Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003

Comments Submitted by:
Privacy Rights Clearinghouse
Joined by:
Consumer Action
National Consumer Law Center
PrivacyActivism
US Public Interest Research Group (US PIRG)
World Privacy Forum

September 18, 2006

Federal Trade Commission
Office of the Secretary, Room H-135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, DC 20580
Filed electronically: https://secure.commentworks.com/ftc-redflags

RE: The Red Flags Project No. R611019

Dear Mr. Secretary:

The Privacy Rights Clearinghouse (PRC)[1] and the above-listed organizations[2] take this opportunity to comment on the joint notice of proposed rulemaking (NPRM) published by the federal banking agencies and the Federal Trade Commission (FTC) ("Agencies").[3] The NPRM implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA).[4]

[1] The Privacy Rights Clearinghouse (PRC) is a nonprofit consumer education and advocacy organization based in San Diego, CA, established in 1992.

[2] Descriptions of the organizations that have signed onto these Comments are included at the end.

[3] The FTC is joined in this proposal by the Federal Deposit Insurance Corporation (FDIC); Office of Comptroller of Currency (OCC); Office of Thrift Supervision (OTS); Federal Reserve Board (FRB); and the National Credit Union Administration (NCUA). We submit our comments only to the FTC with the understanding that these comments will be available to all Agencies concerned in the proposed rulemaking.

[4] [4] FACTA Section 114 amends Section 615 of the Fair Credit Reporting Act (FCRA), which requires the federal banking Agencies and the FTC to establish guidelines for financial institutions and creditors to detect possible identity theft, so called "Red Flags." FACTA Section 315, which amends FCRA Section 605, requires the Agencies to provide guidance when a consumer reporting agency (CRA) reports an address discrepancy to a consumer report user.

We direct our comments as follows:

1. Introduction

The detection of red flags and the need to reconcile address discrepancies are among the most important anti-identity theft measures included in FACTA. Effective business policies and practices that spot attempted and actual identity theft early have great potential for relieving this national crime wave. This was the promise and Congress' intent when it directed the Agencies to adopt Red Flag Regulations along with procedures to reconcile address discrepancies in credit reports.

When it comes to identity theft control, there is little encouragement to be had. Studies conducted in recent years vary somewhat about numbers of victims, costs and recommended solutions.[5] But, no matter which survey methodology is used, the overall conclusions are the same. The numbers are staggering.

Every year identity theft claims millions of victims. Victims spend millions of dollars and countless hours to clear their name. Add to this the emotional toll on victims that cannot be equated to dollars. Financial institutions and creditors write off billions annually in loss due to identity theft and other fraud. The magnitude and seriousness of fraud cannot be overstated.

Long-awaited direction from the Agencies requires a written Identity Theft Prevention Program (Program) which calls for a new scheme of administrative duties for credit grantors and financial institutions. Beyond this, the proposal provides little in the way of affirmative actions entities must take to implement identity theft solutions.

---

[5] *How Many Identity Theft Victims Are There? What Is the Impact on Victims?,* www.privacyrights.org/ar/idtheftsurveys.htm

In adopting FACTA Sections 114 and 315, Congress recognized that lax business practices play a significant role in aiding identity thieves. In response to Congress' mandate, the Agencies rely too heavily on two sets of existing guidelines: (1) the Customer Identification Program rule adopted under section 326 of the USA PATRIOT Act, 31 USC 5318(l), (CIP rule) adopted as a counter-terrorism measure; and (2) the information security guidelines adopted under the Gramm-Leach-Bliley Act, 15 USC 6801, (GLB).

Neither the CIP rule nor the GLB safeguarding guidelines provide an adequate base to effectively prevent and mitigate identity theft. The CIP rules have been in effect for over three years and there is nothing to suggest identity verification procedures required under this rule have had a deterrent effect on new account fraud, a most insidious form of identity theft. Despite the data security measures required by GLB and the law's implementing regulations, data security breaches are almost a daily occurrence.[6]

The red flags listed in the proposal include many of the events closely associated with identity theft. The proposal also correctly adopts a definition of identity theft that includes attempts as well as actual fraud. Potential risks of identity theft resulting from precursors such as phishing are also the right approach.

However, overall, the proposal incorporates far too much discretion that allows financial institutions and creditors to reject even the most obvious signs of identity theft. An effective Program should not allow companies to choose not only which *red flags* to incorporate but also which *accounts* are subject to the red flags. To do so creates the prospect that companies will adopt perfunctory Programs that amount to no more than the status quo. For the final rules and guidelines, the Agencies should act to eliminate the many layers of discretion incorporated into the proposal.

We offer the following comments and suggestions on various aspects of the proposed guidelines and regulations.

2. Comments on Proposed Definitions

a. Board of Directors. The proposal on the one hand signals the importance of an Identity Theft Prevention Program by requiring approval and reporting to the board of directors or "senior management." [71 Fed Reg 40789] However, the principle that a senior management level employee is responsible for the Program is not included for organizations without a board of directors. Instead of "designated employee," the Agencies should specify that, absent a board of directors, a senior manager is charged with overseeing the Program.

[6] The PRC tracks data security breaches. Since early 2005, personal information in over 93 million records has been compromised. Many of these data breaches involve financial institutions or others in the credit industry that are subject to the GLB data security guidelines and would also be required to adopt Programs under the Red Flag Regulations. *A Chronology of Data Breaches,* www.privacyrights.org/ar/ChronDataBreaches.htm .

b. Identity theft. The Agencies are correct in proposing the FTC's definition of identity theft which includes not only actual occurrences but attempts at fraud as well. A thief may try numerous times to open a new account. While the level of success may depend on the effectiveness of a creditor's Program, the attempt alone – which results in an inquiry on the victim's credit report -- is a signal that a consumer's personal information is "in play."

This definition of identity theft, if accompanied by notice to consumers that an attempt has been made, would be a significant deterrent. As a minimum, creditors should alert existing customers to an attempted fraud. Even when the attempt is unsuccessful, the consumer's credit score would be adversely affected by new inquiries on the credit report. With knowledge of a failed attempt, the consumer may take preventive measures such as placing a fraud alert on the credit report and corrective measures such as requesting that an erroneous inquiry be deleted from the credit report.

The Agencies have struck the right balance by including attempts at identity theft. For an effective deterrent, the final rules should go a step further and require contact with the consumer when an attempt at identity theft is made.

c. Account is defined as a "continuing relationship" and the proposal then offers certain examples of accounts, all of which relate to accounts maintained by financial institutions covered by the Gramm-Leach-Bliley Act (GLB). The proposal later goes on to state that:

> The Agencies expect that the final Red Flag Regulations will apply to a wide variety of financial institutions and creditors that offer many different products and services, from credit cards to certain *cell phone accounts*. [71 Fed Reg 40791] [emphasis added.]

Identity thieves often establish cell phone or utility accounts in the victim's name. In truth, setting up a fraudulent cell phone or other non-financial account may be the thief's stepping stone to assuming the victim's entire identity. Once a thief has set up a fraudulent cell phone account, a creditor might open an account by merely verifying an operating cell phone number.

The Agencies have requested comment on whether additional or different examples of accounts should be added. We agree that the regulations should apply to a wide variety of products and services. The definition of "account" should clarify that the regulations cover much more than financial accounts with a financial institution.

Examples of accounts covered by the Red Flags Rules should realistically reflect the variety of ways in which a victim's information may be misused. As the Agencies are well aware, identity thieves are a creative lot, and the fraudulent use of another's identity is not limited to financial services and products. A recent report by the World Privacy Forum, for example, estimates that as many as 250,000 individuals are annually billed for

medical services and products provided to an impostor.[7] As a minimum, account examples should include the most common occurrences of identity theft such as phone and utility accounts. [8]

The Agencies also request comment on whether the definition of "account" should include relationships that are not "continuing" that a person may have with a financial institution or creditor**.** This points to a significant problem with the proposed definition of "account."

By limiting the definition of account to a "continuing" relationship, the proposal fails to integrate new account fraud, a most insidious form of identity theft.[9] This shortcoming is even more evident when the definition of "customer" includes only a "person that has an account with a financial institution or creditor."

The definitions of both "account" and "customer" should be amended in the final rules to clearly apply to accounts opened or attempted by an impostor. Inclusion of such language is consistent with the rule's proposed definitions of "identity theft" and "Red Flags," both of which incorporate the concept of *possible risk* and *attempts* at fraud.

d. Red Flags, as proposed, is defined as a pattern, practice, or specific activity that indicates the possible risk of identity theft. The Agencies request comment on the scope of the definition, specifically whether precursors should be included in the definition. We support this definition and agree that events such as phishing and a security breach involving the theft of personal information signal a heightened risk of identity theft.

3. Inadequacies of Customer Identification Program (CIP) Guidelines

The proposed regulation permits creditors to use their CIP rules to verify the identity of a person opening an account. However, the use of a CIP rule is insufficient to address identity theft. While elements of the CIP rule standards might constitute a starting point for identity verification, the CIP rule fails to address the specifics of identity theft given that its primary purpose is to aid law enforcement in detecting money laundering.

As with the proposed regulations for red flag Programs in general, the CIP rule leaves too much discretion to the creditors to decide which measures to implement. The CIP rule

---

[7] *Medical Identity Theft: The Information Crime that Can Kill You.* (Spring 2006) www.worldprivacyforum.org/medicalidentitytheft.html

[8] The FTC's most recent report on identity theft and other consumer complaints listed fraudulent use of phone and utility accounts as second only to credit card fraud. www.ftc.gov/opa/2006/01/topten.htm

[9] The FTC's 2003 study on identity theft concluded that new account fraud not only takes longer for victims to detect, but also takes more time to correct. www.ftc.gov/os/2003/09/synovatereport.pdf

was designed to give banks significant flexibility.[10] Identity verification for red flags adds yet another layer of discretion. If costs involved in adopting new procedures to detect identity theft are thought to be too high, a company may choose to simply adopt the minimum procedures required by the CIP rule, thus creating an insufficient degree of identity verification for purposes of identity theft prevention.

The treatment of credit cards in the CIP rule is a good example of why the CIP rule standards ought not to be considered adequate for identity theft prevention. Under the CIP rule, credit card issuers are given a special exception, relaxing the requirement of acquiring personal information directly from customers and permitting them to obtain such information from a third party, such as a credit reporting agency. 31 C.F.R. § 103.121(b)(2)(i)(C).

Although the regulatory guidance did not explicitly state so, this exception can be explained by the nature of the CIP rule The rule was designed to aid law enforcement in locating money laundering operations. Just before the CIP rule was issued, the GAO issued a report finding that credit cards were an unlikely target for money launderers.[11]

Hence, a special exception for credit cards would be understandable in the context of money laundering prevention. It is not understandable in the context of identity theft prevention, where credit card fraud is the most common form of theft.[12] Indeed, it is the identity thief's ability to provide enough information to the credit card issuer for the issuer to access the victim's credit report -- *the very practice the CIP rule permits* -- that facilitates this form of theft. Allowing creditors to verify identity by obtaining the victim's credit report, as permitted by the CIP rule, would be to permit a practice that enables identity theft and that fails to ensure that a credit card applicant is really who the person claims to be.

Indeed, the identity verification standard should, if anything, be higher for credit card issuers. In general, at least a minimum threshold of identity verification, tailored to types of financial institutions and the specific nature of identity threat, should be included in the Red Flag guidelines. Such verification should include requiring the use of documentary identification for individuals and contacting the consumer when there are address discrepancies.

Another problem with the use of the CIP rule is the timing of red flag detection as it relates to the identity verification process. The CIP rule requires identity verification to take place "within a reasonable time after the account is opened." 31 C.F.R. § 103.121(b)(2)(ii). The proposed regulations are ambiguous as to when red flag

---

[10] *See* Supplementary Information to the Final Customer Identification Program , 68 Fed. Reg. 25,089, 25,095 ("The final attempts to strike an appropriate balance between flexibility and detailed guidance . . . .").

[11] U.S. Gen. Acct'g Office, *GAO-02-670, Money Laundering: Extent of Money Laundering Through Credit Cards Is Unknown* 15 (2002).

[12] *See* 2003 FTC Report at 34.

detection occurs; they seem to suggest that it can occur after the identity verification process. Proposed § __.90(d)(2)(i)-(ii) (listing identity verification before red flag detection). Performing identity verification after the account was already open made sense for the CIP rule for the purpose of aiding law enforcement in locating money laundering. 68 Fed. Reg. at 25,097 ("[The CIP rule] should provide appropriate resources for law enforcement to investigate money laundering and terrorist financing.").

In the context of identity theft, though, the financial institutions' role is not merely to aid law enforcement in finding identity thieves; it is to prevent those thieves from opening accounts in the first place. If a thief uses a stolen identity to obtain a loan, then the damage is done once the account is opened. If a thief acquires a credit card, the damage can be done minutes after the card is received and activated. In these cases, identity verification in a "reasonable time after the account is opened" will not prevent the damage.

The final rules should clearly state that, at least for certain "bright red flags" such as a fraud alert on a credit report, the bank should not open an account at all until a thorough investigation has taken place. They should clearly state that before an account is opened, a loan is disbursed, or a product is sold with financing, the institution must have confidence in the customer's identity sufficient to outweigh the risk and high cost of identity theft.

4. Too Much Discretion for Identity Theft Prevention Program

The Agencies' proposal adopts a flexible, risk-based approach that allows financial institutions and creditors wide latitude in adopting a Program. The proposal is applicable not only to vast numbers of regulated financial institutions, but also an estimated 3,500 financial institutions and more than 11 million creditors over which the FTC has jurisdiction.

As a general observation, the layers of discretion allowed by the proposal leave doubt as to whether Programs adopted under these vague guidelines will meet Congress' intended goal as an effective deterrent against identity theft. For example, under the proposed approach, financial institutions and creditors may elect not only which *red flags* to include in their Programs, but which *accounts* to include as well.

The red flags included in the proposal's Appendix are all indicators of identity theft. Given the many different kinds of businesses that will be subject to the final rules, some degree of flexibility is not unreasonable. However, some events are such strong indicators of identity theft that companies should not have the discretion to independently deem them irrelevant. Failure to make certain red flags a required part of a company's Program will simply lead to token Programs that do nothing to deter identity theft or help victims.

We suggest that the following events should be a required part of all Programs:

- A consumer fraud alert or active duty alert.

- Any account that would adversely affect a consumer's credit standing should be considered at risk of identity theft and thus subject to a red flag.
- An address discrepancy reported by a consumer reporting agency.
- A consumer's communication with the financial institution or creditor about attempted or actual identity theft should always be a red flag.
- A company's knowledge of a security breach within its own confines or that of an affiliate with which the company has shared customer data.
- Attempts to open a new account with altered documents.
- Suspicious actions by employees such as downloading customer account information or being added to a customer account.

The proposal states that financial institutions and creditors must have a "reasonable basis for concluding that a red flag does not evidence a risk of identity theft." (e.g. proposed FTC rule 681.2(d)(2)(ii)). However, this weak standard is impossible to enforce as a preventive measure and can only be applied *after* a company's Program is identified as deficient. The stronger standard of mandatory red flags is a more effective preventive measure.

5. Fraud Alert as a Red Flag

A fraud alert is the single most important tool consumers have to alert consumer report users that personal information has been compromised. The fraud alert is, among other things, a means of communication, a way consumers have of telling a multitude of unknown users to be on guard. Thus, a fraud alert of any duration, as well as an active duty alert, should *always* be a red flag. The Agencies should require that every Program incorporate a fraud alert or active duty alert as a red flag.

The proposal calls for every financial institution and creditor covered by the rule to adopt a risk-based Program that identifies red flags relevant to its own operation. The proposal lists a number of instances that *could* be incorporated into an entity's Program. (Sample red flags are listed in Appendix J for banking Agencies and Appendix A to Part 681 of the FTC's rules.)

A fraud alert or active duty alert is the number one red flag for both the banking and the FTC list. The proposal not only allows discretion about whether to include a fraud alert as a red flag, but incorporates leeway in deciding what actions to be taken -- assuming a fraud alert is even included as a red flag. A fraud alert should always trigger a notice requirement.

FCRA Section 605A(h) now places certain restrictions on users when a credit report includes an initial fraud alert or active duty alert (Section 605A(h)(B)). Users are required under this section to take "reasonable' steps to verify identity. Contacting the consumer seems to be one "reasonable" option, although not required. For an extended fraud alert, a user's requirements are heightened. Section 605A(h)(2)(A) requires the user, when confronted with an extended fraud alert, to contact the consumer in person, by telephone or other reasonable contact method designated by the consumer.

The Agencies should make clear that the mandatory contact required by Section 605(A)(h) is not made discretionary by this proposed rule. As the proposal now stands, companies could argue that they have the discretion not to include a fraud alert as a red flag at all.

Multiple layers of discretion included in the proposal dilute the value of a fraud alert. Even if included, the company would then have discretion about what action it *may take*. For example, under "Address the Risk of Identity Theft" (71 Fed Reg 40792), the proposal states:

> The regulations then provide an illustrative list of measures that a financial institution or creditor *may take*, including:
>
> * * * * *
>
> (H). Implementing any requirements regarding limitations on credit extensions under 15 USC 16187c-1(h) such as declining to issue an additional credit card when the financial institution or creditor detects a fraud or active duty alert associated with the opening of an account or an existing account.

We suggest an amendment to this section that references mandatory contact under Section 605A(h)(2)(A) with the consumer, at least in the case of an extended fraud alert.

We note, in addition, that the list of red flags makes no distinction between a 90-day fraud alert, active duty alert, and extended fraud alert. This permits the argument that a red flag would be applicable only as long as the initial fraud alert or active duty alert is in effect — 90 days for an initial fraud alert and 12 months for an active duty alert. A red flag prompted by a fraud alert should not be limited in this way. This is a particular concern in the case of a 90-day fraud alert.

Consumers usually initiate short-term fraud alerts as a preventive measure, when they learn their personal information has been compromised but there is uncertainty about whether the information will be misused. Events such as a lost or stolen wallet or notice of a data security breach often prompt consumers to place a short-term fraud alert. After the initial 90 days, consumers can either extend the alert for another 90 days or, if they learn they've become a victim of fraud, file an extended fraud alert along with a police report.

The final rules should specify that a red flag prompted by a fraud alert or active duty alert is not limited to the time the alert is in effect. If the consumer report user has knowledge of a prior alert, it should continue to act as though the alert were in effect for at least a year. Identity thieves, especially those involving savvy organized efforts, may not act to commit fraud soon after information is compromised. A hacker, for example, is likely to know when a target institution is required to give a security breach notice to affected individuals and knows as well that a security breach notice often includes instructions on how to file a short-term fraud alert.

A solid Program will alert the consumer even after an initial fraud alert has expired.

6. Additional Red Flags Suggested

The Agencies have solicited comments on whether the proposed red flags listed in the Appendix are too specific or not specific enough and whether additional red flags should be included.

The red flags listed in the proposal include numerous signals that, if included in a Program and effectively implemented, should work to prevent or mitigate the harm to consumers. The red flags listed in the proposal are not too specific. Instead, given the degree of discretion included in the proposal, ample examples are needed to give financial institutions and creditors notice about what the Agencies consider should be included in a Program. We are at a loss to see why a responsible company, even with the proposal's built-in discretion, would choose not to include as a minimum most of the red flags enumerated by the proposed rule.

The following are suggested as additional red flags:

- Notice from the customer or others that a credit or debit card has been lost or stolen.
- Notice that the consumer's information may have been lost or stolen through a data security breach.
- An address discrepancy on a credit application sent by a consumer in response to a company's solicitation generated by credit report prescreening or other marketing lists.
- Alerts distributed by government, trade associations, or media reports about recent trends in identity theft.
- A creditor or financial institution learns that its business identity has been fraudulently used to obtain personal information, such as in phishing schemes.

7. Inactive Accounts

Congress directed the Agencies to consider whether to include guidelines for notifying a customer when a transaction occurs in an account that has been inactive for two years. The proposal treats activity in an account as a red flag but does not include guidelines on when a customer should be notified. In addition, the red flag replaces the two-year period with a "reasonably lengthy period of time."

This is the wrong approach. First, the "reasonable" standard again allows excessive discretion about what signals unauthorized use in an inactive account. The final rules should at least retain the two-year period as a minimum. More troubling about the Agencies' approach is that it bypasses the need to give consumers notice or otherwise confirm with the consumer that activity in a dormant account is legitimate.

The first line of defense against identity theft is always for the financial institution or creditor to contact the consumer. It is not at all unusual for accounts to become inactive as consumers open new accounts but fail to formally close accounts they no longer intend to use. Inactive accounts, especially for consumers who have a high credit rating, are often tied to an approved line of credit. Renewed activity in such an account should require contact with the consumer. A red flag alone, which the creditor is free to consider relevant or not, is inadequate for inactive accounts.

8. Service Providers

The proposal allows a service provider that services multiple financial institutions or creditors to adopt its own Program. Thus, under the proposal, service providers would not need to incorporate the already discretionary Program adopted by its sponsor financial institution or creditor. This is the wrong result.

If a financial institution or creditor determines, from its risk-based analysis, that a red flag should be incorporated into its own Program, then that risk-based item should in turn be incorporated into service provider Programs. Final regulations should require service providers that service multiple entities to adopt a Program which incorporates all the red flag indicators recognized by its sponsor entity as an identity theft risk.

9. Change of Address Requests and Requests for Replacement Cards

The FCRA requires the Agencies to adopt regulations requiring credit and debit card issuers to assess the validity of address changes followed shortly by a request for an additional or replacement card. The statute sets a minimum of 30 days for a card issuer to assess the validity of an address change when followed by a request for a new or replacement card.

The proposed regulation offers card issuers three options for validating a change of address under these circumstances. The card issuer may:

- Notify the cardholder at the former address,
- Notify the cardholder by a means previously agreed upon, or
- Use other means of assessing the validity of the change of address.

The last choice for validating an address is vague. The Agencies should elaborate further on what is meant by "other means" and give examples of what "other means" would be acceptable. The Agencies should also give preference to verifying an address in ways that involve direct contact with the cardholder. An address change followed by a request for a replacement card is such a strong indicator of identity theft that verification directly with the cardholder is nearly always called for.

Final regulations should also set a period longer than the 30-day minimum. Requesting additional replacement cards soon after a change of address is a method of the "quick-strike thief." This identity theft variation, account takeover, is most effective when the

thief is able to effect a change of address and then obtain a new card before the victim realizes that the usual account statement has not appeared in the mail. Depending on the card issuer's billing cycle, a consumer may not detect a problem within 30 days.

When an address change is tied to a request to issue a new card, the card issuer should be on alert for at least 90 days. Identity thieves, especially those involved in an organized endeavor, are well aware of the rules. The longer a thief must wait to use a victim's information in an account takeover scheme, the less valuable that information becomes because the more likely the potential victim is to realize information has been compromised.

10. Address Discrepancy Reported by a Consumer Reporting Agency

Consumer Reporting Agencies (CRAs) under the FCRA must provide notice of address discrepancy if "substantially" different from the address a user provides when requesting a credit report. Users must, in turn, form a "reasonable belief" that the identity of the person is known for whom the credit report was obtained and take steps to reconcile the address of the consumer with the CRA. The latter is required *only* if the user establishes a continuing relationship with the consumer and regularly and in the ordinary course of business furnishes information to the CRA.

The proposal allows users to form a "reasonable belief" that it knows the identity of the consumer by following the CIP rules. As discussed in Part 3 above, the reasons for identifying a person for purposes of the CIP rules are quite different from reasonably concluding that a person is not an identity thief. The types of accounts favored by terrorists or money launderers are not the types of accounts favored by identity thieves. A prime example of this is an "instant credit" situation where credit cards are offered at point of sale.

Retail credit card offers are routinely extended to any person who makes a purchase. Identity theft thrives in this easygoing atmosphere where every customer who goes through the check-out line is a candidate for a credit card. Such accounts are unlikely to have a connection to terrorism, so the CIP rules require very little identity verification.

The CIP allows the creditor:

> …broader latitude to obtain some information from the customer opening a credit card account, and the remaining information from a third party source, such as a credit reporting agency, prior to extending credit to a customer.
> www.treas.gov/press/releases/reports/326finalbanks.pdf

This makes no sense in the context of verifying identity when a CRA sends a user notice of an address discrepancy. This means a creditor could form a "reasonable belief" about the identity of the customer for whom the consumer report applies simply by obtaining information from the person opening the account -- even if an identity thief -- and then

obtaining information from a third party source such as CRA, which may include inaccurate address information. The CIP rules place no obligation on a creditor to reconcile address discrepancies.

Moreover, the CIP rules do not even require identity verification *before* an account is opened. Rather, an account may be opened and the person's "true" identity verified "within a reasonable period of time after the account has been opened." The Agencies' proposal adopts this standard for identity theft Programs, with the only added requirement that identity be verified during the period the creditor reports to the CRA, usually 30 days.

The threat to consumers from this approach is obvious. A thief with newly found personal information about a victim, for example, from hacking, phishing, mail theft or some other source, could quickly open multiple accounts in the victim's name. Even with an address discrepancy on file with a CRA, accounts could be opened without verifying identity during the user's reporting cycle to the CRA. In the time it takes to verify identity after an account is opened, the victim's credit standing could be ruined.

The Agencies, regrettably on this point, strongly favor business interests over interests of consumers. We respectfully suggest that this is the wrong approach and is contrary to the interests of potential and actual victims, those Congress intended to be served by an Identity Theft Prevention Program. The CIP rule, which allows accounts to be opened before identity is verified, is not the proper standard for an Identity Theft Prevention Program. The CIP has been in effect for over three years, and there is no evidence to suggest the rule has, as a byproduct, reduced new account identity fraud.

If properly implemented, the address discrepancy provision could help reduce new account fraud, a most menacing form of identity theft, one that takes victims longer to detect and longer to recover from. New accounts opened in a victim's name often involve not only that single account, but situations where the thief has assumed the victim's entire identity and has opened or attempted to open several accounts.

An address discrepancy also demands a higher standard of communication, both with the CRA and the consumer. The consumer may never know that someone attempted to open an account using his or her name and other identifying information while changing an address. The thief could then simply go to another institution where he or she might be more successful. A responsible Program, whether strictly required by the statute or not, should include notice to the consumer in addition to a report to the CRA.

11. Employee Training and Oversight

The Agencies are correct to include certain employee actions as red flags. Certainly, an employee who is added to a customer's account or an employee who downloads an unusually large number of customer account records is cause for scrutiny. Insiders have a unique opportunity to obtain customer data for illegal purposes. All too many instances of insiders working with thieves have been reported.

Employee training should be more specifically described in the final version of the guidelines. Some steps necessary to detect identity theft require very specific training. The ability to detect altered identity documents is, for example, a highly skilled endeavor. The training required should, therefore, be commensurate with the company's identified red flags Program.

Companies should also be required to create incentives for employees who are successful at recognizing an attempt at fraud and in mitigating the burdens of victims. Employees who work on commission or are otherwise rewarded for opening new accounts stand to lose a part of their income by *not* opening new accounts. This creates an inherent conflict. Employees who otherwise profit from opening new accounts should not be penalized for being alert to the prospect of identity theft.

12. Measure of Effectiveness

Under the proposal, annual reports are required to the board of directors or senior staff. Reports must include, among other things, discussion of the effectiveness of the Program, the procedures, significant incidents involving identity theft, and management's response and recommendations for changes in the Program.

Reports such as described by the proposal are needed for a company to evaluate its experience with identity theft and measures to improve. However, there is nothing to require that reports go beyond the walls of the financial institution or creditor, or that the creditor follow up with changes to prevent identity theft. This leads to the real prospect that important information about identity theft will end up to be no more than another administrative function.

To effectively address identity theft, such reports should be more than stagnant pages filed away year after year. There should be requirements that creditors adjust their Identity Theft Prevention Programs to address deficiencies raised by the annual reports.

An effective measure of identity theft prevention requires that information be available within business sectors, across industry lines and by regulators. Government regulators should collect at least aggregate data and make that data available to the public. Consumers need information about the effectiveness of creditor identity theft Programs in order to take preventive measures and so that they can make informed decisions about their choice of financial institutions.

13. Compliance Date

We urge the Agencies to move forward quickly to adopt meaningful rules and guidelines to address the identity theft epidemic in this country. The effective date for compliance should be the minimum time allowed by law. Financial institutions and others that extend credit to millions of consumers every day have been on notice since FACTA's adoption three years ago.

We readily acknowledge that some companies are now doing more to stop identity theft early and alert customers to unusual account activity. However, as long as identity theft victims number in the millions with billions of dollars lost to fraud each year, creditors and the financial services industry need to do more. Until effective solutions are firmly in place, victims will continue to bear the brunt of this crime.

14. Conclusion

We offer these comments on behalf of millions of identity theft victims and potentially many more who, statistics show, will be affected in the coming years. The Agencies should reconsider the proposal and eliminate many layers of discretion. Given the great number of financial institutions and creditors covered by the proposed rules, vague and weak standards such as those included in the proposal will be impossible to enforce. The only reasonable solution to the identity theft crisis is for Agencies to adopt stringent regulations that leave no doubt as to the steps companies must take.

We appreciate the opportunity to comment.

Sincerely,

Tena Friery, Research Director
Beth Givens, Director
Privacy Rights Clearinghouse
3100 5th Ave. #B
San Diego, CA 92103
(619) 298-3396
www.privacyrights.org

Joined by:

Linda Sherry, Director, National Priorities
Consumer Action
P.O. Box 1762
Washington, DC 20013
(202) 544-3088
www.consumer-action.org

Chi Chi Wu, Staff Attorney
National Consumer Law Center
Boston, MA 02110
(617) 542-8010
www.consumerlaw.org

Deborah S. Pierce, Executive Director
PrivacyActivism

(415) 386-9351
www.privacyactivism.org

Ed Mierzwinski, Consumer Program Director
U.S. Public Interest Research Group (U.S. PIRG)
218 D St. SE
Washington, DC 20003
(202) 546-9707
Washington, D.C. 20003
www.uspirg.org

Pam Dixon, Director
World Privacy Forum
Cardiff by the Sea, CA 92007
(760) 436-2489
www.worldprivacyforum.org

Consumer Action is a nonprofit consumer education and advocacy organization known for its free multilingual consumer education materials. It was established in 1971 and provides consumers with information on matters of telecommunications, privacy, predatory lending, and banking/credit issues. Consumer Action advocates at the state and federal legislative levels for consumer rights. www.consumer-action.org

National Consumer Law Center (NCLC) is a nonprofit organization specializing in consumer law issues on behalf of low-income people. NCLC works with thousands of legal services, government and private attorneys, as well as organizations, who represent low-income and elderly individuals on consumer issues. NCLC joins these comments on behalf of the Center's low-income clients. www.nclc.org

Privacy Activism is a California nonprofit educational organization that works on behalf of consumer privacy issues. Our particular area of interest is information privacy and the collection and use of personal information in government and commercial databases. www.privacyactivism.org

The Privacy Rights Clearinghouse is a nonprofit consumer education and advocacy organization based in San Diego, CA, established in 1992. It offers assistance and information to consumers on a wide range of informational privacy issues. And it represents consumers' interests in public policy proceedings at the state and national levels. www.privacyrights.org

U.S. Public Interest Research Group (USPIRG) serves both as the non-partisan, nonprofit association of and federal research and advocacy office for the state PIRGs, which have over one million members around the nation. U.S. PIRG and the state PIRGs have published over one dozen research reports on credit bureau accuracy or identity theft since 1991. www.uspirg.org

The World Privacy Forum is a nonprofit, non partisan 501(c)(3) public interest research group. The organization conducts in-depth research and consumer education in the area of privacy. It investigates a broad range of emerging and maturing issues, including consumer data privacy, workplace privacy, identity issues, medical and financial privacy, and large technological infrastructures, including databases. www.worldprivacyforum.org