we do not believe that they will significantly deter wrongdoing. We believe, however, that the FCRA provides the Commission with the necessary tools to preserve the integrity of identity theft reports, and therefore avoid the unnecessary degradation of the consumer reporting process as a whole.

Under the FCRA, an "identity theft report" must be "an official, valid report filed with an appropriate Federal, State, or local law enforcement agency...or such other government agency deemed appropriate by the Commission." The Proposal interprets this provision to mean "an official, valid report filed by the consumer with a Federal, State, or local law enforcement agency." MasterCard is concerned that the removal of the notion that the report must be filed with an "appropriate" law enforcement agency creates significant latitude for those seeking to abuse the system and remove accurate, but negative, information from their consumer reports.

A critical component of the statutory definition of "identity theft report" is that it must be filed with an "appropriate" law enforcement agency. For example, filing the report with a law enforcement agency with the jurisdiction to investigate the alleged crime and refer it for prosecution would likely meet the requirement of filing the report with an "appropriate" law enforcement agency. In this regard, a consumer is less likely to file an untruthful report with a law enforcement agency that would have the inclination to follow up on the report's allegations and take action against someone who falsified allegations. As such, *it is clearly not appropriate to deem an "identity theft report" to be a document filed with any law enforcement agency in the country regardless of whether it has the power or jurisdiction to investigate the crime.* Such an agency is likely to ignore the report, resulting in little or no deterrence to those seeking to file fictitious identity theft reports in order to abuse the system. The Commission illustrates this notion in a footnote to its Supplementary Information:

> Indeed, the Commission's own identity theft complaint collection system...illustrates the possibility for abuse....[T]he Commission [has] established its Identity Theft Data Clearinghouse, a centralized database that accepts identity theft complaints from consumers. The Commission's complaint system, however, 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....Now under the [FACT] Act, 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.[4]

We therefore urge the Commission to adhere to the statutory language that an "identity theft report" is, *at a minimum*, a report filed with an "appropriate" law enforcement agency and include such language in the Final Rule. Furthermore, we urge the Commission to indicate that an appropriate law enforcement agency is an agency that has the jurisdiction to investigate the crimes alleged in the report. Given that there will be a variety of appropriate federal, state, and local law enforcement agencies from which to choose, we do not believe that such a requirement will affect a victim's recovery process, and MasterCard believes that these amendments will help reduce the incidence of fraud associated with identity theft reports.

Duration of Active Duty Alerts

Under the FCRA, military personnel who meet the definition of an "active duty military consumer" may place an active duty alert in their credit files. The active duty alert is intended to provide active duty military consumers with additional safeguards against identity theft while deployed. The statute sets a minimum duration of 12 months for active duty alerts, but allows the Commission to determine if the period should be longer. In the Proposal, the Commission retains the 12-month duration for active duty alerts. MasterCard believes that 12 months is an appropriate period of time for active duty alerts. In this regard, we do not believe that a majority of active duty military consumers will need active duty alerts for more than 12 months. For those who do need them for a longer period of time, they can still receive the appropriate protections by requesting a subsequent active duty alert. Therefore, we urge the Commission to retain the 12-month period to provide protection to the majority of active duty military consumers while allowing others to request additional protection as necessary.

* * * * *

[4] In light of the Commission's discussion of how a complaint filed with the Commission would not be appropriate because of the "possibility for abuse," MasterCard is particularly alarmed that the Commission would apparently deem an automated form, such as its ID Theft Affidavit, as sufficient for purposes of an "identity theft report" if the form were notarized. (*See* proposed Part 603.3(c)(3)). We do not believe that the potential for abuse described by the Commission in connection with filing an automated form (such as the Commission's ID Theft Affidavit) is mitigated by the fact that the person is willing to sign the document in front of a notary public. In fact, a notary public can only attest that the person signing the document is who he or she claims to be. The notary cannot attest to the validity or accuracy of the document, nor does the individual necessarily attest to the notary that the statements in the document are true.

Once again, we appreciate the opportunity to comment on the Proposal. If you have any questions concerning our comments, or if we may otherwise be of assistance in connection with this issue, please do not hesitate to call me, at the number indicated above, or Michael F. McEneney at Sidley Austin Brown & Wood LLP, at (202) 736-8368, our counsel in connection with this matter.

Sincerely,

Jodi Golinsky

Jodi Golinsky
Vice President and
Senior Regulatory Counsel

cc: Michael F. McEneney, Esq.