INDEPENDENT COMMUNITY BANKERS of AMERICA

TERRY J. JORDE
Chairman
JAMES P. GHIGLIERI, JR.
Chairman-Elect
CYNTHIA BLANKENSHIP
Vice Chairman
KEN PARSONS, SR.
Treasurer
ROBERT C. FRICKE
Secretary
DAVID E. HAYES
Immediate Past Chairman

CAMDEN R. FINE
President and CEO

September 18, 2006

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

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

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

Mary F. Rupp, Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428
Attention: Proposed Rule 717,
Identity Theft Red Flags

Robert E. Feldman, Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Attention: RIN 3064-AD00

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, DC 20580
Attention: The Red Flags Rule,
Project NO. R611019

Re: Identity Theft Red Flags and Address Discrepancies under the
Fair and Accurate Credit Transactions Act (FACT Act) of 2003

Dear Sir or Madam:

The Independent Community Bankers of America (ICBA) appreciates the opportunity to comment on the joint agency proposal to identity patterns, practices and specific forms of activity that might indicate the possible existence of identity theft.[1] As

[1] The Independent Community Bankers of America represents the largest constituency of community banks of all sizes and charter types in the nation, and is dedicated exclusively to representing the interests of the community banking industry. ICBA aggregates the power of its members to provide a voice for community banking interests in Washington, resources to enhance community bank education

required by the FACT Act, the federal banking agencies and the Federal Trade Commission are proposing rules that would require banks to develop identity theft programs and establish procedures for handling notices of address discrepancies from consumer reporting agencies. The proposal would also require card issuers to develop procedures for handling a change-of-address request when it is followed by a request for a replacement card.

Overview of ICBA Comments

ICBA commends the agencies for their efforts. Identity theft is a growing problem and community banks have taken numerous steps to protect themselves and their customers. The trust relationship between a community bank and its customer is critical to the ongoing vitality of the community banking industry and it is an asset that community bankers greatly value.

ICBA recommends that the agencies take steps to make the final rule more flexible and more in keeping with what was intended by Congress when it adopted the FACT Act. While the agencies maintain that the intention of the rule is to be flexible and allow each bank to implement a program that meets its own unique needs and the particular circumstances of its market and product offerings, the actual text of the rule is much more proscriptive. ICBA is concerned that the specificity of the requirements in the proposal will create unnecessary burdens for community banks that will detract from their ability to devote resources to combating fraud and particularly identity theft, especially the requirement to conduct a risk assessment. Moreover, given the elements of the rule, it would likely be necessary for community banks to add personnel to administer the Identity Theft Program. For smaller institutions with limited staff, this would be an undue burden and counter-productive to the intentions of the rule by unnecessarily consuming limited resources.

ICBA recommends that the agencies:

- Offer guidelines to help banks conduct the identity theft risk assessment
- Clarify that coordination with existing rules, such as the customer identification rules under the USA PATRIOT Act and the information security guidelines under the Gramm-Leach-Bliley Act, meet the requirements of this rule without requiring duplicate procedures to satisfy this rule
- Grant added flexibility for handling "inactive" accounts to allow banks to coordinate any new requirements with already established rules such as those in place for unclaimed property laws

---

and marketability, and profitability options to help community banks compete in an ever-changing marketplace.

With nearly 5,000 members, representing more than 18,000 locations nationwide and employing over 265,000 Americans, ICBA members hold more than $876 billion in assets $692 billion in deposits, and more than $589 billion in loans to consumers, small businesses and the agricultural community. For more information, visit ICBA's website at www.icba.org.

- Limit the application of the requirements to consumers
- Provide a more focused definition of identity theft that does not include account takeover or *potential* identity theft, especially since virtually each and every transaction offers the potential for identity theft
- Maintain flexibility in the final rule that allows individual banks to tailor their policies and procedures to their own unique circumstances
- Clarify that the bank's board is responsible for oversight and not day-to-day management of the program
- Clarify that the list of red flags in Appendix J are *examples* and not a proscriptive checklist that must be applied to each and every category of account
- Grant card issuers additional flexibility when verifying an address to build on existing procedures
- Allow banks sufficient time to investigate an address discrepancy and clarify that minor discrepancies such as those caused by typographical errors are not covered
- Allow banks sufficient time to update procedures once a final rule issued, at least 12 months
- Substantially increase the estimated burdens imposed by the rule to reflect actual circumstances

The Proposal

FACT Act section 114 requires the agencies to develop guidelines ("red flags") to help banks identify patterns, practices and activities indicating possible identity theft. Under section 114, the agencies also must adopt regulations requiring each bank to develop reasonable policies and procedures to implement the guidelines. The regulations must include a provision requiring debit and credit card issuers to assess the validity of change of address requests. Finally, section 315 of the FACT Act requires the agencies to provide guidance on reasonable policies and procedures banks must use when receiving a notice of address discrepancy from a consumer reporting agency.

The proposal would require each bank to develop a written *Identity Theft Prevention Program* (Program) that includes reasonable policies and procedures to address the risk of identity theft. As part of the proposal, the agencies have identified 31 indicators or "red flags" that indicate possible identity theft, listed in Appendix J to the proposed rule. The proposal would apply a flexible risk-based approach, similar to existing guidelines for information security.[2] A bank's Program would have to include policies and procedures designed to prevent and address instances of identity theft, including steps for verifying information provided by persons opening accounts; measures to detect red flags indicating possible identity theft; steps to assess whether a detected red flag indicates possible identity theft; steps for mitigating the risk of identity theft; staff training; and oversight of service providers. Because the Program would complement existing information security standards and USA PATRIOT Act Customer Identification Program (CIP) requirements, it is recommended that banks coordinate the

[2] *Interagency Guidelines Establishing Information Security Standards* issued under the Gramm-Leach-Bliley Act in March 2001.

Program with those policies and procedures. Finally, the board or appropriate board committee must approve the Program and must receive a compliance report at least annually.

Current Community Bank Procedures

An informal survey of ICBA member institutions confirmed that most community banks currently take steps to prevent or limit fraud, including being on the alert for unusual transactions or activity in customer accounts, holding regular training sessions for employees to alert them to potential risks, and verifying new account information through credit bureau reports. It is important that the agencies recognize that all banks have developed these programs in part to comply with Bank Secrecy Act (BSA) requirements and to ensure they detect and report suspicious activities under existing BSA rules.[3]

Most community banks also take steps to ensure customers are educated about the dangers of identity theft. They provide these alerts through a variety of mechanisms, including brochures available in branches, articles in regular customer newsletters, holding customer education classes in the bank and area retirement centers (often including local law enforcement agents), providing links to Federal Trade Commission (FTC) and other agency information on fraud and identity theft through the bank's website, and lobby posters.[4] In addition, some community banks offer identity theft insurance to customers as part of an account package.

Anecdotal evidence indicates that the steps community banks are currently taking has been successful. While most community banks in the informal survey reported having customers who were victims of identity theft, few reported experiencing a loss at the bank as a result, and those few that reported a loss to the bank experienced losses under $2,500.

ICBA Comments on Specific Elements of the Proposal

Identity Theft Prevention Program

Risk Assessment. The proposal would require banks to develop a written Identity Theft Prevention Program. The first step would be for the bank to conduct a risk assessment of potential identity theft, considering which accounts are subject to possible identity theft; how those accounts are opened; how those accounts are accessed; and the bank's size, location and customer base. In carrying out this risk assessment, the bank

---

[3] The core procedures outlined in the interagency BSA/AML Examination Manual, updated in July 2006, require banks to have in place procedures for customer identification as well as appropriate due diligence programs for account activity that will enable banks to properly detect and investigate any inappropriate or suspicious activity.

[4] ICBA offers a brochure for member banks to offer their customers, *Protecting Yourself From Identity Theft*, available through ICBA's website.

must consider whether the Program should be limited to individuals or also include business customers.

ICBA believes that carrying out the risk assessment would be extremely burdensome and duplicative. This is especially so since there is an absence of guidelines about how the risk assessment should be conducted.[5] While most community banks have taken steps to prevent fraud, requiring a totally new assessment specifically to analyze the potential for identity theft would be burdensome. Moreover, community banks have already conducted this assessment as part of other programs and, to protect both the bank and its customers, are regularly on the alert for possible fraud. In addition, since the scope of identity theft is a changing and broad activity, without guidance from the agencies, the task of an identity theft risk assessment would be extremely time-consuming.

Coordination with Existing Programs. When community banks adopted the Customer Identification Programs (CIP) required by section 326 of the USA PATRIOT Act, they implemented processes and procedures designed to verify the identity of customers. When the CIP procedures were proposed, regulators pointed out that "by requiring identity verification procedures for all new accounts opened after the effective date of the final rules, the rules could also protect consumers against various forms of fraud, including identity theft."[6] Therefore, an additional but separate set of identity theft policies and procedures would be redundant. However, examiners are likely to require banks to have separate policies and procedures to comply with this second requirement. Having separate but parallel policies – in addition to being burdensome – also creates potential confusion.

Similarly, community banks are currently conducting a risk assessment for online banking under guidelines issued by the Federal Financial Institutions Examination Council (FFIEC). The guidance, issued in October 2005, was supplemented by a set of Frequently Asked Questions on August 15, 2006 that specifically address the issue of risk assessment that banks should undertake to protect customers against possible fraud when conducting online transactions or accessing account information.[7]

Since banks already have undertaken or are undertaking risk assessments for a variety of reasons, **ICBA urges the agencies to clearly articulate in the final rule that a risk assessment undertaken to comply with other regulatory requirements, such as**

---

[5] The BSA/AML Examination Manual includes an entire section and matrix to assist banks with a BSA risk assessment, and at the urging of industry representatives, this portion of the manual was enhanced as part of the recent 2006 revisions. The core procedures of the examination manual identify risk assessment as integral to a bank's BSA compliance program, and Appendix J of the manual outlines a detailed risk matrix for banks to use in conducting the assessment.

[6] Treasury Department Press Release, *Treasury and Federal Financial Regulators Issue Patriot Act Regulations on Customer Identification*, Treasury's Office of Public Affairs, July 17, 2002.

[7] See, e.g., *Authentication in an Internet Banking Environment* published by the FDIC at Financial Institution Letter, FIL-103-2005, October 12, 2005 and *Authentication in an Internet Banking Environment, Frequently Asked Questions*, published by the FDIC at Financial Institution Letter, FIL-77-2006, August 21, 2006.

BSA and CIP requirements, can form the basis for any risk assessment required under these rules. This would help eliminate potential redundancy and would clarify for bankers and examiners that an identity theft evaluation should be part of an overall bank fraud prevention program and not a separate, discrete evaluation that is not integrated into the bank's overall operations.

ICBA finds it helpful that the agencies recommend that the Program be coordinated with banks' existing policies and procedures for information security and CIP**. However, while it is important that these programs be coordinated, examiners should also clearly understand that existing policies and procedures that comply with CIP or information security are sufficient to satisfy the proposed Identity Theft Prevention Program requirements and that completely separate and discrete policy and procedures may not be needed**. In fact, separate but parallel policies and procedures could do more to engender confusion and needlessly add to regulatory burden without addressing the underlying risks.

One particular concern with this effort at coordination is that the proposal provides that while the CIP requirements contain certain exceptions, the identity theft procedures would apply to all accounts without exception. This difference is likely to be problematic and burdensome since banks will have to carefully review existing procedures to assess where supplemental policies and procedures are needed to address this distinction. **ICBA urges the agencies to carefully review and reconcile this distinction between the two programs, since it will otherwise make it difficult to implement a coordinated process.**

ICBA also urges the agencies to develop guidelines to help banks conduct an identity theft risk assessment. The guidelines should recommend – but not mandate – steps banks should take and the types of analysis required. A matrix similar to that used for the risk assessment in the BSA/AML Examination Manual would be extremely helpful for community banks.

Definitions

Account. The proposal would apply to accounts. Similar to the privacy rules, an account would be defined as "a continuing relationship established to provide a financial product or service." While this definition is broad, the agencies believe the risk-based nature of the Program would give banks the flexibility to determine which accounts are covered by different elements of the Program. **The ICBA believes that this part of the definition is appropriate.**

However, while the proposed definition includes "continuing" relationships, the agencies are considering whether to include inactive accounts or other relationships that are no longer continuing. **ICBA is concerned that including "inactive" accounts will complicate compliance**, especially at the outset. First, ICBA recommends that the agencies use the term "dormant" account as the one most commonly used in the industry. In evaluating whether these accounts should be included, the agencies must recognize that contact with the customer may be difficult. One typical element of a dormant account is that contact information for the customer is no longer current due to failure of

the customer to provide updated information. **Since many of these accounts have nominal value, ICBA recommends that a minimum dollar value be applied to exempt small value accounts**.

Many dormant accounts may be segregated from other accounts for various reasons or have special codes to identify them in bank computer systems. In part, this treatment is to alert bank staff that special steps may be necessary for these accounts. Therefore, it is important that the agencies recognize additional burden will be involved with creating parallel procedures for accounts that may already have adequate safeguards, making new procedures unnecessarily and needlessly burdensome. Therefore, before including inactive or dormant accounts, ICBA recommends that agencies survey existing practices to assess what safeguards are already in place for these accounts.

The agencies are contemplating defining an "inactive" account as one that has not had activity in two years. The statute specifically requires the agencies to consider procedures for accounts that have been inactive for more than two years when developing the guidelines, but **ICBA urges the agencies not to use two years as a hard and fast rule but as a guideline for inactive accounts**. However, since one of the underlying goals of the proposal is to allow banks the flexibility to tailor compliance to their own unique circumstances, **ICBA recommends that the agencies allow banks to use existing standards already used to determine whether an account is inactive**. In some cases it may be longer than two years and in others it may be less, but using existing definitions already in place will avoid confusion and conflicting requirements. For example, most states have unclaimed property statutes that define whether an account is inactive and banks should have the flexibility to use a comparable definition for compliance with this regulation. Similarly, bank operational systems may apply different standards for different types of accounts and defining whether an account is dormant or inactive will be different for checking, savings and time deposit accounts. Without this flexibility, banks will be confronted with varying definitions of "inactive" account, making it costly to program systems to track when an account becomes inactive for which requirement. In those rare instances where a bank does not have an existing standard to define when inactive accounts, two years could serve as a default provision.

Customer. As proposed, a customer would include both customers and account holders and would be broader than the definition used for existing interagency information security standards. A customer would be any "person," including individuals, partnerships, corporations, trusts, estates, cooperatives, associations, government or governmental subdivisions or agencies, or other entities.

ICBA finds that applying the scope of the role to business accounts may present unnecessary problems and burdens. While business accounts may be subject to identity theft, there is nothing to demonstrate that the problem is widespread or warrants coverage under these procedures. Tracking individual signers on a business account, as the proposal seems to imply would be required, would be extremely burdensome. Routine tracking of business account signers was considered and rejected

by the agencies as a requirement when the CIP rules were finalized.[8] It is important to recognize that there are other procedures and processes in place, especially those under the Bank Secrecy Act rules and regulations that would allow a bank to detect unusual or suspicious patterns of activity in business accounts. The impact of identity theft is greatest for individual consumers, and **ICBA recommends that the final rule's definition of customer be limited to individual consumers** absent some clear showing that the expansive definition in the proposal is warranted.

Identity Theft. Using the definition established by the FTC under the FACT Act, identity theft would be defined as "a fraud committed or attempted using the identifying information of another person without authority." At the time the FTC proposed this broad definition, ICBA recommended a more focused approach that did not include everyday fraud or account take-over but instead focused on instances when someone's identifying information was used without their knowledge.

ICBA continues to believe that applying an overly broad definition of identity theft is inappropriate. In fact, a broad definition that incorporates other types of fraud detracts from the focus on true identity theft and makes it more difficult to address the problem. For example, account takeover should not be included as identity theft because the actual account holder receives regular statements and account information that allows him or her to detect unusual patterns or activity in the account and take appropriate steps to stop the fraud. **Identity theft should be limited to instances where identifying information, including name, date-of-birth-, and Social Security Number, have been appropriated *without that person's knowledge* to open new accounts or conduct transactions without their awareness**.

Red Flags. As proposed, a "red flag" would be any pattern, practice or specific activity that indicates the possible risk of identity theft. For example, it would include instances of phishing or other breaches that might be a precursor to identity theft.

ICBA finds the proposed definition of a red flag overly broad. For example, phishing attempts have become a daily occurrence for users of e-mail. Most people have learned to delete the messages without responding. However, by including this as a potential red flag, banks would be constantly monitoring all accounts. Instead**, the definition of a red flag should be limited to instances where identity theft either has occurred or there is a substantial likelihood that account information has been compromised. ICBA believes that including any instance where there *might* be a possibility of identity theft is far too broad** and creates a distraction. Virtually each and every transaction could involve potential identity theft or fraud. By including *possible* identity theft, banks will need to undertake an identity theft assessment for every transaction rather than focusing resources where the risks are greatest. The final rule should use a risk-based approach that allows banks the flexibility to focus resources where there is the greatest risk of identity theft.

---

[8] If something else triggers enhanced scrutiny, then the bank should investigate further, but the final CIP rules leave that to the discretion of the bank on the premise that the bank is in the best position to know its own customer and assess whether enhanced due diligence is warranted.

Elements of the Program. The proposal would require each bank to develop a written program that includes reasonable policies and procedures to address the risk of identity theft; be designed to protect customers and the safety and soundness of the bank; address financial, operational, compliance, reputation and litigation risks; be appropriate to the bank's size and complexity and the nature and scope of its activities; and be able to take into account changing identity theft risks as they arise. Therefore, the Program would have to include steps for periodic review, including the risks and accounts covered.

ICBA supports including flexibility in the rule so that the requirements for the Program are not one-size-fits-all. Allowing individual banks to tailor the scope of the Program to their own unique circumstances is helpful and will allow community banks to focus resources where they are most appropriate and address the unique risks presented by their own individual operations. This is especially important for community banks, which are often better able to identify risks because they are more familiar with their own customer base and individual customers. However, **ICBA strongly urges the agencies to incorporate this same flexibility in examination procedures** used to measure compliance with the new rule. All too frequently, community banks report examiners fall back on a one-size-fits-all approach and undermine any flexibility that the agencies incorporated into a rule. Therefore, it is critical that this element be preserved in both the final rule and examination procedures.

Identity Theft Prevention and Mitigation. The program would have to include reasonable policies and procedures to prevent and mitigate identity theft in connection with opening new accounts as well as existing accounts. As proposed, banks might want to consider the following steps, depending on the degree of risk involved: monitoring accounts; contacting customers; changing passwords, security codes or other access devices for an account; reopening an account with a new account number; not opening a new account; closing an existing account; notifying law enforcement (and possibly filing a suspicious activity report (SAR)); or implementing credit limits. While banks would be required to verify the identity of persons opening accounts, compliance with existing customer identification program (CIP) procedures under the Patriot Act would be deemed to satisfy this requirement.[9]

ICBA does not believe it will be difficult for community banks to expand existing programs to incorporate the new steps to mitigate against identity theft. For example, many of the steps outlined as ways to mitigate the risk of identity theft are already included in existing procedures, such as information security programs or CIP. However, **ICBA recommends that the final rule clearly recognize that compliance with parallel requirements meet the compliance requirements of this rule**. It is equally important that the final rule – and subsequent examination procedures – acknowledge that the steps a bank takes to mitigate the risks of identity theft need not be segregated into separate policies and procedures but may be part of an overall fraud detection and deterrent program or part of existing procedures for information security or customer identification.

---

[9] While the CIP rules exclude certain customers and accounts, there would be no exclusions under the identity theft requirement.

Board of Directors & Senior Management. Under the proposal, the bank's board or an appropriate board committee would be required to approve the written Program. The board, appropriate committee or senior management also would be responsible for overseeing the Program. As part of this requirement, the proposal would require a compliance report to the board at least annually.

ICBA agrees that the board should be responsible for oversight of the Program and should be informed about the Program and its progress. However, the final rule should clearly specify that the board's responsibility is limited to oversight of the Program and not day-to-day operation. In order to have the needed flexibility to address the evolving threats of identity theft, bank senior management needs sufficient flexibility to adjust the program between board meetings. Moreover, there seems to be an increasing tendency to place increasing responsibility on bank boards of directors for managing daily activities of the bank. This increased responsibility – and liability – can make it increasingly difficult for banks to attract and retain competent and energetic board members. While the bank's board should be informed about and committed to the Program, it should not be responsible for the daily operation of the Program – and that should be clearly articulated in the final rule.

Proposed Red Flag Guidelines (Appendix J). The statute requires the agencies to identify specific examples that might indicate identity theft. The agencies have identified a list of 31 individual "red flags" identified through various sources, listed in Appendix J to the proposal. **Generally, the ICBA believes the outlined list of red flags is appropriate and provides banks with a useful tool. However, ICBA strongly urges the agencies to clearly articulate in the final rule that the list provided in the appendix is a set of *examples* and not a checklist.** It is important that the red flags be treated as examples or indicators of possible identity theft and not *de facto* evidence of identity theft. This is especially important since the risks associated with identity theft are constantly changing as criminals develop new and unique methods of attack. While the presence of a red flag might be indicative of identity theft, as with other suspicious activities, the bank should be in a position to investigate and make a final determination whether there is a problem.[10]

ICBA recommends that the agencies clarify that banks have flexibility when applying the list. While the proposal specifies that the list is not meant to be exhaustive, requiring each bank to have policies to supplement the list based on its own experience and additional guidance from the agencies, ICBA urges the agencies to provide in the final rule that the list should be applied in the same way as the bank conducts its risk assessment. In other words, a bank should be able to use the list as a set of examples but not be required to adhere to the entire list or to document whether each item on the list applies – or does not apply – to a particular category of account. To do so would be extremely and unnecessarily burdensome. Moreover, unless the final rule clearly permits banks to use the listed red flags as examples, there is a danger that examiners will treat the list as a checklist that must be completed by each bank for each type of account. This

[10] This should be similar to procedures specified in the BSA/AML Examination Manual for suspicious activity reporting.

defeats the purpose for developing the list and would interject a rigidity that would quickly make the list less useful, especially as forms of identity theft evolve. Just as it does when determining whether a particular activity is suspicious, a bank should be given flexibility to investigate a red flag to determine whether there is identity theft.[11]

ICBA Comments on Specific Red Flags. Several items included on the red flag list might also be due to normal activity. For example, item number 3 suggests that a spike in activity on a consumer report might indicate identity theft – but it could also indicate that a consumer has been shopping for credit. Item 10a and 10b would require banks to monitor for addresses and phone numbers associated with fraudulent accounts – but to create such a system would entail costs that far outweigh the limited benefits and consume resources unnecessarily. Item 12 suggests that identical addresses or phone numbers might indicate identity theft but members of the same household will have the same address and phone number, and to investigate this each time will be unnecessarily burdensome. Item 18b suggests that failure to make an initial payment on a new account might indicate identity theft – but it could also be due to any number of problems associated with a new account and the bank should be allowed to investigate and resolve the problem without being required to presume identity theft. In other instances, an incomplete application or inconsistent information might be due to typographical errors or the fact that the consumer did not have all the needed information when the application was completed. Since individual banks are in the best position to assess whether a problem is significant or not, each bank should be allowed to make that determination based on knowledge of all the facts and circumstances.

Card Issuers – Change of Address

The proposal would require companies that issue credit or debit cards to adopt specific procedures where a change of address is followed within a short period, generally the first 30 days, by a request for an additional or replacement card. The proposal would prevent the card issuer from honoring the request for the additional or replacement card unless it verifies the validity of the change-of-address. The card issuer could verify the request by: (a) notifying the cardholder of the request at the cardholder's former address and providing a means to promptly report incorrect address changes; (b) notifying the cardholder of the request by any means of communication that the cardholder and issuer had previously agreed to use; or (c) using other means to verify the validity of the address change. Any notice sent to the cardholder would have to be clear and conspicuous and separate from any regular correspondence with the cardholder.

Most community banks already have procedures in place to verify that a change of address request is legitimate. For example, some community banks require the request to be in writing and then the bank verifies the signature on the request against the customer's signature already on file with the bank. Other community banks restrict address change requests to those made in person at the bank. **ICBA recommends that**

[11] And, as with the procedures for SAR filing, examiners should be given clear instructions that, absent a showing of bad faith or willful negligence, the examiner should not substitute his or her judgment for that of the bank.

the final rule clearly incorporate flexibility that allows individual community banks to tailor their procedures for verifying the validity of an address change request to the bank's unique circumstances, including product offerings and geographic market. As long as the bank has developed policies and procedures that allow it to verify a change of address request, and as long as the procedures the bank adopts address the potential risks for that type of account, that should be sufficient. Examiners should not second guess the bank's procedures or impose unnecessary requirements.

Address Discrepancies

As required by section 315 of the FACT Act, the proposal would require banks to adopt reasonable policies and procedures for handling notices from consumer reporting agencies that an address provided by the bank "substantially differs" from the address on file with the consumer reporting agency. **ICBA generally agrees this is appropriate, but it is also important that the final rule clearly state that the requirement excludes minor typographical errors or minor discrepancies. ICBA also recommends that the agencies offer examples of what constitutes substantial differences** or what constitutes a minor difference not subject to the requirement. Absent a clear definition of what constitutes substantial difference, individual banks should be allowed to make that assessment, absent evidence of bad faith or willful neglect.

As proposed, a bank would have to provide the correct address to the credit reporting agency that notified the bank of the discrepancy once the bank can form a reasonable belief it knows the identity of the consumer;[12] if it has a continuing relationship with the consumer; *and* if it regularly furnishes information to that consumer reporting agency. Again, ICBA generally agrees that these are appropriate conditions. However, **ICBA recommends that the final rule clarify that the requirement to furnish the corrected information to the consumer reporting agency applies only if the bank provides that information to the consumer reporting agency *for that type of account.***

Timing. The bank would be required to provide the correct address to the consumer reporting agency with its regular reports during the reporting period that it opens a new account. For existing accounts, the bank must furnish the corrected address during the reporting period when it reasonably confirms the accuracy of the address. ICBA does not disagree with this requirement. However, **ICBA recommends that the final rule include sufficient flexibility to allow the bank to investigate the discrepancy**. Many existing regulations, such as the Federal Reserve's Truth-in-Lending Act rule, Regulation Z, provide sufficient time for a bank to conduct an investigation into a possible error,[13] and similar flexibility should be incorporated here, too.

Finally, **ICBA recommends that this particular element include a sufficient transition period to allow software vendors to update existing software programs** to

---

[12] Similar to the red flags proposal, a bank could satisfy this requirement if it complies with the Customer Identification Program rules of the Patriot Act,
[13] See, e.g., 12 CFR 226.13.

allow banks to provide the needed information to the consumer reporting agencies. Given other demands on software developers, ICBA recommends at least a two-year transition, although the agencies may want to consult with software providers for more accurate estimates of the time needed.

Regulatory Burden

The banking agencies estimate that it will initially take banks 25 hours to create an *Identity Theft Prevention Program*, four hours to prepare the annual report to the board and two hours to train staff on the Program.[14] They also estimate it will take card issuers four hours to develop policies and procedures to assess the validity of a change-of-address request. As noted above, the agencies believe that since banks already have programs for safeguarding customer information and for customer identification, this new requirement will "pose no further burden." Therefore, the times estimated are based on the *incremental* time needed to comply with this proposal.

ICBA finds the agencies' estimates for time to comply with the proposed rule's requirements insufficient. Most community banks estimate it will take much longer to comply – when they feel comfortable even trying to estimate how long it will take. The larger the bank and the more locations it has, the longer it will take to implement the requirements. Therefore, **ICBA strongly urges the agencies to increase the amount of time that banks will need to comply with these requirements**.

Community bankers estimate it is likely to take *at least* two to three times what is estimated to review the final rule, evaluate available supplemental information distributed by trade associations and others, analyze the rule against existing policies and procedures, develop and implement policies and procedures – including compliance and audit procedures, develop and schedule staff training. Larger community banks estimate it could require up to 100 hours and a minimum cost of $10,000 to $20,000. Even building on existing programs, ICBA finds the estimated timeframes unrealistic.

For example, the agencies estimate that it will only require an average of four hours to prepare the annual report on the Program for the board. While this might be adequate for smaller institutions with simple operations, ICBA does not believe it will adequately reflect the kind of analysis and information needed. It is not inconceivable that it might take a community bank up to 10 times as long to develop and prepare this report.

The estimate that it will only take two hours to train staff on the program is especially inadequate. Depending on the size of the institution and the number of

[14] The FTC estimates that low-risk entities may only need 20 minutes to develop and implement a Program with an annual burden of five minutes. ICBA believes that this estimate is extremely inadequate, since it will take low-risk entities much longer than 20 minutes to simply read and assess the requirements, let alone develop and implement a Program. As with the estimates for the amount of time it will takes banks to comply with the requirements, ICBA finds this estimate completely unrealistic.

locations and number of employees it has, it can take many times the estimated amount. For instance, one community banks estimates that it will take five to 10 hours to prepare the training program and an additional two hours to train each group of employees, resulting in well over 50 hours for training alone. Another community bank with 80 employees would plan to hold 2-hour training sessions for groups of 10 employees, requiring a minimum of 16 hours for training alone, excluding the amount of time needed to develop the training. Therefore, **ICBA strongly recommends that the estimated amount of time for training of the new requirements be substantially increased**.

Effective Date

Although the intention of the proposal is to provide banks with sufficient flexibility to tailor a Program to their own unique circumstances, ICBA recommends that the agencies incorporate sufficient time for banks to develop the necessary policies and procedures once a final rule is issued. **At a minimum, ICBA recommends the final rule permit a one-year transition period**.

Conclusion

One community banker commented that the red flags proposal was one of the most burdensome proposals he has seen in a long time. While ICBA believes it is useful to provide community banks with information that raises awareness about potential indicators of identity theft, the requirements of the proposal go far beyond what was mandated by Congress in the FACT Act. It is ironic that the agencies would issue such an extensive proposal at a time when they are simultaneously analyzing unnecessary burdens under a different Congressional mandate.[15] While identity theft is clearly a problem, ICBA believes that the proposal fails to recognize that banks have already taken steps for many years to detect and prevent fraud, including identity theft. The elements and burdens that would be imposed by the proposal if it is adopted without change will consume resources in both time and money that could be better allocated to detecting and stopping fraud. And, the breadth of the proposed definition of identity theft will incorporate all types of garden-variety frauds, detracting from efforts to stop true instances of identity theft.

ICBA commends the agencies for undertaking this difficult task to help bankers protect their customers from the serious problem of identity theft. However, it is extremely important that the final rule be sufficiently flexible and allow individual banks enough leeway to develop programs designed to address their own products, services, geographic markets and customer bases. Otherwise, the final rule will be too rigid to properly address the problem of identity theft.

[15] The Economic Growth and Regulatory Paperwork Reduction Act of 1996 (EGRPRA).

Thank you for the opportunity to comment. If you have any questions or would like additional information, please contact the undersigned by telephone at 202-659-8111 or by e-mail at robert.rowe@icba.org.

Sincerely,

Robert G. Rowe, III
Regulatory Counsel