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

September 18, 2006

Via Electronic Delivery

Office of the Comptroller of the Currency
250 E Street, SW, Mail Stop 1-5
Washington, DC 20219
Attention: Docket Number 06-07

regs.comments@occ.treas.gov

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
Attention: Docket No. R-1255

regs.comments@federalreserve.gov

Mr. Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
RIN 3064-AC00

comments@fdic.gov

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 2006-19

regs.comments@ots.treas.gov

Ms. Mary Rupp
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428
Re: Comments on Proposal 717,
Identity Theft Red Flags

regcomments@ncua.gov

Federal Trade Commission
Office of the Secretary
Room 159-H (Annex C)
600 Pennsylvania Avenue, NW
Washington, DC 20580
Project No. R611019, Red Flags Rule

https://secure.commentworks.com/ftc-redflags

Re: MasterCard Comments on Joint Notice of Proposed Rulemaking: Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003

To Whom It May Concern:

This letter is submitted on behalf of MasterCard International Incorporated ("MasterCard")[1] in response to the Joint Notice of Proposed Rulemaking ("Proposal") issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation ("FDIC"), the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission ("FTC") (collectively, "Agencies") in the *Federal Register* on July 18, 2006. MasterCard appreciates the opportunity to provide comments on the Proposal.

In General

The Proposal aims to use a "flexible risk-based approach" to implement the "red flags" requirements included in the Fair Credit Reporting Act ("FCRA"). We strongly believe that such an approach is critical if the Proposal is to provide meaningful guidance to financial institutions. MasterCard is concerned, however, that the Proposal, on the whole, does not provide sufficient flexibility. The Proposal essentially requires financial

[1] MasterCard International (NYSE:MA) advances global commerce by providing a critical link among financial institutions and millions of businesses, cardholders and merchants worldwide. Through the company's roles as a franchisor, processor and advisor, MasterCard develops and markets secure, convenient and rewarding payment solutions, seamlessly processes more than 16 billion payments each year, and provides industry-leading analysis and consulting services that drive business growth for its banking customers and merchants. With more than one billion cards issued through its family of brands, including MasterCard®, Maestro® and Cirrus®, MasterCard serves consumers and businesses in more than 210 countries and territories, and is a partner to 25,000 of the world's leading financial institutions. With more than 24 million acceptance locations worldwide, no payment card is more widely accepted than MasterCard. For more information go to www.mastercardinternational.com.

institutions and creditors ("institutions") to identify, detect, and address *any* risk of identity theft as part of their Identity Theft Prevention Program ("Program") without regard to the significance of the risk. As a result, the Proposal may require institutions to devote time and energy to addressing issues of relatively low risk. This will complicate financial institutions' efforts to detect and prevent identity theft without necessarily providing a corresponding benefit. In fact, we believe that the extra resources that will be required by financial institutions to implement their Programs may reduce the available resources that could be used more productively to combat fraud and identity theft.

As a general matter, we believe this issue can be address by more closely following the approach used in the Interagency Guidelines Establishing Information Security Standards ("Information Safeguards") which instruct financial institutions to implement a comprehensive information safeguarding program taking various considerations into account. The Information Safeguards establish specific objectives for financial institutions to meet, require them to engage in a risk assessment, and require a program to manage and control the identified risks as appropriate. The approach used by the Agencies with respect to the Information Safeguards has been well received, and we believe it should provide the framework for the final rule issued by the Agencies ("Final Rule").

Our more specific comments on the red flags requirements, in addition to those on other portions of the Proposal, are below.

Red Flags

Section 615(e) of the FCRA requires the Agencies to establish and maintain guidelines for use by each "financial institution and each creditor regarding identity theft with respect to account holders at, or customers of, such entities" and prescribe regulations requiring each financial institution and creditor to establish reasonable policies and procedures for implementing the guidelines to identify possible risks to account holders or customers or to the safety and soundness of the institution or creditor.[2]

Definitions: "Account"

The Agencies use the term "account" in the Proposal to "broadly describe the various relationships an account holder or customer may have with a financial institution or creditor that may become subject to identity theft." The Agencies state that the definition of "account" for purposes of the Proposal is similar to the definition of "customer relationship" in the Agencies privacy regulations. We believe this is appropriate and urge the Agencies to retain the scope of the definition. We do not understand isolated incidents (*e.g.*, use of a foreign ATM or purchase of travelers checks) to be a significant source of identity theft. To broaden the definition to include such transactions would result in financial institutions and creditors devoting resources to identity theft detection and prevention where they are not necessary. This will likely result in fewer resources being dedicated to more productive uses involving continuing relationships with consumers.

[2] As the Agencies note, the statute refers to the "safety and soundness of the institution or customers." We concur with the Agencies that the statute should probably refer to the creditor instead of customers.

As stated above, we believe that it is useful to have a term for relationships to be protected under the Proposal. However, we are concerned that the Agencies have chosen the term "account" to define those relationships. The term "account" is used in Section 615(e) of the FCRA. The FCRA provides a definition for that term (including as to how it is used in Section 615(e)) that is much more narrow than the definition provided by the Agencies in the Proposal.[3] Specifically, Section 603(r) of the FCRA states that "account" "ha[s] the same meaning[] as in section 903 of the Electronic Fund Transfer Act," *i.e.*, a demand deposit, savings, or other consumer asset account. We believe that the Agencies would create confusion if, in a regulation implementing a portion of the FCRA, they created and defined a term that is already used but defined differently in the FCRA. Instead of using the term "account," the Agencies could use the term "continuing relationship" or something similar without affecting the substance of the Proposal.

If the Agencies' retain the use of the term "account", however, we request that the Agencies reiterate in the Final Rule their understanding that the term "account" as used in the Final Rule deviates from the definition of "account" in the FCRA and that the use of such term in the Final Rule is not intended to define the term as it is used in the FCRA (including Section 615(e)). The FCRA provides a definition for the term "account" which is not limited to any section, purpose, or context. It is the definition for the term "account," regardless of where or how it appears in the FCRA, such as in Section 615(e). We ask only that if the Agencies choose a term that has a different statutory definition than that provided in the Final Rule that the Agencies make it clear that no inference should be made between the use of the term in the Final Rule and the term as it appears in the statute.

In addition, we urge the Agencies to revise their assertion in the Supplementary Information that Section 615(e) of the FCRA does not use the term "account." In fact, the term is used in Section 615(e), such as to define one class of individuals to benefit from the Final Rule, *i.e.* individuals who hold an "account." However, the term is not particularly limiting in a defining the scope of Section 615(e) because "customers" are also to be protected under Section 615(e) and there is no statutory definition of "customer." Understandably, the Agencies have determined that "account holders at, or customers of" a financial institution or creditor should coincide generally with individuals who have a customer relationship with such institutions under the Agencies' privacy regulations. The statement in the Supplementary Information, however, that the term does not appear in Section 615(e) is incorrect and implies a limited application of the definition of "account" provided in Section 603.

Definitions: "Identity Theft"

Under the Proposal, the definition of "identity theft" is critical in establishing the scope of the Proposal due to the use of the term as part of the definition of a "red flag" (discussed below). The Agencies propose to adopt the definition of the term "identity theft" as implemented by the FTC. Therefore, the definition would be "a fraud committed

[3] The Agencies state in the Supplementary Information that they recognize the FCRA has a different definition for "account" but that such definition is used "in other contexts." We believe that the definition provided in the FCRA is applicable to the term everywhere it appears in the FCRA, as the statutory language does not limit its applicability to certain portions or contexts.

or attempted using the identifying information of another person without authority." We urge the Agencies to eliminate the reference to "attempted" fraud as part of the definition of "identity theft" for purposes of the Proposal.

As discussed in more detail below, the Proposal would require financial institutions and creditors to develop a program to "prevent and mitigate" identity theft in connection with account opening or any existing account. As drafted, the Proposal would require these programs to "prevent" attempted fraud in these contexts. It is not clear how a financial institution or creditor could develop such a program. It should suffice if the institution has a Program designed to *prevent the fraud itself.*

Definitions: "Red Flag"

The Proposal defines a "red flag" to be "a pattern, practice, or specific activity that indicates *the possible risk* of identity theft" ("Red Flag"). (Emphasis added.) In the Supplementary Information the Agencies attempt to clarify the intended breadth of the definition by indicating that a "possible risk" of identity theft may exist even where the "possible existence" of identity theft is not necessarily indicated. This definition appears to be too broad because there are few transactions for which there is absolutely no possible risk of fraud. As discussed below, we believe this issue can be addressed by utilizing an approach that is truly risk based rather than one that focuses on any possible risk of identity theft.

The issue of breadth is compounded through the Agencies' intent to include "precursors" to identity theft as part of the definition of "red flag." According to the Agencies, examples of a "precursor" to identity theft are phishing scams or a data breaches. The term "precursor," however, is not defined. Regardless of the definition, it is not clear how a financial institution's program would address precursors any differently than it would address the risk of identity theft that would result from such precursors, *i.e.*, the attempted misuse of the consumer's information. If this is true, any reference to precursors would be redundant. Yet, because "precursors" are specifically described in the definition of "Red Flags," it appears that the Agencies intend to emphasize this issue in a manner that would not otherwise be addressed in connection with an institution's efforts to thwart identity theft.

The Program: A Suggested Approach

We applaud the Agencies stated desire to emulate the approach provided in the Information Safeguards and to allow an institution the flexibility to develop risk-based programs based on an institution's size and complexity to prevent identity theft. We concur and believe the Agencies should modify the Proposal so that it more clearly follows the approach taken in the Information Safeguards. In so doing the Agencies will have provided broad but clear and specific goals to be achieved while allowing each institution the flexibility to develop a risk-based program to protect customers and institutions themselves from identity theft. In particular, we suggest that the Final Rule approach this issue as follows:

1. Establish a Concrete Objective for Financial Institutions and Creditors. The Program should describe an institution's policies and procedures to prevent and mitigate the misuse of an individual's identity to commit identity theft.

2. Specify Expectations for the Development of the Program. The Program should involve appropriate senior management and should be based on a risk assessment.

3. Specify Expectations for the Management and Control of Risks. The Program should be designed to control the identified risks as appropriate based on the risk assessment. Programs should not be required to address a particular "possible risk" unless addressing such risk is appropriate in light of the risk assessment. The Proposal should describe various issues that should be *considered* when developing a risk-based Program. For example, such issues could include the collection of certain information at account opening, assessing such information, transaction monitoring, managing third party operations (*e.g.*, in loan origination by a broker), mechanisms through which accounts can be accessed, response programs, etc.

4. Adjustment of the Program as Necessary. The risk assessment should be ongoing, resulting in adjustments to the Program as necessary, with reporting to senior management as appropriate.

The approach outlined above is very similar to the approach used in the Information Safeguards. Although the Information Safeguards provide some specific things to consider as part of an institution's ability to manage and control identified risk, the Information Safeguards essentially allow the institution to make its own assessments and judgments with respect to information security. The Information Safeguards do not attempt to micromanage institutions, nor do they establish procedures that must be implemented to meet the objectives. We believe the Information Safeguards have been successful, and we do not see a need to deviate from the general approach used by the Agencies in drafting the Information Safeguards.

We believe the Proposal does depart from the approach taken in the Information Safeguards in material ways. For example, instead of asking institutions to use a risk-based approach to assessing identity theft threats, the Agencies appear to expect institutions to document each and every "possible risk," regardless of whether it is reasonably foreseeable, significant, likely, or material.[4] Without clear language in the regulation itself, the implication may be that the institution must identify each of those patterns, practices, or specific activities if it is going to have policies and procedures to detect them. This requirement for such a cumbersome document is dissimilar from the Information Safeguards because it does not allow for the institution to inject any risk

[4] Such documentation would be necessary for purposes of examinations for compliance, for example.

assessment in the Program's development. Rather, the written Program must apparently have policies and procedures to identify all risks, no matter how insignificant.[5]

We note that the Agencies may believe that the Proposal offers institutions some flexibility to narrow their Programs on based on a risk assessment. For example, the Supplementary Information indicates that an institution may exclude various types of transactions unless such transactions are "likely to be subject to identity theft and should, therefore, be included in the scope of its Program." Yet the plain language of the Proposal requires identification and institution responses to any possible risks of potential fraud without regard to this risk assessment. In other words, the risk assessment in the Proposal does not provide a basis for the development of a risk-based Program.

In addition to requiring an institution to have policies and procedures to identify the universe of circumstances that could involve a risk of identity theft, the Agencies have published an appendix of 31 Red Flags ("Appendix"). We understand that the statute requires the Agencies, as part of the guidelines, to identify "patterns, practices, and specific forms of activity that indicate the possible existence of identity theft." We ask that the Agencies make clear that any Appendix be solely for illustrative purposes only. An institution should be permitted to assess its own risks without the suggestion that it *must* or even should consider specific patterns or activities identified by the Agencies as part of its Program. While the Agencies may be able to provide some guidance through the Appendix to less sophisticated institutions, it is not possible or expected for the Appendix to substitute for the expertise or sophistication of larger institutions' fraud management departments. Furthermore, we believe that absent some clear indication that an institution is not obligated to consider the Appendix, a practical result may be that the items included in the Appendix become *de facto* requirements as a result of the examination process. The end result would be an institution being required to dedicate resources to address a pattern or practice even when doing so is not the most effective or efficient allocation of resources.

With respect to the risk assessment itself in Section __.90(d)(1)(ii), the Proposal lists four items that must be considered. It is our understanding that items in the Proposal are not necessarily those that are relevant to an institution in connection with its anti-fraud efforts. It may be more appropriate for the Agencies to provide general items for consideration when an institution is deciding how to manage and control its risk. For example, the Final Rule could require institutions to consider how much information to collect at account opening, appropriate mechanisms for account monitoring, risks associated with identity verification, and the like. Such items would be more relevant and consistent with the types of issues addressed in the Information Safeguards. They would also foster a more robust and complete Program to protect customers.

Section __.90(d)(2) provides some of the more significant requirements with respect to the implementation of the Program itself. Specifically, an institution must include reasonable policies and procedures designed to prevent and mitigate identity theft,

---

[5] A requirement to adopt a risk-based Program would satisfy the statutory requirement in Section 615(e)(1)(B) that the Program "identify possible risks" of identity theft. The statute does not require the identification of "all" possible risks, nor did Congress signal such an intent.

including policies and procedures to: (i) verify a person's identity at account opening; (ii) detect the Red Flags identified in the written Program; (iii) assess whether the Red Flags evidence a risk of identity theft; and (iv) address the risk of identity theft commensurate with the risk. We ask the Agencies to revise this portion of the Proposal so that an institution may focus more on achieving the objective—preventing and mitigating identity theft—than on a particular process. The Agencies should identify a clear objective and allow institutions the flexibility to determine how best to achieve that objective on a case-by-case basis. The Agencies should allow institutions to develop their own account opening and transactional processes, however, to meet those objectives. For example, we commend the Agencies for indicating that an institution could use its Customer Identification Program ("CIP") in connection with account openings as opposed to prescribing new procedural requirements.

If the Agencies retain specific process requirements with respect to how an institution implements its Program, we urge the Agencies to clarify their intent. For example, we believe that the process should lead to the an institution forming a reasonable belief that it knows the identity of the consumer or the validity of the transaction, whether at account opening or later in the ongoing relationship. The Proposal suggests that an institution, even if it concludes as part of its CIP that it is dealing with the true consumer, must still identify various Red Flags and "address" them. For example, a Red Flag may arise because the institution cannot verify the date of birth provided.[6] Under the regulations implementing Section 326 of the USA PATRIOT Act ("CIP Rules"), an institution need not verify each piece of information collected, so long as it can form a reasonable belief that it knows the identity of the individual. Under the Proposal, however, it would appear that the institution would need to do something affirmatively to "address the risk" posed by the alleged Red Flag. If the process requirements in the Proposal remain in the Final Rule, it would be more appropriate to require institutions to use the Red Flags as a means to identifying the validity of the underlying transaction, and taking whatever steps are necessary to mitigate any meaningful risks if the validity is in question.[7]

MasterCard also offers a comment with respect to the Supplementary Information pertaining to Section __.90(d)(2). The Agencies state that "if the financial institution or creditor is notified that a customer provided his or her password and account number to a fraudulent website, it likely will close the customer's existing account and reopen it with a new account number." It is not clear whether this is likely what an institution would or should do today, and it is certainly not clear whether this is what an institution should do in the future as anti-fraud systems evolve. This is an instance where an institution's risk-based program should be permitted to operate, now and in the future, without "hardwiring" the required response through Agency "guidance" in the Supplementary Information.

---

[6] Inability to verify date of birth may evidence a risk, no matter how insignificant, of attempted fraud, and therefore could be a Red Flag, as the term is defined.

[7] The Red Flags in question would need to be determined using a risk assessment. An institution would not identify every Red Flag, but rather those of such a risk as to warrant additional action.

The Program: Staff Training

The Agencies correctly expect an institution to train its staff to implement the Program. It is likely, however, that the Agencies intend an institution to train only the appropriate staff with respect to relevant portions of the Program. For example, one of the institution's customer service representatives will probably need different training than one of the institution's accountants or custodial staff in order to effectuate the Program. Therefore, we ask the Agencies to clarify that the expectation is not that the institution will provide the same level of training to each of its employees. Rather, the institution should provide a level of training to each employee that is consistent with what is necessary to carry out the Program.

The Program: Oversight of Services Providers

MasterCard believes the Agencies have approached the topic of service providers and their role with respect to an institution's program correctly. We urge the Agencies to retain these provisions in the Final Rule. In particular, the Agencies note the role that service providers can play in assisting an institution implement its Program. Service providers can offer valuable skills and expertise to institutions in their efforts to prevent and mitigate identity theft. On the other hand, the Agencies also correctly note that an institution is ultimately responsible for its compliance with its Program.

The Agencies would "allow[] a service provider that provides services to multiple financial institutions and creditors to conduct activities on behalf of these entities in accordance with its own program to prevent identity theft, as long as the program meets the requirements of the [Final Rule]. The service provider would not need to apply the particular Program of each individual financial institution or creditor to whom it is providing services." We applaud the general intent of the Agencies to provide flexibility to service providers. It would be impossible for a service provider that provides services to hundreds or even thousands of institutions to tailor its services to each nuance of each institutions' Program.

We ask the Agencies to clarify, however, that a service provider need not have its own "program" that meets each of the requirements of the Final Rule. The apparent objective of the Agencies is that a service provider perform services in a manner consistent with the requirements of the Final Rule. Such an approach would be similar to the approach taken in the Information Safeguards. A bank need not require its service provider to adopt specific information security protections under the Information Safeguards. A bank need only require, however, that the service provider implement and maintain an information security program that meets the objectives of the Information Safeguards. We believe that this approach has worked well in the context of the Information Safeguards, and we urge the Agencies to replicate it in the Final Rule. Therefore, it would not seem necessary to require a service provider to have a full-fledged "program" so long as the service provider's services meet the objectives of the Final Rule.

The Program: Board of Directors

The Proposal would require that the board of directors (or an appropriate committee of the board) ("Board") approve the written Program. We concur with the Agencies that the Program is of such importance as to warrant senior management's involvement. It may not necessarily be appropriate, however, that the Board approve the minutiae of the Program. For example, given the changing risks of identity fraud, it is conceivable that a Program could need revisions fairly frequently and urgently. Yet changes to the Program may not be as frequent or as urgent as they should be if the Board must approve each and every one of them. We believe, therefore, that senior management should be permitted to approve and revise the Program.

Fraud Alerts and the Equal Credit Opportunity Act

The Agencies have taken the opportunity to opine on an interpretation of the Equal Credit Opportunity Act ("ECOA") as part of the Proposal. The interpretation in the Proposal is consistent with an interpretive letter issued previously by the FDIC. The Agencies state in a footnote to the Supplementary Information that "when a credit file contains a fraud or active duty alert, a creditor *must* take reasonable steps to verify the identity of the individual in accordance with [the FCRA] before extending credit, closing an account, or otherwise limiting the availability of credit." (Emphasis added.) To do otherwise, according to the Agencies, would violate the ECOA because it would be discrimination against the consumer for exercising a right under the Consumer Credit Protection Act, of with the FCRA is part.

This interpretation does not appear to be consistent with the statute. Section 605A(h) describes both the consumer's request embodied in a fraud alert as well as the obligations of a user of a consumer report ("User") when the User receives a fraud alert in a consumer report. For example, Section 605A(h)(1)(A) and (B) state that an initial or active duty alert is a notification to a User "that the consumer does not authorize" certain credit transactions in the consumer's name, and that a User is prohibited from permitting certain transactions "*unless* the user utilizes reasonable policies and procedures to" identify the person requesting the transaction.[8] (Emphasis added.) It would appear by the plain language of the statute that if an institution is not going to utilize certain policies and procedures the institution's denial of the transaction is: (i) *precisely what the consumer requested;* and (ii) *required under the statute.* Furthermore, the statute is not ambiguous on this point—it clearly envisions circumstances in which the User does *not* utilize such policies and procedures. In such circumstances, the User is not permitted to engage in certain transactions. In fact, *denial of the transaction is the default in the statute.* Only if the User takes additional steps can the transaction be approved. Respecting the wishes of the consumer and complying with the law simply cannot be considered discriminating against the consumer.

It would also be unusual for Congress to draft Section 605A(h) as they had if they truly intended to require affirmative action by a User in response to a fraud alert. We

[8] A similar provision is present in Section 605A(h)(2)(A) and (B) relating to extended fraud alerts.

believe it is more likely that Congress would have stated that a User "must" use reasonable policies and procedures to verify the consumer's identity if it receives a fraud alert instead of using language that defaults to a denial of credit. We are also unsure as to whether identity theft will increase or decrease if otherwise cautious creditors are forced to proceed with an application from a consumer that has placed a fraud alert in his or her file. All else equal, it is certainly the case that more fraudulent applications will be approved if creditors who would have otherwise denied an application must continue the application process despite the presence of a fraud alert. Some creditors may also simply stop offering certain products through certain channels if a fraud alert requires additional diligence that is not practical or cost effective for the User to conduct, such as certain instant credit products. This will restrict the availability of such credit products to all consumers, not just those with a fraud alert on their file. On the other hand, consumers may be more likely to use fraud alerts if they know that it will not result in automatic denial of applications in certain circumstances. This may be a positive effect, although we are unaware of any evidence that consumers avoid using fraud alerts for these reasons.[9] Regardless, given that the statute can reasonably (and more correctly) be interpreted not to require additional due diligence, the Agencies must believe that the consumer benefits associated with their ECOA interpretation outweigh the harms.

Inactive Accounts

Section 615(e)(2)(B) of the FCRA requires the Agencies to consider including provisions as part of the Proposal pertaining to transactions occurring with respect to certain accounts that have been inactive for two or more years and requiring Institutions to provide for consumer notices in such circumstances. The Agencies state that a two-year limit may not be an accurate indicator of identity theft given the variety of accounts that would be covered. In the alternative, the Agencies have included a provision in the Appendix pertaining to use of inactive accounts as a possible Red Flag.

We commend the Agencies for not including specific notice requirements with respect to the use of credit or deposit accounts that have been inactive for two years. Not only is the two-year timeframe not particularly accurate, but in many instances the consumer will receive a notice of the transaction in the form of a periodic statement under current law, such as the Truth in Lending Act or the Electronic Fund Transfer Act. We also believe that such a requirement would be counter to the overall goal and theme outlined by the Agencies to allow institutions to develop risk-based Programs based on a variety of factors specific to each institution. Any provision similar to Section 615(e)(2)(B) of the FCRA, therefore, should not be "hardwired" in any Final Rule or Appendix.

Duties of Card Issuers

Section 615(e)(1)(C) of the FCRA requires the Agencies to prescribe regulations applicable to "card issuers" to ensure that if a card issuer receives notification of a change

[9] It is our belief that the vast majority of creditors do not deny an application based solely on their inability or unwillingness to engage in additional due diligence.

of address for an existing account and "within a short period of time (during at least the first 30 days after such notification is received)" receives a request for an additional or replacement card for the same account, that the card issuer not issue the additional card unless the card issuer takes certain steps to assess the validity of the request. In particular, the statute states that in such a circumstance the card issuer should: (i) notify the cardholder of the request at the old and the new address and provide the cardholder a means of reporting incorrect address changes; (ii) notify the cardholder of the request by "such other means of communication as the cardholder and the card issuer previously agreed to"; or (iii) use other means of assessing the validity of the change of address in accordance with the card issuers Program.

The Proposal generally tracks the statutory language, and we urge the Agencies to retain the same general approach in the Final Rule. In particular, it is important that card issuers have the opportunity to use their own reasonable means of assessing the validity of the change of address as part of their Programs. For example, it may be that the validity of the address change is assessed at the time the address change is made, regardless of any possibility of a request for an additional card in the future. Therefore, a card issuer would not necessarily need to engage in additional verification when the additional card is requested unless its Program suggested that additional verification steps were required.

Although the Proposal tracks the statute closely, the Agencies provide definitions for certain terms undefined in the statute. For example, the Proposal defines a "cardholder" to be a "consumer who has been issued a credit or debit card." The Agencies note that the definition of "consumer" in the FCRA is an "individual," and therefore that this portion of the Proposal would cover individuals who have been issued credit or debit cards, including commercial credit and debit cards. We urge the Agencies to reconsider the scope of this portion of the Proposal. It is our experience that commercial credit and/or debit cards are much less likely to be the target of fraud schemes of the type addressed in __.91. To require issuers of commercial cards to comply with __.91 when it may not be the most efficient allocation of fraud prevention resources would appear to be counterproductive. In this regard, the Proposal would force card issuers to dedicate limited resources to compliance with __.91 when such resources may be better allocated toward consumer cards in an effort to achieve the same goal.

Additionally, we note that the Proposal states that any written or electronic notice that a card issuer provides in connection with the general requirement must be "clear and conspicuous and provided separately from its regular correspondence with the cardholder." This scope of applicability of this provision is unclear. As drafted, it applies to *any* written or electronic notice provided in connection with __.91. We believe that this provision should apply only to notices provided pursuant to __.91(c)(1) when no other mechanism is used to verify the validity of the address change. Otherwise, it would prohibit other types of supplementary written or electronic notices, such as those that could be included on periodic statements. We doubt this was the Agencies' intention. Furthermore, Section 615(e)(1)(C)(iii) of the FCRA appears to give card issuers more flexibility than the limitation in __.91(d) would suggest.

Duties of Users of Consumer Reports Regarding Address Discrepancies

Section 605(h) of the FCRA requires the Agencies to prescribe regulations "providing guidance regarding reasonable policies and procedures that a user of a consumer report should employ when such user has received a notice of [address] discrepancy" from a nationwide consumer reporting agency. The regulations must describe reasonable policies and procedures for use by a User: (i) to form a reasonable belief that the User knows the identity of the person to whom the consumer report pertains; and (ii) if the User establishes a continuing relationship with the consumer, and the User regularly furnishes information to the consumer reporting agency that provided the discrepancy notice, to reconcile the address of the consumer with the consumer reporting agency by furnishing such address to such consumer reporting agency in the next regular furnishing period.

Reliance on CIP

The statutory language in Section 605(h)(2)(i) of the FCRA requires a User "to form a reasonable belief that the user knows the identity to whom the consumer report pertains." This language is similar to that found in the CIP Rules.[10] The Proposal implements the first requirement in a straightforward manner. In particular, a User that receives a notice of discrepancy must develop and implement reasonable policies and procedures for verifying the identity of the consumer for whom it has received a notice of discrepancy. Given the similarity between Section 605(h) of the FCRA and the CIP Rules, we applaud the Agencies for the inclusion in the Proposal of the explicit statement that a User "that employs the policies and procedures regarding identification and verification set forth in the CIP Rules under these circumstances satisfies this requirement, whether or not the user is subject to" those regulations. We urge the Agencies to retain this provision in the Final Rule.

Although the Proposal allows for a User to rely on its CIP, or a program that would comply with the CIP Rules if the User is not subject to them, the Supplementary Information indicates that this benefit is available only "so long as [the User] applies [its CIP policies] is *all* situations where it receives a notice of discrepancy." (Emphasis added.) It is not clear why a User can rely on its CIP to comply with the Proposal, but only if it uses such policies in all circumstances. It might be possible that a User could form a reasonable belief that it knows the identity of the consumer without employing its CIP—either because use of the CIP was not necessary under the circumstances or because it needed to use different policies to form such a belief.

We also note that reliance on CIP would not require an institution to verify the identity of an applicant for credit who is denied, for example. We ask the Agencies to clarify that it is not their intent to require institutions to verify the identity of individuals with whom they will not establish continuing relationships. This would not appear to provide significant benefits, and could prove to be quite awkward. For example, an

[10] Compare to 31 C.F.R. 103.121(b)(2) ("The procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer.).

applicant is not likely to provide additional information or otherwise cooperate in any further investigation of his or her identity once the person learns that they will not be approved for credit.

Reconciling the Address

The second obligation for Users under Section 605(h) is to "reconcile" the address discrepancy with the consumer reporting agency if the User "establishes" a continuing relationship. The statute prescribes how the User is to reconcile the address—Congress did not intend for Users to speculate as to what it meant to "reconcile" the address. Rather, the statute states that the User must reconcile the address "by furnishing such address to such consumer reporting agency as part of information regularly furnished by the user for the period in which the relationship is established." In this regard, the statute is instructive as to what Congress intended for Users to do in order to "reconcile" the consumer's address.

The requirements of Section 605(h)(2)(B)(ii) apply only if the User "establishes a continuing relationship with the consumer." Therefore, it would appear that Congress intended Section 605(h)(2)(B)(ii) to apply only if the User sets up, founds, generates, or otherwise initiates a continuing relationship. The reconciliation requirement would not apply if the relationship is not set up, founded, generated, or initiated. This can occur in at least two circumstances. First, the User may not have any relationship with the consumer because an application is declined, for example. Second, the User may have an existing relationship with the consumer, in which case the relationship is not "established" in connection with the obtaining of the consumer report or notice of discrepancy in question.

The Proposal, however, would appear to apply the requirements of Section 605(h)(2)(B)(ii) to circumstances in which a continuing relationship is not established as a result of the transaction involving the consumer report. One such circumstance could involve the use of consumer reports in connection with account reviews. Specifically, the Proposal indicates that the requirement to "reconcile" the address applies not only when the User establishes a relationship, but also if the User "maintains" a relationship. This exceeds the statutory requirement and congressional intent. It also imposes significant burdens on Users because of the Agencies' proposed requirement to verify addresses. Under the Proposal, Users who obtain large numbers of consumer reports as part of account review efforts would be required to verify millions of addresses a year. As we discuss below, this is not a simple or necessary task. For these reasons, we ask that the Agencies revise the Proposal to reflect more accurately the statutory language.

The Proposal includes an additional requirement, however, with respect to the obligation to reconcile the address. Specifically, the Proposal would require a User to furnish an address "that the user has reasonably confirmed is accurate" to the consumer reporting agency. We urge the Agencies to eliminate the requirement to confirm the consumer's address.

As noted above, Congress stated the scope of the obligation to "reconcile" the address, and there is no reference in the statute to confirming the consumer's address. Had

Congress intended such a requirement, we believe Congress would have specifically stated it, especially given the fact that Congress broached the subject of forming a reasonable belief about the consumer's identity. Had they intended Users to form a reasonable belief about the address itself, we believe Congress would have so stated and not have expected such an intent to be inferred from a more general requirement to update the consumer reporting agencies' files.

We respectfully suggest that the proposed requirement to verify the address goes beyond, and is redundant to, the obligation of the User to "form a reasonable belief that it knows the identity of the consumer." By using this language in the FCRA which was drawn from the CIP Rules, it would be reasonable to assume that Congress intended for the Agencies to implement Section 605(h) in a manner similar to the CIP Rules. As implemented and specifically clarified by the relevant Agencies, and as was understood by Congress, the existing CIP Rules do *not* require a financial institution to confirm any piece of a consumer's identifying information, *including the consumer's address*. We do not believe that Section 605(h)(2)(ii) should be read to impose additional requirements than those deemed appropriate for national security purposes under the PATRIOT Act. Furthermore, if the User has formed a reasonable belief that it knows the identity of the individual, it would seem reasonable to conclude that the consumer provided a valid address.[11] Not only does there appear to be limited anti-fraud benefit to the additional requirement to verify the address once the identity itself has been verified, but the requirement would be difficult and costly to implement. For example, the Proposal suggests using a third-party source to verify the address. It is a trusted third party, however, which provided the address discrepancy. Must a User consult a variety of third parties until the address can be confirmed? What if the address is new and not yet in a third party database? The Proposal also suggests that the financial institution could review its own records to verify the address. This is true, but would be successful for only a small percentage of the cases involving an address discrepancy.[12] The Proposal also suggests verifying the address with the consumer. If the consumer is legitimate, this would be redundant in most circumstances or serve only to correct a misspelled street name or other clerical error.[13] If the person in question is an impostor, the person would only "verify" the fraudulent address.

It is also important to consider that neither the statute nor the Proposal addresses what a User should do if it forms a reasonable belief that it knows the identity of the consumer, but that it cannot "reasonably confirm" the accuracy of the address before the time in which the address must be furnished to the consumer reporting agency. We do not

---

[11] For example, the consumer may have provided a secondary address not previously furnished to a consumer reporting agency. This is perfectly valid, although the Supplementary Information suggests that for a consumer to do so would be the consumer providing an "incorrect" address.

[12] If the Agencies retain the requirement for Users to reconcile addresses on existing accounts in addition to verifying the address, we urge the Agencies to indicate that an acceptable means of verification is to rely on reasonable policies and procedures to assess the validity of the address change at the time the change is made, as opposed to at the time the notice of discrepancy is received.

[13] The congressional intent behind Section 605(h) was clearly to reduce identity theft and related fraud. It is unlikely Congress enacted Section 605(h) as a requirement for Users to have more accurate internal records pertaining to legitimate consumers.

believe Congress felt it was necessary to address such a circumstance, as it likely did not envision the additional requirement included in the Proposal. For these reasons, we urge the Agencies to eliminate any requirement to verify a consumer's address in response to an address discrepancy under Section 605(h) of the FCRA.

Obligations for Existing Accounts

The Proposal would require a User to satisfy the obligations described in Section 605(h) in response to an address discrepancy received by a User in connection with an existing account, such as part of an account review. Although we strongly believe that the Final Rule should not include such a requirement, we ask that if this requirement is retained the Agencies indicate that if the User has procedures in place to form a reasonable belief of the consumer's identity before allowing the consumer to modify his or her address on an account, that the User need not employ additional procedures in response to an address discrepancy notice. A requirement to employ such procedures twice in connection with the same event (*i.e.*, the change of address) would appear to be unnecessary and redundant.

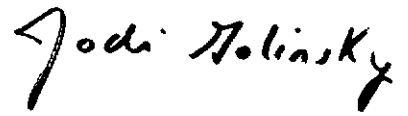
Effective Date

MasterCard requests that the Agencies provide institutions with sufficient opportunity to review and implement the Final Rule. We believe it would be appropriate to establish an immediate effective date for the Final Rule with compliance required 18 months after it is published in the *Federal Register*. This will give institutions the ability to conduct an inventory of existing operations while developing new programs that may be necessary for compliance. In light of the fact that any revisions to existing policies and procedures by institutions will likely require significant integration of systems and technology, we believe that forcing institutions with highly sophisticated and interdependent anti-fraud mechanisms to consider and implement significant changes in less than 18 months may result in suboptimal results.

* * * * *

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 LLP, at (202) 736-8368, our counsel in connection with this matter.

Sincerely,



Jodi Golinsky
Vice President &
Regulatory and Public Policy Counsel

cc: Michael F. McEneney, Esq.