

Satterfield, Kevin

21

From: deanna.heggestad@wachovia.com on behalf of eugene.m.katz@wachovia.com
Sent: Monday, September 18, 2006 1:29 PM
To: Regs.Comments
Subject: Wachovia's Comment Letter Re: OCC Docket Number 06-07
Attachments: OCC COMMENT LETTER_20060918121529.pdf

Attached is Wachovia's comments to the Joint Notice of Proposed Rulemaking: Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 and the proposed implementation of its Sections 114 and 315.

ForwardSourceID:NT0000C602

Wachovia appreciates the opportunity to comment on this proposal. Should you have any questions, please contact me.

Eugene M. Katz
Wachovia Corporation
Legal Division
Tel.: (704) 383-7707
Fax: (704) 715-4494

CONFIDENTIALITY NOTICE: The contents of this message may be confidential and may contain privileged attorney-client communication or attorney work product. If you are not the intended recipient of this message, please destroy.

9/18/2006

Wachovia Corporation
Legal Division
NC0630
One Wachovia Center
301 South College Street
Charlotte, NC 28288

Tel 704 374-6611

Eugene M. Katz
Senior Vice President and
Assistant General Counsel
Direct Dial: 704 383-7707
Fax: 704 715-4494
Email: gene.katz@wachovia.com



WACHOVIA

September 18, 2006

Via Electronic E-mail : regs.comments@occ.treas.gov

Office of the Comptroller of the Currency
250 E Street, NW
Public Reference Room
Docket No. 06-07
Mail Stop 1-5
Washington, DC 20219

Re: OCC Docket Number 06-07: Proposed Interagency Regulation and Guidelines on Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, issued July 18, 2006

Ladies and Gentlemen:

This letter is submitted on behalf of Wachovia Corporation and its national bank subsidiaries Wachovia Bank, National Association and Wachovia Bank of Delaware, National Association (collectively referred to as "Wachovia"). In this letter Wachovia provides comments to the Joint Notice of Proposed Rulemaking: Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), and the proposed implementation of its Sections 114 and 315.

Given the recent barrage of attacks upon consumers' personal and financial data, Wachovia supports Congress' and the agencies' intent to improve fraud and identity theft prevention processes. Wachovia serves over 13.4 million customer households and businesses, and, we take very seriously the trust that those customers have placed with us. Wachovia thus has been a leader in the financial services industry's efforts to reduce fraud and identity theft. Based on peer industry studies, it has the best performance in managing fraud losses and identity ("ID") theft and has held this distinction for the last five years.¹

¹ Additionally, Wachovia has led the BITS anti-fraud work group for the past four years; we are a founding member of the Identity Theft Assistance Center; and we were first to provide a fraud and identity theft protection kit to customers. Wachovia managers and subject matter experts are on product development advisory boards for a large number of technology companies that offer fraud and ID theft solutions, and they have collaborated with the Federal Trade Commission, U.S. Department of Homeland Security and other government agencies on fraud and ID theft prevention initiatives.

Wachovia clearly recognizes that Congress' amendments to the Fair Credit Reporting Act require the adoption of a certain level of regulation and/or guidance.² However, as a result of the expertise and experience that Wachovia has gained in fraud and ID theft reduction initiatives, we respectfully submit that the proposed regulation and guidelines as written are overbroad, go beyond the "reasonable" standard set by Congress, and present financial institutions with undue regulatory burden and costs, which customers ultimately bear, while not achieving their laudable intent of increased consumer protection.

GENERAL CONCERNS

I. Loss of Agility

Wachovia is concerned that, if the proposal goes forward as currently drafted, financial institutions will lose some of their fraud/identity theft response "agility" and current dynamic management practices because they will be locked into undue regulatory oversight and documentation burdens. While espousing dual goals of flexibility and a risk-based approach, the regulations instead call for implementation of an administratively burdensome identity theft prevention program ("Program") that would include such things as approval at the board of directors level, mandated board updates, initial and periodic assessments, policies, procedures, monitoring, and a prescribed, static (and therefore subject to becoming outdated) checklist of 31 "Red Flag" identity theft factors -- some too specific, others too general; some not actionable, and some not even applicable to financial institutions.

As discussed below, we recommend that the regulation be substantially rewritten to give financial institutions broad discretion and strategic capabilities to manage fraud and identity theft risks.

II. Minimalist Approach

The agencies have proposed requirements that are not mandated by statute. For example, the proposal:

- Requires a Program approved at the board of directors level that must be updated (and, it would follow, again submitted to the board for approval) regularly.

Fraud and identity theft prevention processes must be dynamic and able to change quickly as new schemes and scams arise. To allow for this fluidity, a board-approved Program would have to be (1) so general that it would serve little purpose, or (2) updated and approved very frequently, an impractical and inefficient process, or (3) approved retroactively, which makes little sense.

² These statutory mandates are summarized by the Agencies themselves in the "Supplementary Information" published in the Federal Register at 71 Fed. Reg. 40786, 40788 (July 18, 2006).

Also, official policy-level programs, especially board-approved ones, are expected to be administered and then "monitored" for compliance – by external regulatory agencies, internal audit departments and-or line-of-business assessment areas. Experience teaches that this often leads to form over substance.

- Puts banks in the position of proving a negative

Section __90(d)(2)(iii) states that institutions "must have a reasonable basis for concluding that a Red Flag does *not* {emphasis added} evidence a risk of identity theft." Experience tells us that it is almost impossible to prove a negative. Including this component in the regulation sets up a situation for examiner "second guessing".

All such efforts divert time, staff and financial resources away from the consumer protection goal, and they are superfluous, given the generally recognized good job that financial institutions already perform in the fraud/ID theft prevention arena.

Wachovia therefore strongly recommends that the regulators take a minimalist approach to the required regulation and guidance, and include only those things that the statute absolutely mandates.

III. Disproportionate Expense for Value Received

The cost of implementing a Program as currently proposed would be exorbitant for large, sophisticated banking companies, as it would require the necessary assessment processes, technology enhancements, manual procedures, monitoring, investigation, additional employees for those duties, training of both customer-contact and back-room support staff, and so forth. The costs incurred by financial institutions ultimately are passed on to consumers. Also, the effort involved in implementing the envisioned program would divert company resources from other day-to-day business needs and special initiatives, resulting in lost opportunity in addition to actual hard dollar and time costs.

For example, consider the following that would be involved to address the 31 "Red Flags" from a technology point alone:

- Wachovia has more than 20 million deposit accounts. It opens and processes those accounts on numerous systems, including front-end applications and records systems for demand deposits, time deposit and securities accounts (which also house FDIC insured deposits in certain sweep account products); and maintenance and other specialized monitoring systems.
- Similarly, its vast number of credit accounts are opened and housed on numerous front-end application-taking and record processing systems for consumer, mortgage, commercial, student and credit card lending product systems.

- Other specialized areas such as loss management and anti-money laundering units have specialized systems which conceivably could house identity-related data.

While Wachovia cannot, at this time, estimate the precise technology expenditure for the Program envisioned by the proposal, we do know that a recent anti-money laundering enhancement project, which involved approximately 16 systems, cost Wachovia several million dollars.

Regarding training, we estimate that more than 20,000 hours would be required for customer contact staff on the actionable "Red Flags."

Significant expense on fraud and identity theft prevention would be better utilized by focused measures developed in response to experience and expertise than by expenditure on "program" implementation and documentation.

IV. Risk Assessment – Both Not Enough and Too Much

Under the proposed regulation, each institution would have to implement a written Program based on a bank-defined assessment of its own accounts, customers and risk tolerance.

- The Agencies have provided little guidance on how this assessment should be performed, leaving the door open to inconsistent regulatory oversight among the Agencies themselves and among individual examiners. If the Program and the accompanying assessment process remain requirements as proposed, Wachovia requests that the Agencies provide general guidance so that banks' assessment approaches would be somewhat consistent, but without creating a one-size-fits-all situation. We suggest assessment guidance that would vary by bank size/sophistication -- for example large versus small, multi-national versus national, regional and/or community banks, etc. -- 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, including financial, operational, compliance, reputation, and litigation risks.
- On the other hand, the proposed regulation expects banks to perform risk-based analysis and assessment, act upon and document for the 31 Red Flags individually and *in combination* (Subpart J – 41.90(d)(1)(i)). Since there can be more than 2 billion combinations of the 31 Red flags, this is an unrealistic expectation.

Wachovia recommends that the Red Flags identified in the proposed regulations be utilized only as illustrative examples and referenced as a source of current best thinking and practices in identifying ID theft risk drivers. This approach would enable financial services institutions to comply with the purpose and intent of the proposed regulation while being able to adapt response strategies over time as new ID theft risk drivers evolve.

Also, if the Agencies proceed with the regulation, they should make it clear that institutions are not required to aggregate data for this regulation, but should have plans to use combined data if they already are aggregating it for other purposes.

V. Unintended Adverse Consequences

The regulation may have unintended adverse reputation, financial and legal consequences for financial institutions by:

- Creating an inappropriate expectation in customers' minds about what banks are and are not capable of doing to prevent identity theft.
- Creating potential exposure to threats of litigation that today does not exist. Under the proposed regulation, and in spite of the inappropriate expectation noted above, there is no safe harbor provision for financial institutions to give effect to the execution of a best efforts/good faith effort response to a customer whose identity has been stolen.
- Impairing financial institutions' ability to manage and reduce fraud and identity theft both currently and in the future, due to the specificity that the proposal requires in individual banks' board-approved programs. For example, it would require delineating those account and product types that are most at risk and delineating incidents of ID theft from a bank's own experience. This is tantamount to publishing potential internal weaknesses for future use – identity thieves, fraudsters and other financial criminals may find they have clues, if not roadmaps, in their hands.

SPECIFIC COMMENTS

In addition to the general concerns expressed above, Wachovia now provides comments on some specific questions that the Agencies had asked in their proposal as well as on certain of the "Red Flags" themselves.

A. Definition of "Account"

The Agencies asked for comment on:

- a) Scope of the proposed definition of "account," specifically whether reference to "financial products and services 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" is appropriate to describe the relationships that an account holder or customer may have with a financial institution or creditor that should be covered by the Red Flag Regulations.*
- b) Whether the definition of "account" should include relationships that are not "continuing" that a person may have with a financial institution or creditor.*

While we agree in concept with the proposed definition, we suggest that the definition for this rule and the definition found in the FFIEC guidance for AML purposes be synchronized.

Regarding lending, we suggest that retail sales contracts, loans through a correspondent relationship and loans otherwise purchased by the institution be specifically exempt from the definition. The financial institution is not responsible for customer identification programs ("CIP") on these type loans.

We believe that relationships that are not "continuing" should be excluded, and we recommend that the definition specifically exclude stored value cards, gift cards and other prepaid card products. We also presume the word "continuing" would exclude an application which is declined and does not become an account.

Regarding "dormant accounts," from a lending perspective, home equity lines of credit may have card access features, and the lines seldom may be used. The regulation should clarify that this, in and of itself, will not constitute a classification as a dormant account. Each financial institution should be given the ability to determine when an account is dormant based on the account transaction activity.

B. Definition of "Customer"

The Agencies solicited comment on the proposed definition of "customer" which would encompass both "customers" and "account holders," meaning a person that has an account with a financial institution or creditor, and would include any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

This appears inclusive of all parties to a transaction. However, regarding lending, guarantors and authorized users are exempt from the CIP requirements in the USA PATRIOT Act, and therefore we recommend they be exempted from this rule as well. Also, we recommend (1) excluding large businesses, and distinguishing them from small businesses, using the Regulation B test of "annual gross revenues," and (2) eliminating such entities as: trusts, estates, corporations, limited liability corporations, limited partnerships, and partnerships of three or more. The institution should have the ability to include these based on their internal risk assessments.

C. Scope and Definition of "Red Flags"

The Agencies specifically ask whether "Red Flags" should be defined expansively to include precursors to identity theft which indicate "a possible risk" of identity theft.

Wachovia agrees that precursors are a concern, but we do not think they should be within the context of the definition. For example, credit grantors have no control over information a customer may provide in response to phishing schemes or email scams.

Also, other regulations require financial institutions to have in place processes and procedures to address security breaches.

D. Red Flag Sources

The Agencies state that they compiled the Red Flags from numerous sources, including topical literature, credit bureau information, financial institutions, creditors, fraud detection software designers and Agency experience. The Agencies ask whether the enumerated sources are appropriate.

We believe that none of the sources are inappropriate. In addition to these, financial institutions have the ability to go to other sources as they see fit.

E. Anticipated impact on Current Policies, Procedures and Third-Party Processes

The Agencies ask for comment on possible impact of a requirement that financial institutions independently assess whether third-party products meet any Red Flags regulation requirements, rather than relying on third-party representations.

Financial institutions obtain credit information from nationally recognized credit reporting agencies and other credit information reporters. These businesses utilize internal processes such as FALCON and HAWK to assist in identifying mismatched personal information, and to put the institution on notice of that fact via these processes. Additionally, institutions have processes and policies in place to comply with the requirements of legislation including the Gramm-Leach-Bliley and USA PATRIOT Act CIP requirements.

We believe that well-run financial institutions would not and should not rely solely on any third-party's representations of its capabilities, but should always assess those capabilities themselves. Presuming that banks already do such assessments, a requirement to do so would have little impact.

F. Red Flag Factor Appropriateness

The Agencies request comment on whether the factors that "must be considered" are appropriate and whether any additional factors should be included.

Wachovia already has noted that a static listing can quickly become outdated and a form-over-substance "checklist." As noted previously, we recommend that the Red Flags be used as examples only – they should not be a prescribed list that banks must address individually and/or in concert.

G. Measures To Address ID Theft Risk

The Agencies list nine measures that financial institutions or creditors might take and asks if they should be included as "examples" and whether additional measures should be included.

Wachovia believes these are generally recognized measures and should only be "examples," with institutions being free to use or expand upon them as appropriate. Institutions should not be held to a prescribed list of measures that may or may not be relevant.

However, if the Agencies do prescribe the nine measures, rather than using them as examples, we request clarification on the term "implementing any requirements" referenced in measures "H" and "I." In response to the Notice of Proposed Rulemaking comment letter in May 2006, we provided significant information relating to the accuracy and integrity of information shared with and received from credit reporting agencies, and the difficulties in maintaining data accuracy. We noted that despite the best efforts of all parties involved in this process, human errors do occur. Our objective should be to minimize these occurrences by our internal processes and procedures with the ability to access and comment on any future requirements.

H. Service Providers

The Agencies ask 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.

In response to the previous request for comment regarding the impact on a financial institution, we pointed out that financial institutions obtain credit information from nationally recognized credit reporting agencies and other credit information reporters. These businesses utilize internal processes such as FALCON and HAWK to assist in identifying mismatched personal information, and put the institution on notice of that fact via these processes.

Additionally, these suppliers of credit information have, through representations and warrants contained in contracts, assured the institution they are in compliance with the applicable laws and regulations pertaining to data accuracy, identity theft and privacy under FACTA, USAPA and the FCRA. The institution should only have the responsibility after it receives the data from the credit reporting agencies.

I. Board Reporting

The Agencies request comment on the frequency with which reports should be prepared for the board, a board committee, or senior management.

Wachovia has questioned herein the efficacy of a Program that requires board-level approval and mandated board reporting as unnecessarily bureaucratic and which will inhibit banks' flexibility and agility in fighting fraud and ID theft. However, should the Agencies proceed with this requirement, we submit that annual reporting is sufficient, and would conform to existing privacy and anti-money laundering compliance program reporting requirements.

In this regard, should a change in the Program be required, appropriate updates could be provided to the board as soon as practical. We do not recommend delaying the implementation of a necessary change until board approval is secured. Often a pro-active immediate change is necessary for immediate implementation to mitigate a risk. Should the board, at the time of annual reporting, disagree with a Program change, the program can be modified to accommodate the board's directives.

J. Inclusion/Exclusion of Appendix J Red Flags and Their Specificity

The Agencies solicit comment on whether the Red Flags in Appendix J are too specific or not specific enough, and whether more or different Red Flags should be included.

As stated above, Wachovia strongly recommends that the Red Flags list be used solely as examples and not a static requirement for institutions. This is due in part to the fact that some are too specific, others not specific enough, that some are not actionable, and others are not applicable.

Also, lists such as this tend to become a "laundry list" that auditors or examiners may concentrate on during reviews. Some bank staff may find themselves focusing on the "31 items" to pass an audit or exam, rather than concentrating on the goal of fraud/ID theft prevention. If the Agencies proceed with this approach, we recommend some guidance be included as to how the institution should document its decisions not to include a particular Flag. Without additional guidance, this can become a burdensome task to the institution and an open-ended opportunity during a regulatory examination, with examiners perhaps second-guessing a bank's decision to not use a particular Flag in the Program.

Nonetheless, Wachovia has recommendations and/or requests clarification to the following specific Red Flags (not all 31 Red Flags are addressed):

1. A notice of address discrepancy is provided by a consumer reporting agency (CRA).

Banks today get such notices from the CRA (using an asterisk at the top of an individual's credit report) but monitoring them could be difficult. If the regulation is issued, it should include a requirement that CRAs emphasize the discrepancy.

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.*

For banks to be able to act upon the types of information noted above, banks would be dependent upon CRAs to provide us with significant amounts of factual data. Banks pull consumer reports only for specific individuals in certain limited circumstances (FCRA "permissible purposes"). When those specific occasions arise, the consumer reporting agencies would have to provide prior history for comparison with current activity.

Even with such knowledge, determining inconsistent activity would require sophisticated modeling and analytics. We believe that this expertise would be better developed by experts in the identity theft prevention and not left up to individual financial institutions. Financial institutions do not possess the confidential knowledge of the CRA's database structure and data sources to be able to develop a sophisticated tracking device to detect anomalies in a CRA's database.

Also, regarding item 3a (a recent and significant increase in the volume of inquiries on a consumer's report): this may not be indicative of inconsistent activity. Given the increasing financial awareness of consumers, there are more instances of consumers shopping for the best financial "deal" (rate, terms) in addition to the best product. In conjunction with the ease of use of the Internet, multiple inquiries are to be anticipated when a consumer is contemplating a purchase or investment. These should be considered on a case-by-case basis.

4. *Documents provided for identification appear to have been altered.*

While altered documents are addressed in account-opening procedures or teller transaction processes today, it is done so for a different purpose than in the proposal. Using it as an actionable ID theft flag would require a new mindset on the part of our staff, procedures, training, etc. – and it would have to be executed accurately thousands of times a day, a virtually impossible expectation. Training staff to review customer identification documents tends to be problematic for most large institutions. This flag should be revised to indicate documents that have "obvious and questionable alterations."

- 5. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.*

See the first comment in # 4 above.

- 6. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.*

See the first comment in # 4 above.

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

This Red Flag presents serious operational issues. It presumes that signature cards are instantaneously accessible to sales staff in the field, which is not true today. For them to be instantaneously accessible, they would have to be available systemically, within seconds; creating such a technological solution would be extremely costly. Ironically, without costly systematized access controls, having signature cards instantaneously available for fraud/ID theft prevention purposes could actually make them more readily accessible to unauthorized persons.

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

- *The address on an application is fictitious, a mail drop, or prison.*
- *The phone number is invalid, or is associated with a pager or answering service.*

Wachovia thinks this is not actionable and should not be included. Banks would not necessarily know this information. Also, regulations prohibit requiring a phone number on loan applications.

- 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.*

This is not an actionable flag for many institutions, and should not be included. Institutions do not always have all of this information, especially home or cell phone numbers. More importantly, they do not have the ability today to cross-reference data provided by different persons and housed within a single system and certainly not when data (even a SSN, the most obvious cross-reference) is housed on different systems which do not talk to each other; it would require sophisticated, costly technological solutions.

Further, a "hit" on two identical pieces of data – for example, an address or a phone number – does not necessarily mean something is wrong. It could be an old phone number reissued, or indications that individuals have moved. Investigating "false

positives” could be extremely time consuming and costly, and provide little value. Also, trying to do this at account opening would be a highly inefficient customer-service process.

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

This is a common occurrence, requiring additional action on the part of bank personnel. It is not necessarily a fraud or ID theft indicator. This Flag is simply too broad and ambiguous to be useful.

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

This Flag also is too broad and ambiguous. Further, it is logical that different information may have been obtained for different reasons (phone number contact on one account might be a cell phone while on another it might be a landline); or it may just be that the information is out of date.

15. The person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

This also is too ambiguous and broad to be useful.

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,

This is a Flag that is not reasonable in light of “real world” activity. It is normal for a person who moves to want new checks. Any customer moving from one home to another will get caught by this Flag.

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 telephone call patterns in connection with a cellular phone account.*

The term “material” would need to be defined for the items above. What is material for a 21-year-old may be different than that for a 70-year-old.

19a. Nonpayment when there is no history of late or missed payments is not necessarily a Red Flag. Nonpayment situations are monitored closely by collections

departments, usually on a monthly basis. A Red Flag would occur when a missed payment occurred in conjunction with something else: for example, a missed first payment on the account, or missed with returned mail.

19c. This is not information that banks necessarily would have. But if they did, identifying changes in purchasing or spending patterns would require substantial technological enhancements, especially if EFT patterns were involved. However, identifying such changes might not be useful because there are many pattern variations that normally follow certain product use: for example, (1) if a customer changes from a plain ATM card to a Debit/POS card or signs up for online billpay, this will automatically cause material changes in his account pattern – increased EFTs and/or EFTs of a different type; or (2) lifestyle events (overseas travel, graduation from college and move into professional work force, etc.) will affect purchasing or spending patterns.

19d. This is not applicable to financial institutions. Further, when banks have telephone numbers in our records (optionally, not required), we do not necessarily know whether it is a cellular phone or a landline.

20. *An account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).*

This Red Flag is reasonable and most banks already monitor dormant account use. That said, the Agencies should recognize that, except for “dormant” accounts, “expected” account use varies from customer to customer, and lack of use may be “normal” for many customers and certain types of accounts.

22. *The financial institution or creditor is notified that it has opened a fraudulent account for a person engaged in ID theft.*

The term “notified” in the red flag context is too broad. An institution responds each time it has knowledge that a fraudulent account has been opened, but it can receive that information in many different ways. Notification should be defined with more specificity.

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

Most institutions have instituted a systematic periodic review of each employee’s systems access to ensure they have access only to systems necessary for their work. However, while it might prove to be of some value, most institutions have no current way to detect when an employee downloads customer information for any reason. Implementing a technological process for this flag would have significant time and

cost impact to all institutions. Further, monitoring/analysis infrastructure would be required to determine whether access or downloads were problematic; there are many legitimate reasons that staff might obtain such access or data; for example, reports to generate sales leads or customer portfolio analysis.

28. *The financial institution or creditor detects attempts to access a customer's account by unauthorized persons.*

Wachovia and other banks already have access restrictions that detect access to some internal systems, but it would be difficult to restrict or detect access to individual accounts.

29. *The financial institution or creditor detects or is informed of unauthorized access to a customer's personal information.*

See Wachovia's comment to # 28.

30. *There are unusually frequent and large check orders in connection with a customer's account.*

For this to be actionable, vendors would have to report to banks on orders and banks would have to investigate to eliminate "false positives"; there are legitimate reasons for large orders, such as businesses changing their names or logos. Also, checks can be ordered by consumers through many different vendors.

K. "Cardholder" Definition

The Agencies ask whether the definition of a "cardholder" is appropriate.

We recommend that the definition specifically exclude a person who has been issued a stored value card, a gift card, or a card used as an access to a home equity line of credit account. Additionally, we recommend that a guarantor and an authorized user of an account be excluded because the institution as a normal business practice does not apply the same CIP rules as with the account owner(s).

L. Definition of "Clear and Conspicuous"

The Agencies ask if the definition of "clear and conspicuous" is appropriate.

We support the definition of clear and conspicuous as found in the Privacy regulation 12 CFR 216.3(b)(1).

M. Address Changes

The Agencies request comment on whether the section dealing with address changes should elaborate further on the form that a notice must take.

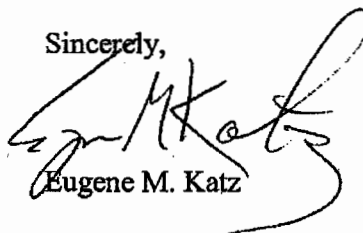
For purposes of assessing the validity of the consumer-initiated change of address, we recommend the proposal include an additional measure for first authenticating the customer making the request for the change of address (such as, if requests comes into a call center, the card issuer will ask a series of "out of wallet" questions, (i.e., specific questions for which only the customer would know, the answer), to ensure the caller is the true person; otherwise, in face-to-face situations, employ CIP procedures already in place to verify identity. This would require further clarification around the definition of "customer" (see response #3). Having authenticated the person requesting the change of address and determining that the person is authorized to make the request, would mitigate the need for burdensome, elaborate procedures following a request for an additional or replacement card.

We believe that providing notice to the card holder at the former address with a means of promptly reporting an incorrect address is a prudent measure and should be retained. We believe the proposal is broad enough to permit a card issuer to develop its own reasonable procedures with regards to providing such notice, as long as the definition of clear and conspicuous is better defined (see response #13).

* * *

In light of the foregoing, Wachovia respectfully urges that the Agencies substantially modify the proposal to better enable adaptability, flexibility; and management agility, which are critical to combating the dynamic and fluid nature of fraud and identity theft. Wachovia appreciates the opportunity on comment on this proposal. Should you have any questions, please contact me.

Sincerely,



Eugene M. Katz