Wells Fargo & Company
420 Montgomery Street
San Francisco, CA 94104

September 18, 2006

Office of the Comptroller of the Currency
250 E Street, SW.
Public Reference Room Mail Stop 1-5
Washington, DC 20219
regs.comments@occ.treas.gov

Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, DC 20551
regs.comments@federalreserve.gov

Robert E. Feldman, Executive Secretary
Attn: Comments, Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Comments@FDIC.gov

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

Mary F. Rupp, Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, Virginia 22314-3428
regcomments@ncua.gov

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

Re: Red Flags Rule
OCC Docket Number 06-07; Regulatory Information Number (RIN) 1557-AC87
Federal Reserve System Docket No. R-1255
FDIC RIN 3064-AD00
OTS No. 2006-19; RIN 1550-AC04
FTC RIN 3084-AA94
Wells Fargo & Company Comments on joint proposed rule regarding Identity Theft Red Flags and Address Discrepancies under Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA)

Dear Sirs and Madams:

This letter is submitted on behalf of Wells Fargo & Company and its affiliates ("Wells Fargo") in response to the joint proposed rule regarding Identity Theft Red Flags and Address

Discrepancies under Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), published in the Federal Register on July 18, 2006 at 71 FR 40786 (the "Proposed Rule" or "Rule"). Wells Fargo appreciates the opportunity to comment and encourages the OCC and the other joint drafters of the Proposed Rule (the "Agencies") to consider adopting the suggestions set forth herein.

This letter will begin with general comments about the need for the Proposed Rule to allow for greater flexibility in implementing Sections 114 and 315 of FACTA, and how in several respects, the Proposed Rule goes beyond the intent and requirements of the statute. Following the general comments, this letter will address specific comments pertaining to Address Discrepancies, the Identity Theft Prevention Program, the Red Flag Guidelines outlined in Appendix J, and the duties of Card Issuers regarding Changes of Address.

General Comments

Greater Flexibility Needed

The Proposed Rule needs to permit greater flexibility in implementing sections 114 and 315 of FACTA so that financial institutions, such as Wells Fargo, can more effectively achieve these sections' goal of preventing and mitigating identity theft. We support this objective and have historically made fighting fraud and identity theft a top priority. Identity theft negatively impacts financial institutions in the form of poor public perception and reputation risk, customer dissatisfaction, and the costs of absorbing the losses associated with the identity theft or fraud.[1] Long before the passage of the FACT Act, Wells Fargo had developed and implemented sophisticated procedures designed to help combat identity theft and fraud. In order to enable Wells Fargo and others to successfully continue their fight against fraud and identity theft, the final rule must truly be risk-based and provide institutions with broad discretion and flexibility to effectively respond to ever-changing threats.

We respectfully submit that the current Proposed Rule is too restrictive with respect to how it requires financial institutions to implement an Identity Theft Prevention Program ("Program") and mandates expensive changes which ultimately will do little to help mitigate and prevent identity theft. Wells Fargo strongly supports the prevention and mitigation of identity theft and allocating the necessary resources for achieving that goal; but the anticipated costs associated with implementing the Proposed Rule are disproportionately excessive when compared with the marginal benefit that would be achieved in preventing identity theft. As just one illustration of this, at least six of the 31 Red Flags listed in Appendix J fixate on address differences for the same individual without any practical recognition that large numbers of individuals, routinely and appropriately, provide and use multiple addresses (e.g., winter and summer homes; the address of a joint accountholder for one account and his or her own address for another account; a business address for an individual's small business and a personal address for his or her personal accounts; etc.); yet the Proposed Rule would require a financial institution to ***detect*** any of these address issues as a red flag and then ***justify*** a "reasonable basis for concluding that [such] Red Flag does not evidence identity theft." Section __.90(d)(2)(iii).

[1] House Report 108-263 on H.R. 2622, page 25: acknowledging that the financial institution generally absorbs the financial losses from an identity theft.

While we have no objection to expending appropriate resources to achieve the goals of the Proposed Rule, we encourage greater flexibility under the Rule for allocating those resources as we deem most effective, based on the examples set forth in the Rule and our own years of experience in combating identity theft and fraud.[2] The Proposed Rule should be amended as suggested herein in order to allow financial institutions the freedom to implement measures they know will better achieve the identity theft mitigation and prevention goals of FACTA. Greater flexibility is also consistent with the legislative history relative to the Red Flags Guidelines and Regulations.[3]

Parts of Proposed Rule Go Beyond Requirements and Intention of FACTA

There are several parts of the Proposed Rule that go beyond the intentions and purposes of Sections 114 and 315, and are simply not supported by the statute or its legislative history. For example, as will be discussed in more detail later, the proposed definitions of "Account" and "Customer" in Sections __.90(b)(1) and (b)(3) would include accounts of small business entities, contrary to the purpose of the statute to protect consumers. In addition, although financial institutions, consumer reporting agencies, and consumers should all have a responsibility to take reasonable steps to help mitigate and prevent identity theft, several parts of the Proposed Rule would place a disproportionate share of this burden on the financial institutions. This is neither supported by the legislative history or language of FACTA, nor effective in combating identity theft.[4]

Estimated Burden for Compliance is Unrealistic and Inaccurate

The Agencies' projections regarding the amount of time and resources it would take institutions to comply with the Proposed Rule are substantially underestimated and unrealistic. Although financial institutions such as Wells Fargo have robust fraud and identity theft prevention systems in place today, these new requirements proposed by the Rule would demand a significant commitment of time and financial resources before attaining compliance. Among other things, these proposed regulations would require: (1) establishing, implementing, and maintaining a comprehensive, risk-based identity theft prevention program which includes: (2) reconciling notices of address discrepancies and reporting addresses back to the consumer reporting agencies with regard to an institution's existing accounts; (3) training employees for that program; (4) involving the board of directors and senior management in the approval,

---

[2] Senate Report 108-166 on S. 1753, page 13: "The Committee believes that the [Agencies] are equipped to establish broad parameters for such guidelines, but that individual institutions are in the best position to determine how best to develop and implement the required policies and procedures."

[3] Senate Report 108-166 on S. 1753, page 13: "The Committee intends for the guidelines to provide flexibility to institutions given the changing nature of identity theft and related crimes."

[4] To the contrary, the legislative history acknowledges that all parties have a responsibility in combating identity theft: "the 'Fair and Accurate Transaction Act of 2003,' provides consumers with the tools they need to fight identity theft . . ." "[FACTA] enlists financial institutions' support in fighting identity theft by requiring them to develop procedures to 'red flag' identity theft . . ." House Report 108-263 on H.R. 2622, page 22 – purpose and summary.

implementation, and maintenance of the program, including providing annual reports thereto; (5) overseeing service providers; and (6) validating changes of address. Wells Fargo strongly urges the Agencies to understand what a significant undertaking it will be to become compliant with the final rule and appreciate the considerable resources that would be necessary. Regardless of the form and content of the final rule, it is critical that the Agencies provide for at least eighteen months from the effective date of the final rule to attain compliance.

Subpart I – Duties of users of Consumer Reports Regarding Address Discrepancies and Records Disposal

Section __.82 – Duties of users regarding address discrepancies

Proposed § __.82(c) implements the requirement in section 315 that the Agencies prescribe regulations describing reasonable policies and procedures that will enable the user of a consumer report ("user") to form a reasonable belief that the user knows "the identity of the person to whom the consumer report pertains" when the user receives a notice of address discrepancy. It further provides that a user must develop and implement reasonable policies and procedures for "verifying the identity of the consumer for whom it has obtained a consumer report" whenever it receives a notice of address discrepancy. A "notice of address discrepancy" is defined as "a notice sent to a user of a consumer report by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer." In addition, proposed § __.82(d)(1) provides that a user must develop and implement reasonable policies and procedures for furnishing to the CRA, from whom it received a notice of address discrepancy, an address for the consumer that the user has reasonably confirmed is accurate when certain conditions are satisfied.

The Proposed Rule goes beyond what is required by the statute with respect to the duty of a user to verify the identity of the consumer and furnish a reconciled / confirmed address back to the consumer reporting agency, when a notice of address discrepancy is received. In particular, the Rule attempts to expand the circumstances under which a user would be required to furnish an address back to a consumer reporting agency to include existing relationships, by adding the word "maintains." We urge the Agencies to delete the word "maintains" from § __.82(d)(1)(ii) of the Proposed Rule so that it is consistent with the requirements of the statute, and to clarify that the duty to verify the identity of the consumer and furnish a reconciled / confirmed address is limited to newly established relationships only, and not existing relationships.

Section 605(h)(1) of the FCRA makes no reference to applying to existing accounts. Moreover, section 605(h)(2)(B)(ii) provides that the regulations implementing this part shall describe reasonable policies and procedures for use by a user, "if the user *establishes* a continuing relationship with the consumer . . ." (Emphasis added). By contrast, § __.82(d)(1)(ii) of the Proposed Rule provides that a user would have a duty to furnish an address back to a consumer reporting agency when the user "establishes or *maintains* a continuing relationship with the consumer." (Emphasis added). This would result in a user having to furnish an address back to a consumer reporting agency on *existing* accounts, which is not supported by the

language of Section 315. By only stating that "*if* the user establishes a *continuing* relationship with the consumer," Congress clearly was referring to a relationship that was not yet established or continuing. The intent of the statute was to limit this requirement to newly established relationships only, and not to apply it to *existing* relationships. On existing relationships, financial institutions have already verified the identity of the consumer at the time the relationship was established and therefore, imposing additional requirements would be of little value and overly burdensome. Accordingly, the addition of the word "maintains" to the Proposed Rule is not supported by the intent and plain language of the statute, and Wells Fargo strongly encourages the Agencies to delete it and to limit this rule to new relationships only.

In order for the Proposed Rule to make clear that existing relationships are excluded from the obligation to verify the identity of the consumer and reconcile / confirm the consumer's address before furnishing an address back to a consumer reporting agency when an notice of address discrepancy is received (as contemplated by the statute), we strongly encourage the Agencies to not only remove the word "maintains" from the Proposed Rule, but also to add a specific carve-out for existing relationships. A specific carve-out to exclude existing relationships would remove any ambiguity about a user's duties when a notice of address discrepancy is received. More importantly, such a carve-out would help reduce the millions of "false positive" notices of address discrepancy received by users from consumer reporting agencies, which currently overwhelm users and do little to actually help mitigate or prevent identity theft.

If the Proposed Rule expands the statute to include existing relationships, it would impose a substantial burden on Wells Fargo and other financial institutions which request consumer reports on existing relationships for reviewing those accounts with little, if any, corresponding benefit either to consumers or to financial institutions. In such cases, Wells Fargo is not ordering a "full" consumer report and therefore is typically not even receiving back from the consumer reporting agency the address it has on file for the consumer; only a notice that an "address discrepancy" exists. Financial institutions routinely request limited credit report information (e.g. just FICO scores and major derogatory credit indicators) on hundreds of millions of their existing credit accounts on a monthly or quarterly basis. To assure the best possible match with each request, the consumer reporting agencies require creditors to provide the names, ***addresses***, and SSN's of their accountholders with these requests. Today, when the agencies provide this limited credit report information to the user for these tens of millions of accountholders, it is accompanied with hundreds of thousands or more of address discrepancy indicators. (Our experience shows that our current address for these accountholders is, overwhelmingly, a correct one.)

A major shortcoming of the current obligation of a consumer reporting agency to issue a notice of address discrepancy is that there is no downside to the consumer reporting agency for taking an overly conservative approach and issuing notices of address discrepancy even where there is uncertainty as to whether or not a "substantial difference" actually exists. Wells Fargo's own experience, since consumer reporting agencies started issuing notices of address discrepancy, has taught it that such notices are rarely indicative of, or helpful in preventing, identity theft or fraud. Since the inception of the notice of address discrepancy reporting requirement, some Wells Fargo lines of business have reported receiving notices of address

discrepancy on as many as fifty-percent of the consumer reports requested. The percentage of notices received is even higher on business purpose relationships, where a consumer report is often requested, with the business address, on the principals of the business. Moreover, in an overwhelming number of cases where Wells Fargo receives a notice of address discrepancy, experience has demonstrated Wells Fargo has the correct address for the consumer. There is also no obligation on the consumer reporting agencies to update their records with the reconciled address reported back to it by the user. This could result in a perpetual loop where the consumer reporting agencies continue to issue notices of address discrepancy where a substantial difference does not necessarily exist and on addresses which users have already reconciled and furnished back to the consumer reporting agencies. This will create unnecessary burdens on users to verify the identity of the consumer and furnish the address back to the consumer reporting agency.

In addition, Wells Fargo encourages the Agencies to consider adding a "safe harbor" provision which would protect user's from private rights of action under Sections 616 and 617. Section 615(h)(7) bars private rights of action with respect to any of the duties required by that section, which includes the Red Flag regulations and guidelines. However, the protection does not extend to the address discrepancy requirements. Without a safe harbor provision, users of consumer reports could become targets of private rights of action looking to blame a user every time there is an occurrence of identity theft, or to capitalize on technical violations of the address discrepancy requirements. Accordingly, we strongly recommend the Agencies provide for a safe harbor provision similar to that set forth in section 615(h)(7) of the FCRA, and limit enforcement to the respective Agencies.

Subpart J – Identity Theft Red Flags

Section __.90 – Duties regarding the detection, prevention, and mitigation of identity theft

§ __.90(b)(1) Definition of "Account"

In response to the Agencies request for comment on the scope of the definitions of "Account," Wells Fargo respectfully submits that this definition is too broad and not what was intended or contemplated by the FACTA. In particular, the definition of "Account" should specifically exclude any reference to business purpose accounts or accounts that are not "continuing."

The Agencies propose defining "Account" to mean "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 a financial activity under section 4(k) of the Bank Holding Company Act, 12 U.S.C. 1843(k)." However, the Proposed Rule goes on to give examples of accounts by providing that "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; and (ii) A demand deposit, savings or other asset account for personal, family, household, or *business purposes*, such as a checking or savings account." (Emphasis added).

By including accounts for "business purposes," the proposed definition has exceeded the scope of what was intended by the statute. There is nothing in the statute itself or its legislative history to indicate that Congress intended for Section 114 to apply to business purpose accounts. To the contrary, the legislative history clearly states that the intent of the FACTA, and the FCRA in general, was to protect *consumers*. For example, in describing the "purpose and summary" of the FACTA legislation, the legislative history provides that FACTA "provides *consumers* with the tools they need to fight identity theft . . ." (Emphasis added). It also describes the FCRA in general as "landmark *consumer* protection legislation enacted in 1970 . . . ." In addition, it describes the risks of identity theft by observing that "While American *consumers* have realized undeniable benefits from the free flow of credit reporting information . . . [*consumers*] have also become increasingly concerned abut the risk of their personal financial information falling into the wrong hands." (Emphasis added). The purpose and summary section of the legislative history further recognizes that the FACTA bill "contains numerous measures which protect *consumers* from identity thieves" and that "the bill directs [the Agencies] to develop identity theft 'red flag' guidelines . . . to help protect *consumers*." (Emphasis added).

The risk of identity theft in business banking relationships is extremely low. This is due in large part to the in-person manner in which most business banking relationships are initiated. In Wells Fargo's experience, a majority of the business banking accounts are opened in a face-to-face environment, so the banker usually has personal interaction and familiarity with the business customer. Wells Fargo business bankers reported that identity theft for businesses was virtually nonexistent. Rather, businesses are more prone to internal fraud from an individual within their own organization; not the type of identity theft experienced by consumers which the FACTA aims to prevent. Although identity theft is possible for small business and may occur in isolated situations, protecting businesses or business purpose accounts from identity theft is beyond the purpose and intent of the FACTA. Accordingly, we urge the Agencies to redefine "Account" to be consistent with the intent and purpose of the FCRA and FACTA, by eliminating any reference or example to a "business purpose" account.

As an alternative to eliminating "business purpose" from the examples of accounts, we strongly urge the Agencies to consider limiting the scope of the definition of "Account" to small businesses. If business purpose accounts must be included in the definition, we would suggest adopting a definition that includes small businesses only, defined by those that had gross revenues of one-million or less in their preceding fiscal year, similar to the language utilized by Regulation B at 12 CFR § 202.9(a)(3). It is not appropriate to attempt to regulate identity theft risks for business purpose accounts in these Red Flag regulations and guidelines.

§ __.90(b)(3) Definition of "Customer"

The Proposed Rule defines a "Customer" as "a person that has an account with a financial institution or creditor." The definition of "Customer" should replace "person" with "consumer" to clarify that a Customer does not include a business purpose account or relationship.

The FCRA's definition of "person" includes non-individuals such as partnerships and corporations. As a result, the Proposed Rule's definition of "Customer" will necessarily include business purpose accounts, which is not mandated by the statute. The Agencies acknowledge in the Supplementary Information that they chose this broad definition because, in addition to individuals, various types of entities, such as small businesses, can be victims of identity theft. As previously discussed, although it is possible small businesses could be subject to identity theft, it is not very likely or as prevalent compared with individual consumers. More importantly, however, the protection of small businesses (or any other non-consumers) from identity theft is simply not contemplated by the FACTA and beyond its scope and intent. Accordingly, we strongly urge the Agencies to change the definition of "Customer" to "a consumer that has an account with a financial institution or creditor." Alternatively, we urge the Agencies to consider limiting the scope of this definition to small businesses, as described above in the definition of "Account."

§ __.90(b)(4) Definition of "Identity Theft"

The Proposed Rule ascribes the same meaning to "Identity Theft" as the FTC defined that term in 16 C.F.R. § 603.2(a), which is "a fraud committed or attempted using the identifying information of another person without authority." The FTC's definition was issued pursuant to its authority under 603(q)(3) of the FCRA to further define that term. Because that definition was based on the original FCRA definition[5] in the context of definitions relating to *fraud alerts* only, it is not appropriate to borrow the FTC's definition of Identity Theft to use in the context of the Red Flag regulations. This definition uses the term "person," which the FCRA defines to include non-individuals and consumers, and thus it would include frauds committed or attempted using the information of other businesses. Using the FTC's definition of Identity Theft in the context of the Red Flag regulations is inappropriate and beyond what was contemplated or intended by FACTA. Accordingly, that term should be redefined to exclude non-consumers and attempted thefts of identity.

The definition of Identity Theft should be limited to frauds committed using the identifying information of another consumer and specifically exclude businesses. For the reasons more fully described above regarding the definitions of "Account" and "Customer," expanding the definition of Identity Theft to include businesses would be inconsistent with the purpose and scope of the FACTA. Although the definition uses the term "person," which would therefore include non-individuals, its definition of "identifying information" ironically already implies it is limited to individuals only. Specifically, the examples the definition provides of "identifying information," such as name, social security number, date of birth, or biometric data like fingerprints, voice prints, or retina images, are all characteristics that are particular to an actual individual person and which a business entity would not possess.

In addition, the definition of Identity Theft should be limited to actual instances of fraud committed using the identifying information of another consumer, and exclude any references to "attempted" fraud. Measures to combat Identity Theft should be aimed at preventing actual occurrences. Expanding the definition to include mere ***attempts*** creates logical contradictions

[5] Section 603(q)(3)

with burdensome and ineffective implications for the identity theft prevention programs of financial institutions by requiring them to devote resources to false leads thus distracting resources and attention from ***actual*** instances of identity theft. Furthermore, a broad definition to include attempted identity theft is also unnecessary because such attempts and precursors to identity theft are already addressed by a financial institution's Identity Theft Program and the requirements under the Proposed Rule. For instance, Section __.90(c) would require the Program to include reasonable policies and procedures to address the *risk of identity theft* to its customers. Section __.90(d)(1)(i) would further mandate that the Program include policies and procedures to identify Red Flags that are relevant to detecting the *possible risk of identity theft* to customers.

It is noteworthy that the proposed definition of "Red Flag" includes a "*possible risk* of identity theft," the proposed meaning of "Identity Theft" contemplates "attempts" at identity theft, and Section __.90(d)(1)(i) of the Proposed Rule provides that a "Program must include policies and procedures to identify **Red Flags** . . . that are relevant to detecting a possible risk of **identity theft** to customers." Substituting the terms "Red Flag" and "Identity Theft" with their actual proposed definitions would require the Program to "include policies and procedures to identify **possible risks of identity theft** [Red Flag definition] that are relevant to detecting a possible risk of **a fraud committed or attempted using the identifying information of another person without authority** [Identity Theft definition]." If the definition of "Identity Theft" is substituted again for the reference to "Identity Theft" in the "Red Flag" definition in the previous sentence, then Section __.90(d)(1)(i) would require an Identity Theft Program to "include policies and procedures to identify a pattern, practice, or specific activity that indicates the possible risk of a fraud committed or attempted using the identifying information of another person without authority that is relevant to detecting a possible risk of a fraud committed or attempted using the identifying information of another person without authority." When the actual proposed definitions are substituted, it would apparently require a Program to have policies and procedures to identify "*possible* risks of fraud that are relevant to detecting *possible* risks of fraud," which would effectively include virtually any type of event or transaction. This would certainly weigh down a financial institution's ability to detect and analyze legitimate instances or risks of identity theft, and effectively render the Identify Theft Program meaningless. Clearly, if the proposed definitions of "Red Flag" and "Identity Theft" are retained, complying with the requirements of Section __.90(d)(1)(i), as described in the previous sentence, would be unworkable. For all of the foregoing reasons, a separate definition should be issued for Identity Theft that is particular to the context and appropriateness of the Red Flag regulations, and which excludes references to businesses or attempted identity theft.

§ __.90(b)(5) Definition of "Red Flag"

The proposed definition for "Red Flag" is "a pattern, practice, or specific activity that indicates the possible risk of identity theft." The Agencies have requested comment on the scope of the definition of "Red Flag" and specifically, whether the definition of "Red Flag" should include precursors to identity theft. Wells Fargo strongly urges the Agencies to qualify this definition to read "*significant* risk of identity theft" or alternatively "*material* risk of identity theft."

Including "possible" risks within the definition of "Red Flags" would unnecessarily cause institutions to expend valuable resources chasing false positives and insignificant risks, reducing their ability to effectively combat real identify theft risks. In addition, using the term "*possible* risk" in the Red Flag definition would result in an awkward and redundant obligation under § __.90(d)(1)(i) to establish a Program which identifies "possible risks" (e.g. "Red Flags") that are relevant to detecting a "possible risk" of identity theft. Furthermore, the requirements of Section 114 of the FACTA (§ 615(e)(1)(B) of the FCRA) to prescribe regulations requiring each financial institution and creditor to establish policies and procedures to identify *possible risks* are already addressed in Section __.90(d)(1)(i) of the Proposed Rule.

Section 615(e)(1)(B) of the FCRA directs the Agencies to "prescribe *regulations* requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing the guidelines . . . to identify *possible risks* to account holders or customers . . ." (Emphasis added). The Agencies have achieved this directive in § __.90(d)(1)(i) which provides that the Identity Theft Prevention Program required by § __.90(c) "must include policies and procedures to identify Red Flags . . . that are relevant to detecting a *possible risk* of identity theft to customers or to the safety and soundness of the financial institution or creditor." (Emphasis added).

In the Supplementary Information, the Agencies state that the proposed definition of Red Flag is based on the statutory language and that it is intentionally expansive to include precursors to identity theft which indicate a "possible risk" of identity theft. The Agencies are correct in their attempt to implement the requirements of § 615(e)(1)(B), which says the regulations should identify "possible risks" to account holders or customers. However, using the term "possible risk" in the definition of "Red Flag" is unnecessary, because § __.90(d)(1)(i) of the Proposed Rule, which provides that the Identity Theft Program "must include policies and procedures to identify Red Flags . . . that are relevant to detecting a *possible risk* of identity theft to customers," already addresses these requirements.

Using the term "possible risk" in § __.90(d)(1)(i), properly implements the requirements of the statute to "prescribe *regulations* requiring [the establishment of] reasonable policies and procedures for implementing the guidelines . . . to identify *possible risks* to account holders or customers . . ." However, by also using the term "possible risk" in the definition of "Red Flag," and by using the term "Red Flag" in § __.90(d)(1)(i), it dilutes the meaning of that term and results in a redundant requirement under § __.90(d)(1)(i) to establish a Program which identifies "*possible risks*" that are relevant to detecting a "*possible risk*" of identity theft. In addition to including the phrases "Red Flag" and "possible risk," § __.90(d)(1)(i) is even further complicated by the inclusion of the term "Identity Theft" which is described as "a fraud committed or attempted" (discussed in more detail under the section on the definition of Identity Theft).

Using "possible risk" in the definition of Red Flag results in an unworkable obligation under § __.90(d)(1)(i) and will overly burden financial institutions with false leads and distract resources and attention from actual instances of identity theft. Therefore, we strongly urge the Agencies to change the definition of "Red Flag" to "a pattern, practice, or specific activity that indicates a significant risk of identity theft" or ". . . a material risk of identity theft."

§ __.90(c) Identity Theft Prevention Program

Proposed paragraph § __.90(c) states that each financial institution or creditor must implement a written Identity Theft Prevention Program that includes reasonable policies and procedures to address the risk of identity theft to its customers and the safety and soundness of the financial institution or creditor in the manner described in § __.90(d). In addition, proposed paragraph § __.90(c) states that the Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

Wells Fargo agrees with the observation that the "appropriateness" of a Program will vary depending on the size and complexity of the financial institution. To further this notion, we believe it is critical for the Agencies to add language specifying that, when designing policies and procedures for its Program, it is appropriate for a financial institution to take into account the cost and value of proposed polices and procedures. Without this specific acknowledgment, institutions could arguably be expected to incorporate all of the Red Flags equally; even where they have determined that certain Red Flags would result in excessive costs or resources, but add little value to the overall Program. This will also clarify that an institution's Program is truly intended to be risk-based and tailored for its particular needs and risks.

§ __.90(d) Development and implementation of Program

Section __.90(d)(1)(i) provides that the Program must include policies and procedures to identify which Red Flags, singly or in combination, are relevant to detecting the possible risk of identity theft to customers or to the safety and soundness of the financial institution or creditor, using the risk evaluation described in § __.90(d)(1)(ii). Under the sub-heading entitled "Risk-based Red Flags," that section further requires that the Program must, at a minimum, incorporate any relevant Red Flags from Appendix J (the Red Flag Guidelines), applicable supervisory guidance, incidents of identity theft that the financial institution or creditor has experienced, and methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks.

The Agencies request comment on whether the enumerated sources of Red Flags are appropriate. Wells Fargo generally agrees that the enumerated sources listed are appropriate. However, we are very concerned with the proposed language mandating the incorporation of these enumerated sources, which states that, "*At a minimum*, the Program *must* incorporate any relevant Red Flags from: [the enumerated sources of Red Flags]." (Emphasis added). This language requiring the incorporation of the enumerated sources of Red Flags not only goes against the notion of a truly risk-based approach, but it is contrary to the Agencies' intentions stated in the Supplementary Information.

Wells Fargo strongly encourages the Agencies to clarify that the enumerated sources of Red Flags listed in proposed paragraph § __.90(d)(1)(i)(A)-(D) (and in particular, the Red Flag Guidelines in Appendix J) are suggested guidelines only, and not a mandatory checklist against

which a financial institution's Program will be judged. If institutions are required to incorporate all of the enumerated sources of Red Flags into their Program, they will lose their ability to design a Program tailored to their specific needs and based on their particular experience. This will result in an ineffective, one-size-fits-all Program.

The Supplementary Information states that "the Agencies are not proposing to prescribe which Red Flags will be relevant to a particular type of financial institution or creditor. For this reason, the proposed Regulations provide that each financial institution and creditor must identify for itself which Red Flags are relevant to detecting the risk of identity theft, based upon the risk evaluation described in § __. 90(d)(1)(ii)." The Agencies are apparently referring to the word "relevant" in § __. 90(d)(1)(i), which states: "At a minimum, the Program must incorporate any *relevant* Red Flags . . ." (Emphasis added).

At first glance, the word "relevant" seems to qualify the compulsory "*At a minimum*, the Program *must* incorporate any relevant Red Flags . . . ," language, making incorporation of those items appear optional. However, the language in proposed paragraph § __.90(d)(2)(iii) eliminates any illusion that incorporation of the enumerated sources is optional: "an institution or creditor *must have a reasonable basis* for concluding that a Red Flag does not evidence a risk of identity theft." (Emphasis added). This sentence conveys a clear expectation that all of the enumerated sources of Red Flags *must* be incorporated into the Program, and puts the burden squarely on the financial institution or creditor to prove why a particular Red Flag should not be included in its Program. This would effectively require institutions to unnecessarily squander valuable resources conducting reviews and analyses of every Red Flag, without regard to the actual degree of risk or relevancy to the particular institution. As discussed earlier, virtually any activity related to a financial account could pose a "risk of identity theft." Requiring institutions to have a reasonable basis for concluding that a Red Flag does not evidence a mere "risk of identity theft" will overly burden them with false leads and distract resources and attention from actual instances of identity theft. In addition, this requirement would put institutions in a defensive position of having to engage in a time-consuming administrative exercise of documenting and re-reviewing; time that could be better allocated to designing and implementing a truly effective Program.

This is not a risk-based approach and contrary to the Agencies' statement that they are not proposing to prescribe which Red Flags will be relevant. To be consistent with the Agencies' statements in the Supplementary Information, the Proposed Rule should reflect an actual risk-based approach. Accordingly, Wells Fargo strongly recommends that the sentence "an institution or creditor must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft" be deleted to accomplish the goal of giving institutions a truly risk-based approach to designing a Program appropriate to their risks. Alternatively, if that sentence is maintained, we strongly recommend the term "a risk of identity theft" is qualified to say "a *significant* risk" or "a *material* risk." This would be consistent with the suggested changes to the definition of "Red Flag" and appropriate for the same reasons discussed in that section.

Section __.90(d)(1)(i) also requires that the Red Flags identified by the Program reflect changing identity theft risks to customers and to the financial institution or creditor "as they

arise." In addition, the Supplementary Information states that new Red Flags must be incorporated on a "continuing basis" to ensure the Program reflects changing identity theft risks.

Wells Fargo agrees that updating the Red Flags to address changing identity theft risks is vital to an effective Program. However, these terms could arguably require an institution to review and assess its Program on a daily basis. This would require substantial resources and result in an unreasonable burden. We therefore suggest the Agencies clarify this language to say that institutions would have a "reasonable amount of time" to adapt their Programs upon identifying new Red Flags.

Wells Fargo supports the statement in the Supplementary Information that, "Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent, and mitigate identity theft." We therefore urge the Agencies to give each financial institution real autonomy and flexibility to design a Program appropriate to its specific risks.

§ __.90(d)(4) Oversight of service provider arrangements

Proposed paragraph § __.90(d)(4) provides that whenever a financial institution or creditor engages a service provider to perform an activity on its behalf that is covered by § __.90, 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 that section. Service provider is broadly defined in the Proposed Rule as "a person that provides a service directly to the financial institution or creditor."

The Agencies invite comment on whether permitting a service provider to implement a Program, including policies and procedures to identify and detect Red Flags, that differs from the programs of the individual financial institution or creditor to whom it is providing services, would fulfill the objectives of the Red Flag Regulations. The Agencies also invite comment on whether it is necessary to address service provider arrangements in the Red Flag Regulations, or whether it is self-evident that a financial institution or creditor remains responsible for complying with the standards set forth in the Regulations, including when it contracts with a third party to perform an activity on its behalf.

Wells Fargo believes it is unnecessary for the Agencies to specifically address service provider arrangements in the Red Flag Regulations and that this provision should be removed. The Rule ultimately holds a financial institution or creditor responsible for implementing and maintaining a Program. Moreover, previous regulatory guidance[6] already makes it self-evident that a financial institution or creditor would be accountable for any service providers used to implement its Program. By having a specific provision just for service provider oversight, the Proposed Rule gives unnecessary attention to the subject, and causes potential confusion about why oversight of service providers was specifically singled out. If use of service providers is mentioned at all in the Proposed Rule, Wells Fargo recommends that it simply acknowledge that service providers may be used and make it part of the overall Program.

[6] *See* OCC Bulletin 2001-47: Third Party Relationships

§ __.90(d)(5) Involvement of board of directors and senior management

The Agencies are requesting comment regarding the frequency with which reports should be prepared for the board, a board committee, or senior management. They also request comment on whether responsibility for oversight and implementation of the Program between the board and senior management has been properly allocated.

The Proposed Rule would require the board of directors or an appropriate committee of the board to approve the Program. The Rule would also obligate the board of directors, an appropriate committee of the board of directors, or senior management, to oversee the development, implementation, and maintenance of the Program.

Wells Fargo strongly urges that any requirement for board or senior management involvement with the Identity Theft Prevention Program make clear that this requirement does not include the operational aspects of such a Program. Rather required board "oversight" and "approval" should be limited to directing the creation of a Program, high-level reports on its structure and resources, periodic reports on its effectiveness. Any requirement involving the board or senior management in operational aspects would unnecessarily delay the implementation of the Program and hinder the institution's ability to adapt the Program quickly to changing identity theft risks. In the Supplementary Information, even the Agencies acknowledge the difficulty with keeping a Program updated to address constantly changing identity theft risks: "While the Agencies expect to update Appendix J periodically, it may be difficult to do so quickly enough to keep pace with rapidly evolving patterns of identity theft or as quickly as financial institutions and creditors experience new types of identity theft." Similarly, boards of directors and senior management would have difficulty responding to new types of identity theft quickly enough. They are not the appropriate levels for reviewing, implementing, and maintaining an Identity Theft Prevention Program which, by its very nature, must be able to change quickly as new risks arise, in order to be effective. Rather, such obligations should be left to the levels of management more familiar and involved with the day-to-day fraud and identity theft risks, who can respond more effectively, and on a continuing basis, to newly arising identity theft risks.

Further, requiring review and approval of the Program at such a high level of an organization is unnecessary, because the Proposed Rule would still ultimately hold each financial institution or creditor responsible for implementing a Program. The Agencies should defer to institutions to implement a Program consistent with the Rule as they deem appropriate and refrain from attempting to micromanage the details of how that Program should be implemented internally.

If the Agencies decide to retain a requirement for board involvement with an Identity Theft Prevention Program, we recommend that the requirement be stated at a level which acknowledges that the board must oversee a wide variety of risks and programs. A requirement for "approval" implies that specific corporate actions would need to be taken by the board whenever a Program is changed. As stated above, we are concerned that such a requirement

introduces an unnecessary element of bureaucracy and inflexibility, requiring additional corporate resources and potentially interfering with the institution's ability to quickly respond to changes in possible identity theft threats as well as diverting the board's attention from the myriad of other issues it must oversee. Oversight through periodic reporting to the board should be sufficient to address concerns about corporate accountability for a Program.

Finally, we urge the Agencies to make it clear that in a holding company structure with multiple subsidiaries covered by the Proposed Rule, the approval and/or oversight of a Program by the holding company board or a committee thereof will be sufficient, as long as the Program by its terms applies to subsidiaries of the holding company.

Appendix J – Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

The Agencies have developed a list of proposed 31 Red Flag Guidelines to implement Section 114 of the FACTA which directs the Agencies to develop guidelines which identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. The Agencies are soliciting comment on whether the proposed Red Flags listed in Appendix J are too specific or not specific enough, and whether additional or different Red Flags should be included.

As discussed in greater detail earlier in this letter, the Rule should be changed to clarify that the Red Flag Guidelines in Appendix J are suggested guidelines only, and not a mandatory checklist against which a financial institution's or creditor's Program will be judged. Although Wells Fargo makes specific comments below regarding certain Red Flags, each comment below should be read in the context of the general concern that these Red Flag Guidelines be provided as suggested guidelines only and not compulsory components of its Program.

Information From a Consumer Reporting Agency

3. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries.

b. An unusual number of recently established credit relationships.

c. A material change in the use of credit, especially with respect to recently established credit relationships.

d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

COMMENT: This Red Flag is too subjective, vague, and unmanageable, as it would be

relative to the personal habits and characteristics of each individual consumer. Credit application, scoring, underwriting and accounting systems are not set up to detect this type of detail on individual accounts. For example, most loan decisions today are made systematically using scorecards with little or no human intervention. In addition, financial institutions' systems do not currently have the capacity to monitor accounts individually for these patterns and if required to do so, it would render decisions via scorecards virtually meaningless, slow down the application process, and substantially increase underwriting costs.

Moreover, terms such as "recent," "significant," and "unusual" are too relative to be meaningful. This Red Flag would require a manual review of millions of accounts, at astronomical costs to Wells Fargo. Even if a manual review of all accounts for these anomalies were possible, those terms would be unworkable. For instance, what is "unusual" for one account may be perfectly "normal" activity for another. In addition, with respect to 3(d), Wells Fargo would have no way of knowing why an account was closed, beyond what is reported by the CRAs, which is typically either "closed by consumer" or "closed by credit grantor." Accordingly, Wells Fargo strongly recommends this Red Flag be removed.

Documentary Identification

7. Other information on the identification is not consistent with information that is on file, such as a signature card.

COMMENT: Having information "on file" does not necessarily mean that information is readily accessible across all lines of business of an organization. This Red Flag should clarify that there will not be an expectation that every part of an organization is going to be able to have reasonable access to information "on file" just because one part may have such information. Using signature cards as an example, they often do not exist on all accounts. Even where a signature card is on file, they are physically located in one location and are not imaged. As a result, the ability to cross reference and access signature cards across all parts of the organization is extremely limited.

Personal Information

8. Personal information provided is inconsistent when compared against external information sources. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

9. Personal information provided is internally inconsistent. For example, there is a lack

of correlation between the SSN range and date of birth.

COMMENT: Although resources exist to verify the authenticity of a SSN with respect to the age of a consumer, these systems are not typically deployed in all lines of business nor within all areas of a line of business. We request this Red Flag clarify that it is not meant to require an institution to purchase services or program that verify the authenticity of a SSN if that process is not part of the institution's underwriting procedures today.

10. Personal information provided is associated with known fraudulent activity. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

11. Personal information provided is of a type commonly associated with fraudulent activity. For example:

a. The address on an application is fictitious, a mail drop, or prison.

b. The phone number is invalid, or is associated with a pager or answering service.

12. The address, SSN, or home or cell phone number provided is the same as that submitted by other persons opening an account or other customers.

13. The person opening the account or the customer fails to provide all required information on an application.

14. Personal information provided is not consistent with information that is on file.

COMMENT on Red Flags 10-14: The Agencies should clarify that these Red Flags are not meant to suggest that financial institutions will be required to maintain enterprise-wide databases of known fraudulent applications. Although some individual lines of business may maintain some of this information, it is not done at the enterprise level. In addition, even for those lines of business that retain such information, it is not easily accessible by all other parts of the organization due to system constraints and information sharing limitations. There is currently no one-size-fits-all solution for automating sharing of knowledge on all customers across all parts of the company and to implement such a system would entail unreasonable costs and substantial resources.

Address Changes

16. Shortly following the notice of a change of address for an account, the institution or creditor receives a request for new, additional, or replacement checks, convenience checks, cards, or a cell phone, or for the addition of authorized users on the account.

COMMENT: This Red Flag is not particularly indicative of identity theft. It is common for a consumer to request new checks in close proximity to moving. We recommend this Red Flag be removed or qualified accordingly.

17. Mail sent to the customer is returned as undeliverable although transactions continue to be conducted in connection with the customer's account.

COMMENT: We recommend this Red Flag be removed, as it is not a very reliable indicator of identity theft. If this Red Flag is retained, it should clarify that it applies to physical mail only and not electronic mail.

Anomalous Use of the Account

19. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

COMMENT: Similar to Red Flag #3 above, this Red Flag is too subjective and vague, and therefore unmanageable. These patterns may or may not indicate an anomaly depending on the type of account. There are a number of legitimate circumstances under which these patterns might occur, so these Red Flags are not particularly helpful as indicators of identity theft. In addition, the terms "not consistent with established patterns of activity" and "material" are too subjective to be helpful or useful.

Wells Fargo's lines of business already utilize sophisticated fraud detection systems which are tailored to the specific product or account, but are not set up to detect this type of detail on individual accounts. To do so would require systems changes or a manual process that would unreasonably hinder the application process, while offering little, if any, benefit in combating identity theft. Accordingly, Wells Fargo recommends this Red Flag be removed or alternatively, that the final Rule clarifies that these Red Flags are

suggested considerations for an Identity Theft Prevention Program and not mandatory components.

Notice From Customers or Others Regarding Customer Accounts

24. The financial institution or creditor is notified that its customer has provided information to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website.

COMMENT: We recommend the Agencies qualify the type of "information" a customer may have provided to mean information with which an unauthorized third party could perpetrate fraud or identity theft. Examples of this type of information might include name, birth date, social security number, account number, personal identification number (PIN), or any combination of those pieces of information. We also recommend that the Agencies clarify in the Supplementary Information or Commentary that upon the occurrence of an event described in Red Flag #24, an institution would have the discretion to analyze and determine appropriate action to be taken, and that there would not be an automatic expectation to close the account in every instance.

Other Red Flags

26. The name of an employee of the financial institution or creditor has been added as an authorized user on an account.

27. An employee has accessed or downloaded an unusually large number of customer account records.

COMMENT: Because employees and their families are also customers of Wells Fargo, it is not necessarily unusual or an indication of identity theft if an employee has been added as an authorized user on an account. Similarly there are many legitimate reasons why an employee may have accessed or downloaded an unusually large number of customer account records. Since these are not reliable indicators of identity theft, Wells Fargo has not implemented systems to detect or monitor these activities. In addition, even if we were able to monitor when and if an employee was added to an account, it could raise issues of privacy for the employee as well as for the account holder. Accordingly, we suggest that these Red Flags be eliminated or qualified.

Section __.91 – Duties of Card Issuers Regarding Changes of Address

Section 114 specifically provides that the Agencies must prescribe regulations requiring credit and debit card issuers to assess the validity of change of address requests. The Agencies request comment on the provision requiring validation of an address change request and, in

particular, whether the Agencies should elaborate further on the means that a card issuer must use to assess the validity of a request for a change of address.

Wells Fargo recommends that the Agencies clarify the Proposed Rule to state that a card issuer will be in compliance with this section if it chooses to always perform the change of address validation requirements outlined in § __.91(c)(1)-(3), regardless of whether or not there is a subsequent request for an additional or replacement card for the same account. Wells Fargo is currently unable to link a change of address occurrence with a subsequent request for an additional or replacement card. Consequently, we would be unable to validate an address change request only in situations where a request for an additional or replacement card is subsequently made. However, Wells Fargo already performs validations of address change requests even where there is not a later request for another card.

Conclusion

Mitigating and preventing fraud and identity theft has always been a top priority for Wells Fargo. We strongly support the goals of sections 114 and 315 of the FACTA and are committed to allocating appropriate resources to the ever-changing risks of fraud and identity theft. To achieve these goals, we believe a final rule which provides greater flexibility and a true risk-based approach to the establishment and implementation of an Identity Theft Prevention Program is essential. Therefore, we respectfully urge the Agencies to consider all of the comments and suggestions herein, and promulgate a final rule that is flexible, risk-based, and consistent with the requirements of the statute.

If you have any questions or would like to discuss any of the issues raised herein, please do not hesitate to contact me at (515) 222-8218 or Michael.D.Wood@wellsfargo.com.

Sincerely,

/s/ MICHAEL D. WOOD

Michael D. Wood
Senior Counsel