Consumers Union
Nonprofit Publisher of Consumer Reports

August 28, 2006

Office of Comptroller of the Currency
Board of Governors of the Federal Reserve Board
Federal Deposit Insurance Corporation
Office of Thrift Supervision
National Credit Union Administration
Federal Trade Commission

Re: Comments of Consumers Union on Proposed Regulations on Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003

OCC Docket Number 06-07, RIN 1557-AC87
FRB Docket Number R-1255
FDIC RIN 3064-AD00
OTS No. 2006-19, RIN 1550-AC04
NCUA Proposed Rule 717
FTC Project No. R611019, RIN 3084-AA94

Consumers Union, the nonprofit publisher of *Consumer Reports*,[1] offers these comments on the Proposed Identity Theft Red Flags rule. Financial institutions and other creditors play a significant role in facilitating identity theft. A thief generally must open a new account or misuse an existing account in order to turn stolen personal information into cash. Increased care by financial institutions, credit grantors, and other entities that open new accounts will reduce the ease of committing identity theft.

The red flag rules will not fulfill this promise if they permit so much discretion to financial institutions and creditors that those entities do not need to increase the levels of care they currently exercise in opening new accounts and in handling transactions in connection with existing accounts.

[1] Consumers Union is a nonprofit membership organization chartered in 1936 to provide consumers with information, education, and counsel about goods, services, health and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's publications, including *Consumer Reports*, have a combined paid circulation of approximately 7.4 million and regularly carry articles on its own product testing, health, product safety, marketplace economics, and legislative, judicial, and regulatory actions which affect consumer welfare. Consumers Union's income is solely derived form the sale of *Consumer Reports*, its other publications and services, and from noncommercial contributions, grants, and fees, and Consumers Union's publications and services carry no outside advertising and receive no commercial support.

West Coast Office
1535 Mission Street
San Francisco, CA 94103
415.431.6747 tel
415.431.0906 fax
www.consumersunion.org

Summary of Issues

- The address discrepancy duties of users of consumer reports should not be satisfied merely by failure to verify the identity of the customer.

- The Customer Identification Program (CIP) rules are insufficient as the obligations of a user of a consumer report after a notice of address discrepancy.

- The regulations should require contact with the customer when activity resumes after two years of inactivity unless this pattern would be expected for the type of account.

- The emphasis on detecting precursors to identity theft and the risk of possible identity theft is the right approach.

- The regulations should not give a financial institution or creditor the discretion to exclude from the red flag program any types of accounts which are opened by individuals or which reflect on the credit standing or financial reputation of an individual.

- The regulations should not give a financial institution or creditor the discretion to exclude from the red flag program any red flags which are relevant to the types of accounts included in its Program.

- The red flag program must protect persons who are not current customers of the financial institution or creditor when someone impersonates them with that entity.

- The regulations should require that consumers be told when a red flag which requires response has been detected.

- Staff training must be supplemented with monitoring, oversight, and auditing

- A decision to outsource should not lead to lower red flag standards.

- The definition of account is too narrow because it is tied to financial products and services which can be offered under the Bank Holding Company Act.

- The definition of “board of directors” is flawed for non-board entities.

- The obligations of card issuers should extend for more than 30 days after a change of address.

- A change of cardholder address followed by a request for additional or replacement cards should generally require actual contact with the cardholder.

- Email notice to the customer without prior E-Sign consent will contribute to phishing.

1. Duties of users of consumer reports regarding address discrepancies and notice to holders of inactive accounts.

1.A It should not be sufficient to determine that no reasonable belief in the identity of the consumer can be formed.

The regulations should be amended to require that the user of a consumer report must verify the identity of the applicant before opening a new account once the user has been notified of an address discrepancy. In their current form, the proposed regulations require only that the user do one of two things: 1) form a reasonable belief that it knows the identity of the consumer; or 2) determine that it cannot form a reasonable belief that it knows the identity of the consumer. See Section 681.1(c); __.82(c).[2] The regulations contain no restriction on granting of the credit after a user of a consumer report determines that it cannot form a reasonable belief in the identity of the applicant. This does not make sense.

Congress specifically required new steps after an address discrepancy notice. The Fair Credit Reporting Act (FCRA), as amended by FACTA, requires more than an inability to form a reasonable belief in the identity of the consumer. The FCRA requires that the regulations describe reasonable policies and procedures for the user of a consumer report to "form a reasonable belief that the user knows the identity of the person to whom the consumer report pertains." 15 U.S.C. section 1681c(h)(2)(B). The statute does not state or imply that inability to form a reasonable belief is or should be adequate.

Presumably a purpose of this FACTA requirement was to reduce the number of new accounts opened using false addresses, a common method of committing identity theft and of delaying its discovery. The address discrepancy section will be rendered meaningless if the user can satisfy its obligations under the regulations simply by determining that the user is unable to verify the identity of the customer, and then grant the credit application anyway.

While the explanatory material, at page 26, points out that other portions of the CIP rules may require responses such as denying a new account, or closing an account, the proposed regulations appear to be fully satisfied when the user determines that it is unable to form a reasonable belief that it knows the identity of the person.

Suggested change: At section 681.1(c), delete "or determine that it cannot do so" and substitute "denying the application if it cannot do so." Make the same change at sections 41.82(c) (OCC), 222.82(c) (FRB), 334.82(c) (FDIC), 571.82(c) (OTS) and 717.82(c) (NCUA).

[2] The varying numbering systems for these otherwise identical regulations make providing comments a challenge. The FTC numbered sections will be discussed, with parallel sections also noted.

1.B The safe harbor for the use of the Customer Identification Program rules in response to address discrepancies is not appropriate.

Sections 681.1(c) and __.82(c) permit the use of the procedures "regarding identification and verification" under the Customer Identification Program (CIP) rules. However, those do not set the appropriate standard for investigating customer identity after an address discrepancy in this context for several reasons. First, the CIP rules allow the activity to verify the address to occur *after* the account has been opened. This could make sense in a context for which the CIP rules were designed – routine screening of all new customers. Here, however, there has already been an address mismatch between the application address and the address on file at the consumer reporting agency. This should call for more action before, not just after, an account is opened.

Second, the CIP rules do not require contacting the consumer. Because the use of a false address is so central to the effective commission of identity theft, there should be a strong presumption in favor of contacting the consumer.

It is also not clear whether the use of the CIP rules as a safe harbor will require use of the full rules, or just a portion of them. The explanatory material at page 26 points out that the CIP rules may require responses from financial institutions such as denying a new account or closing an account but the regulations are not clear whether the response obligations under the CIP rules apply equally to another type of creditor who opts to use the rules for this safe harbor purpose. If the cross reference to the CIP rules is not eliminated, then it should at least be tightened to clarify that the safe harbor applies only when the entity also follows the portion of the rules addressing how to respond to the inability to form a reasonable belief in the identity of the consumer.

The explanatory material suggests that a purpose of referring to the CIP rules is to ensure that the red flag guidelines are not inconsistent with the CIP rules. However, it also would not be inconsistent to permit that the CIP rules be used, but to specify when more steps are needed or when the timing should be earlier.

Suggested change: At section 681.1(c) and each section numbered __.82(c), delete: "A user that employs the policies and procedures regarding identification and verification set forth in the Customer Identification Program (CIP) rules implementing 31 U.S.C. 5318(I) under these circumstances satisfies this requirement, whether or not the user is subject to the CIP rules."

Alternative suggested change: At section 681.1(c) and each section numbered __.82(c), modify: "A user that employs the policies and procedures regarding identification and verification set forth in the Customer Identification Program (CIP) rules implementing 31 U.S.C. 5318(I), including the rules with respect to denying or closing an account when the identity of the consumer cannot be verified, under these circumstances satisfies this requirement, whether or not the user is subject to the CIP rules."

1.C The regulations should change their approach to the FACTA Section 114 issue of notice to holders of previously inactive accounts.

The agencies ask whether the proposed regulations should be revised to impose a direct requirement to notify the consumer when there is activity on an account that has been inactive for the previous two years. The proposed regulations currently treat this as a red flag, giving financial institutions and creditors broad discretion about whether to include this red flag at all, and about whether or not to notify the account holder if the flag is included and detected. Consumers Union respectfully suggests that the regulations should instead require notice to the consumer. If there is to be any exception at all, it should be tied to a specific characteristic of the account that makes it highly unlikely that long inactivity followed by activity is an indicator of possible risk of identity theft. Such a characteristic might be that a certificate of deposit is for a two or three year term, so that normal use of the account would not involve activity within a two year period. Short of any such limited exceptions, however, the regulations should be revised to require notice to the consumer when there is activity after a two year period of inactivity.

Suggested change: Add a new section to require notice to the consumer when a transaction occurs in connection with a consumer's credit or deposit account that has been inactive for two years.

2. The Red Flag program: Overview of comments.

The red flag regulations make several important positive choices, but these positive choices are undermined by the broad discretion which the regulations confer on financial institutions and creditors to decide what to include in the Program and how to respond to those red flags which are included. This broad discretion may cause the regulations to have very little impact.

Consumers Union supports the following positive aspects of the proposed regulations. The proposed regulations use an expansive definition of account, although the definition needs changes to fully protect the person impersonated when he or she is not an account holder at that institution and to apply to credit extended for nonfinancial products and services. The regulations use a strong definition of identity theft. The regulations appropriately adopt the "precursor" approach, which requires response from the financial institution or creditor when there is an indication of possible identity theft risk. The regulations also require that, once an account and a red flag type are included in a Program, a financial institution or creditor must have a reasonable basis for concluding that a detected red flag does not evidence a risk of identity theft. However, these benefits will be undermined unless more clarity and stringency is added to the "risk based approach" used in these proposed regulations.

Consumers Union believes that the "flexible, risk based approach" will undermine the effectiveness of the red flag process. The risk based approach lets financial institutions and creditors make the key decisions about which accounts and red flags to consider, and what to do about identified risks. This could very easily permit "business as usual." The fact that Congress required regulations to address the issue of red flags shows that Congress thought that financial institutions and creditors were not already doing enough to respond to red flags.

The risk based approach in these proposed regulations builds in the flaws and failures of "business as usual" in at least three ways. First, the explanatory material suggests that the regulations are intended to permit each financial institution or creditor to decide which accounts, or which types of accounts, will be covered by each entity's red flag program. Second, the proposed regulations let each financial institution or creditor select which red flags it considers relevant. An entity that does not select a red flag for inclusion in its Program avoids all obligations of additional response when that red flag is present. Third, once a red flag is included in the Program and is detected, the financial institution or creditor has broad discretion in how to address it and can even choose not to tell the customer about the known danger sign. As discussed in more detail below, Consumers Union believes that there should be less discretion to exclude account types and red flags, and that consumers should be told whenever a red flag is detected.

2.A The emphasis on detecting precursors to identity theft, instead of waiting for proven cases, is the right approach.

The proposal seeks comment on the "precursor" approach, including whether the definition of red flags should include precursors to identity theft and the use of the concept of "possible risk" of identity theft. Consumers Union strongly agrees that the definition of red flag, and the nature of the Program to be developed under the red flag process, should include a strong focus on detecting and responding to precursors to identity theft and to the possible risk of identity theft. It is not enough to address identity theft only after an investigation confirms it. Including "precursors" in the definition of a red flag and including "possible risks" is essential. The use of a definition of identity theft which includes attempts is valuable for the same reasons. As discussed in the next two sections below, the value of the precursor approach should not be undermined by permitting excessive discretion to exclude types of accounts or types of red flags from the Program.

2.B The regulations should be changed to clarify that they do not confer discretion to exclude types of accounts held by or affecting individuals from the red flag program.

The explanatory material states that the risk based approach allows a financial institution or creditor to select which types of accounts are subject to its red flag program. In discussing the definition of customer, the explanatory material states (at p. 16, and note 12) that "a financial institution or creditor would have the discretion to determine which type of customer accounts will be covered under its Program, since the proposed Red Flag regulations are risk-based." It cites section __.90(d)(1) for this principle. It is hard to see this free reign in the actual language of the regulation, but section __.90(d)(1) cross references __.90(d)(1)(ii), which requires at (A) that the financial institution or creditor consider "which of its accounts are subject to a risk of identity theft."

Consumers Union takes no position on the appropriateness of excluding certain types of accounts that might be held by highly sophisticated businesses with their own risk assessment and prevention programs, although we note that identity theft from businesses is widely reported to be a growing problem. However, there should be no flexibility to exclude accounts which are held by individuals or which generate information about individuals that reflects on their financial or credit reputations. (At page 22, the explanatory material suggests that a financial institution might decide that only credit accounts and not deposit accounts should be included in its red flag program.) The regulations should require inclusion of all accounts in which individuals hold or borrow funds, and any other type of account which is a basis for any reporting to a consumer reporting agency about an individual. An example of this latter category would be a business account with a personal guarantee, which may result in adverse reporting to the consumer reporting file of an individual.

The explanatory material should clarify that any flexibility to exclude types of accounts should be limited to accounts that are not held by individuals, do not affect the funds of individuals, do not extend credit to individuals, and do not affect the financial or credit reputation of individuals. The language of the regulations should be changed to eliminate the discretion to exclude types of accounts, or to restrict that discretion to business accounts.

Suggested change: Subsection 681.2 (d)(1)(ii)(A) and each subsection numbered __.90(d)(1)(ii)(A) should be modified to read: "<u>The nature of the possible risk of identity theft to which each type of account offered by the financial institution or creditor is subject.</u>"

Conforming changes should be made in any other section which can be read to confer flexibility to exclude individual accounts or categories of accounts which are offered by the entity and are held by or affect individuals.

2.C The regulations should clarify that a financial institution or creditor does not have unfettered discretion to choose which red flags are relevant, but instead may exclude only those that are not applicable to any type of account included in the entity's red flag program.

The proposed regulations require that each financial institution or creditor select the relevant red flags. See Section 681.2(d)(1) and each section numbered __.90(d)(1) (requiring selection of "relevant" red flags in two places in the text). This language could confer unbridled discretion to select which red flags must be detected and thus may prompt any response. If the purpose of allowing the financial institution and creditor to select only the "relevant" red flags is simply that certain types of red flags are only associated with certain types of accounts, then the language should be tightened to make it clear that the "relevance" determination is not subject to unfettered discretion. The modification would clarify that the relevance standard permits exclusion only of those red flags that are objectively not relevant to any type of account covered by the red flag program of that financial institution or creditor.

Unfettered discretion of each financial institution or creditor to select the "relevant" red flags would significantly undermine the red flag process. Many of the red flags listed in the guidelines are clear indicators of a heightened risk of identity theft. It should never be acceptable for a financial institution or a creditor to deem those red flags not relevant. Examples of red flags of this type are numerous. They include:

> Apparent alteration of identity documents;
>
> The person presenting the identification doesn't match the physical description on the identification;
>
> The SSN range and date of birth are inconsistent;
>
> The address or phone number on the application is the same one used on other applications which have proven to be fraudulent;
>
> A person informs the financial institution or creditor that it has opened a fraudulent account;
>
> An employee of the financial institution or creditor has been added as an authorized user of the account;
>
> Attempts at unauthorized access are detected; and
>
> An employee has accessed or downloaded an unusually large number of customer account records.

The regulations should not give a financial institution or creditor the flexibility to decline to select red flags for its Program unless it does not offer any accounts where a particular type of flag can occur.

Suggested change: Section 681.2(d)(1) and each section numbered __90.(d)(1) should be modified to replace "that are relevant to detecting" with "<u>for detecting</u>" and to modify: "At a minimum, the Program must incorporate any relevant Red Flags from:" to read: "At a minimum, the Program must incorporate any Red Flags <u>relevant to the types of accounts offered by the financial institution or creditor</u> from: [the list follows]."

2.D The regulations inappropriately limit the duty of a financial institution or creditor solely to those who are already "customers." The definition of customer should be changed to make it clear that the red flag program must cover those persons being impersonated even if they are not existing customers of the financial institution or the creditor.

Sections 681.2(c) and __.90.2(c) require that each financial institution and creditor have an Identity Theft Prevention Program which includes policies and procedures "to address the risk of identity theft to its customers" and for safety and soundness. Under definition (b)(3), a

"customer" means a person who has an account. Limiting the Program to "customers" means that red flags which are designated and detected still do not need to be addressed by the Program if the person the thief is trying to impersonate is not already in an account relationship with the financial institution or creditor selected by the thief. While this sounds like nonsense, it is also an accurate description of the duty imposed by the proposed regulations as written.

There is no indication that Congress intended such an irrational limitation on the scope of the red flag process. Congress did not limit the purposes of the red flag program to the protection of existing customers, as do the proposed regulations as written. Instead, the statutory language requires the agencies to establish guidelines "for use…*with respect to* account holders at, or customers of, such entities…" FCRA Section 615(e)(1)(A)(emphasis added).

Suggested change: Amend section 681.2(b)(3) and each section numbered __.90(b)(3) to read: "Customer means a person that has an account with a financial institution or creditor, and a person in whose name such an account is sought."

Alternative suggested change: If the definition of customer is not expanded, then section 681.2(c) and each section numbered __.90(b)(c) should be revised so that the Program must address identity theft prevention even if the person being impersonated is not a current customer of the financial institution or creditor. One way to do this would be to require in section 681.2(c) and each section __.90(c) that: "The Program must include reasonable polices and procedures to address the risk of identity theft to its customers and to individuals who may be impersonated by its actual or potential customers…" A conforming change would be needed at subsection 681.2(d)(1)(i) and __.90(d)(1)(i), which also refer only to detecting a possible risk of identity theft "to customers" and to the financial institution or creditor, but not to the other persons impersonated.

2.E The regulations should require that financial institutions and creditors notify consumers when a red flag is detected which requires response, in addition to other steps which should be taken.

The proposed regulations require a response by the financial institution or creditor only when all of these preconditions occur: an account is included in the program, a type of red flag is determined to be relevant and so included in the Program, a red flag is detected, and the financial institution or creditor cannot conclude that that the red flag does not evidence a risk of identity theft. After all these preconditions have been met, the regulations describe what response is expected, in subsections 681.2(d)(2)(iv) and __.90(d)(2)(iv). However, these subsections leave it up to the financial institution or creditor whether or not to tell the consumer about the red flag. The regulations should instead require that the consumer be told, without suggesting that notice should be the only response. If a consumer is being impersonated at one financial institution or creditor, it may very well be occurring, or likely to occur again, at a different location. The consumer might be able to discover or thwart the impersonator if the consumer learns about each attempt. Without notice, the consumer won't receive this opportunity. A consumer who knows that someone is trying to misuse an existing account might decide to close that account even if

the financial institution doesn't think that closure is essential. Without notice, the consumer doesn't have a chance to make that personal choice.

Suggested change: Revise subsection 681.2(d)(2)(iv) and __.90(d)(2)(iv) to require that (B), contacting the customer, be performed in every case, and that the financial institution or creditor also address the risk by other methods, such as those described in (A), (C) – (I).

2.F The regulations properly impose a requirement that a financial institution or creditor must have a reasonable basis to conclude that a red flag does not evidence a risk of ID theft.

Consumers Union is in strong support of the principle reflected in subsection 681.2(d)(2)(iii) and the parallel sections numbered __.90(d)(2)(iii) of the other proposed regulations that a financial institution or creditor must have a reasonable basis to conclude that a red flag does not, in the particular instance, evidence a risk of identity theft. Identity theft thrives when financial institutions and other creditors make decisions which may be convenient for them, but harmful to the consumer, in the absence of complete information. Once a red flag which has been included in the Program is detected, it should impose an obligation for a higher level of pre-transaction activity to prevent or reduce the risk of identity theft.

2.G Staff training must be supplemented with monitoring, oversight, and auditing.

The regulations require staff training in the Program, at subsection 681.2(d)(3) and subsections __.90(d)(3). However, the regulations should also require monitoring and oversight with periodic auditing to evaluate the effectiveness of that staff training.

Suggested change: Add to subsection 681.2(d)(3) and each subsection numbered __.90(d)(3), "and must maintain and implement a plan to monitor, evaluate, and audit compliance with that training."

2.H An outsourcing entity should remain responsible for compliance, and should not be able to reduce its level of obligation by outsourcing to a smaller entity.

Section 681.2(d)(4) and the sections numbered __.90(d)(4) require "steps designed to ensure" that outsourced activities are conducted in compliance with a Program that meets the requirements of the regulations. This is helpful, but raises two concerns. First, these regulations should plainly state that the outsourcer is responsible if there is a failure of compliance. Second, the cross references to sections 681.2(c) and 681.2(d) and to ___.90(c) and ___.90(d) do not make it clear whether the Program of the entity receiving outsourced work must be "appropriate to" its own size and complexity or to the size and complexity of the entity for whom it is performing the work. The higher of the two standards should apply. A billion dollar financial institution should not be able to expose its customers, or potential customers, to a less stringent Program simply by choosing to outsource to a much smaller vendor. Instead, the sections on

oversight of service providers should make it clear that the outsourcer is responsible to ensure that the receiver of the work has a Program that would qualify if it were the program of the outsourcer itself.

Suggested change: Section 681.2(d)(4) and each section __.90(d)(4) should be revised to require that "…., the financial institution or creditor must take steps designed to ensure that the activity is conducted in compliance with a Program that meets the requirements of paragraphs (c) and (d) of this section. That Program must also meet the requirements that would apply if the activity were performed without the use of a service provider. In addition to any responsibility on the service provider imposed by law, regulation or contract, the financial institution or creditor is responsible in the event of a failure of compliance with the regulations or with the Program."

2.I The definition of "account" should be expansive. The definitions of "account" or "customer" should be altered to apply the red flag program to potential ID theft victims who do not have an account with the entity where the impersonator attempts to open or use an account.

The introductory material characterizes the definition of "account" as expansive, and asks whether it should include non-continuing relationships. Consumers Union supports an expansive definition of "account." The regulations and guidelines should reach any relationship in which funds could be intercepted, credit could be extended, or another step that would be taken which would ostensibly obligate an individual or other covered entity to the financial institution or to a third party. This might include some types of non-continuing relationships.

The use of the term "account" could imply that a financial institution has no obligation to the actual consumer who does not have an account with it when an imposter attempts to open such an account. This would be the wrong result. The lack of an account relationship between the financial institution or other covered entity and the true individual should not eliminate the obligation to verify the identity of the person claiming to be that individual. The discussion at Part 2.D, above, suggests a way to resolve this concern through changing the definition of customer.

2.J The definition of "account" excludes many types of credit offered by non-banks.

The red flag process should apply to an account, such as a cell phone account, where services are advanced for later payment, particularly where nonpayment on the account can result in an adverse report to the consumer reporting file. However, the definition of "account" may prevent this result.

"Customer" is defined as a person "that has an account with a financial institution or creditor." Sections 681.2(b)(3) and __.90(b)(3). However, a relationship is not an "account" unless it is a continuing relationship established "to provide a financial product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to

such financial activity" under the Bank Holding Company Act (BHCA). Section 681.2(b)(1) and __.90(b)(1).

Even if this definition of "account" works for financial institutions, it unwisely limits the types of accounts offered by non-financial institution creditors that are subject to the red flag regulations and guidelines. For example, a cell phone or utility service is not a *financial* product or service, so appears to fail to qualify under the definition of account.

Fake cell phone accounts were part of how the scammers who stole ChoicePoint information impersonated consumers. Cell phone, wireless, and utility accounts constitute a significant proportion of the ID theft complaints to the FTC-sponsored Consumer Sentinel database. Taken together, there were more complaints about new account fraud for these types of accounts in three recent years than for credit cards.

The Consumer Sentinel information reveals:

Complaints about unauthorized new accounts as a percentage of total identity theft complaints

	2003	2004	2005
Credit card	19.3	16.5	15.6
Total of wireless, phone, And utility	20.1	20.1	19.7

Source: FTC Consumer Sentinel, Identity Theft Data Clearinghouse, *How Identity Theft Victims' Data is Misused, 2003 – 2005*. http://www.consumer.gov/sentinel/Sentinel%20CY-2005/victim_info_misused.pdf

Suggested change:

At section 681.2(b)(1) and each section __.90(b)(1), add: "Account, with respect to a financial institution, means a continuing relationship established to provide a financial product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such financial activity under section 4(k) of the Bank Holding Company Act, 12, U.S.C. 1843(k). Account, with respect to a creditor who is not a financial institution, means a continuing relationship for the extension of credit, including the payment for goods or services after delivery of such goods or services on a monthly or other periodic basis. Account includes:

(i) An extension of credit for personal, family, household or business purposes, such as a credit card account, margin account , [or] retail installment sales contract, such as a car loan or lease, or such as an arrangement for monthly or periodic payment for the rendering of goods or services; and

(ii) [no change]."

2.K The definition of "board of directors" is flawed for entities without a board of directors.

Where there is no board of directors, the regulations define "board of directors" at subsections 681.2(b)(2)(ii) and __.90(b)(2)(ii) to mean "a designated employee." An issue that is important enough for the regulations to require the attention of the board of directors or a managing official for entities with boards should not simply be the purview of any designated employee for entities without boards. A covered entity should not be free to select any employee, no matter how little authority or responsibility that employee may carry within the company, as the person to oversee its Program duties. At a minimum, the regulation should require that the employee designated be at a specific level of authority or responsibility.

Suggested change: Modify subsection 681.2(b)(2)(ii) and each subsection numbered __.90(b)(2)(ii): "In the case of any other creditor that does not have a board of directors, a designated employee <u>at the level of senior management.</u>"

3. Changes of address to card issuers in proximity with requests for more cards.

3A. Requests for additional or replacement cards should trigger added obligations for at least 90 days after a change of address.

The FCRA requires that the regulations impose obligations on card issuers when a request for an additional or replacement card is received in a short period of time after a change of address. The FCRA §615(e)(1)(C) parenthetically notes "(during at least the first 30 days after such notification is received)." The phrasing of the parenthetical suggests that Congress set a minimum, but not a maximum, on the regulators' discretion to select a time period which is "short" for purposes of the proximity between a change or address and a request for an additional or replacement card.

These regulations can and should select a longer time period, such as 90 days. Thieves can use a change of address to redirect a statement, thus lengthening the time it will take to discover fraudulent use of a replacement or additional credit or debit card. Added scrutiny after an address change which is followed by a request for replacement or additional cards is a good way to reduce this form of fraud. Using the shorter 30 day period means that a thief could redirect the statement, wait 31 days, and then request and use a new card while the consumer is still waiting for his or her statement to arrive at the real address. Irregularities and delays in the U.S. mail may mean that the real consumer won't think of fraud when a statement is a few days or even a week late. Changing statement dates and dates that fall on different days of the month for different cards can make it more difficult for the consumer to notice that a particular statement did not arrive. Triggering the extra care obligations for the first 90 days, instead of just the first 30 days, would increase the likelihood that the consumer would be notified or other action taken to determine if fraud was involved in the request for a replacement or additional card.

The longer time period is particularly important for debit cards, because the disruption to household finances is more significant when a debit card is misused. Despite legal rights to the return of funds after an unauthorized withdrawal, the absence of stolen funds for the ten business day period permitted by the Electronic Fund Transfer Act can significantly impair a family's ability to pay bills and sustain cash flow.

Suggested change: Change "30" to "90" at subsection 681.3(c) and each section numbered __.91(c)(3).

3.B The regulations should only very rarely permit a means of assessing the validity of a change of address other than contacting the customer.

A change of address followed by requests for more cards is a well known and easy to use method of theft from existing accounts. Because of this, the regulations should require that the card issuer must *contact and notify* the consumer unless there are special circumstances that prevent reaching the consumer in a timely manner (for example when the attempt to contact is met with information such as extended vacation, medical incapacity, or other unavailability of the cardholder.) This issue is of particular importance for holders of debit cards, whose accounts may be drained and financial lives disrupted by a thief who receives an additional or replacement card at the changed address.

Suggested changes: Section 681.3(c)(1) and (2) and each section numbered __.91(c)(1) and (2) should be changed to: "notify and receive a response from the cardholder." Section 681.3(c)(3) each section numbered __.91(c)(3) should be changed to restrict it to be used only: "When there are special circumstances that prevent reaching the consumer in a timely manner using the methods described above, then….."

3.C Email notice should be used only with E-Sign consent, to avoid creating more opportunities for phishing.

Section 681.3(c)(2) and __.91(c)(2) permit email notice with an agreement even where there has been no consent to email receipt of notices under the federal E-Sign Act. Consumers may ignore change of address inquiry emails because of an assumption that these are false "phishing" emails. There is also a risk that false, phishing emails will be sent posing as notices about address changes. Limiting the use of email only to those circumstances where the consumer in fact has consented to the use of email under the strictures of the federal Electronic Signatures in Global and National Commerce Act (E-Sign) may help to reduce the volume of wholly unexpected emails. While the regulations require a prior agreement to communicate by email, that "agreement" might be in the fine print of a long online access screen that may not have been read. E-Sign sets up a somewhat more formal process for eliciting agreement, making it more likely that the consumer may realize that he or she has agreed to the use of email for this purpose.

Suggested change: At section 681.3(c)(2) and each section numbered __.91(c)(2), add: "If that form of communication is electronic, the cardholder should have previously agreed to its use under the Electronic Signatures in Global and National Commerce Act."

Conclusion

While these regulations make a few strong choices, such as taking the "precursor" approach, their value will be undermined by the multiple layers of discretion they provide to financial institutions and creditors to exclude accounts, to exclude red flags not considered relevant, and to decide how much care to take – and whether to tell the customer – even after a red flag has been detected which can't be dismissed as not evidencing a risk of identity theft. The red flag process should be strengthened by tightening or removing these layers of discretion, and should require notice to the customer in addition to other appropriate preventative and remedial steps.

Consumers Union may also join in comments filed by other consumer organizations addressing these proposed regulations in more detail.

Very truly yours,

Gail Hillebrand