

# The Case for Scoring To Meet Identity Fraud Prevention Program Requirements

ADAM ELLIOTT AND SANDRA FERRIAN

*The authors explain why identity risk scoring, which can accurately predict the risk of fraud, is an important tool in an Identity Theft Prevention Program.*

**F**or more than three decades, legislation of the financial services sector designed to combat criminal money laundering, terrorism and, more recently, to address identity theft, has required financial providers to implement procedures to track customer information. At the heart of this anti-money laundering, counter terrorism, and identity theft legislation is an underlying requirement of verifying the true identity of the customers. However, criminals seeking to evade information tracking and identity thieves have kept pace with technological improvements in identifying documentation relied upon to identify bank customers. Counterfeit identification and increased diversion of nonpublic identifying information traditionally used to verify customers has opened the door for an upsurge of identity theft. The relative ease of misrepresenting customer identifying information, combined with a culture of abundant “instant” credit, has resulted in legislation and regulations that

---

Adam Elliott is president of Minnesota-based ID Insight, a company that helps financial institutions reduce fraud through access-point intelligence. Sandra Ferrian is the company's general counsel.

require financial institutions to implement processes to verify customer information as part of identity theft prevention programs that will be required for financial services providers. The recent FACT Act regulations take the requirement of identifying customers one step further to require verification not only when an account is opened but also under circumstances that pose higher risk for identity theft. In situations where there is a significant risk of fraud, a customer identification practice that includes a statistical analysis of the risk of fraud as part of the customer identification process for the specific transaction request will assist the financial institution in meeting its regulatory mandates of being able to form a “reasonable belief” about the identity of the customer while providing information that is more predictive of the risk of fraud than most manual verification methods. In addition, statistical scoring of fraud risk can offer immediate, actionable decisions, and provide information about address discrepancies at a lower cost than other manual practices.

## **THE BANK SECRECY ACT**

In 1970, the Foreign Transactions Reporting Act, known as the Bank Secrecy Act (“BSA”),<sup>1</sup> provided the first regulation of bank practices aimed at curbing money laundering activities. The Bank Secrecy Act established record keeping and reporting requirements for individuals, banks,<sup>2</sup> and other financial institutions. Reporting data focused on identifying the customers undertaking targeted transactions. The Bank Secrecy Act requires that banks have a Customer Identification Program (“CIP”)<sup>3</sup> that is appropriate for their size and type of business. As part of the CIP, banks must use documentary or nondocumentary methods of identification to enable the bank to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer. Banks are required to conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider demographics of the customer, types of products offered, size and geography of the bank, and the

types of identification services available.<sup>4</sup> In addition, banks must provide a resolution of any substantive discrepancy discovered when verifying the identifying information obtained.<sup>5</sup>

## **THE USA PATRIOT ACT**

In response to the September 11, 2001, terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA PATRIOT Act”).<sup>6</sup> The USA PATRIOT Act required financial institutions to implement customer identification procedures and report certain types of transactions to facilitate tracking criminal financing of terrorism. Rules promulgated to implement the USA PATRIOT Act provided little specific guidance to methods of customer identification, other than to identify minimum specific information that should be verified when opening an account or credit instrument, such as name, address, and a tax identification number.<sup>7</sup> The method of identifying this information was left to the institution. The focus of the regulation is account opening, and monitoring of account changes is not part of the regulatory requirements. The effectiveness of the Bank Secrecy Act and the USA PATRIOT Act depends on the ability to accurately verify the financial services customer.

## **THE FACT ACT**

The rise of identity theft<sup>8</sup> gave rise to enactment of the Fair and Accurate Credit Transactions Act (“FACT Act”) of 2003,<sup>9</sup> which added several new sections and amended the Fair Credit Reporting Act of 1970,<sup>10</sup> including provisions related to customer verification under circumstances that could be indicative of fraudulent activities.<sup>11</sup> Section 114 of the FACT Act requires each financial institution or creditor to develop and implement a written Identity Theft Prevention Program (“Program”) to detect and prevent identity theft applicable to the opening of certain accounts or changes to certain existing accounts, and requires credit and debit card issuers to assess the validity of change of address notifications under certain circumstances. In addition, Section 315 of the FACT Act requires agencies charged with rule making to provide guidance regard-

ing reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy. The FACT Act provided little guidance as to what specific verification measures are required, leaving that to the agencies charged with promulgating the guidance and rules for those “red flag”<sup>12</sup> situations indicative of fraud.

The “Red Flag” guidelines and regulations required by the FACT Act have been published and compliance is mandated on November 1, 2008.<sup>13</sup> The guidelines and regulations that are required to be implemented are founded on recognized practices in identity theft. The regulations include rules as to the circumstances under which a financial institution must and should undertake verification, and guidelines as to what an appropriate Program must involve. The inclusion of guidelines is important as the changing nature of identity theft requires flexibility in response and prevention of identity theft.

These regulations require the financial institution to establish an Identity Theft Prevention Program, which is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or certain changes to any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.<sup>14</sup> The Program must be designed to detect and react to identity theft risks for the products offered by the institution.<sup>15</sup> Further, the rules require that the Program be “periodically” updated to reflect the financial institution’s “own experiences with identity theft, changes in methods of identity theft, changes in methods to detect, prevent and mitigate identity theft, changes in accounts that it offers or maintains, and changes in its business arrangements.”<sup>16</sup> To further drive home the importance of the Identity Theft Prevention Program, the final rule requires that the board of directors, or an appropriate committee, approve the Program, and they, or a member of senior management, have oversight obligations.<sup>17</sup> Compliance may be provided by a third-party provider so long as the financial institution maintains appropriate oversight.<sup>18</sup>

## REQUIRED VERIFICATION

The “Red Flag” regulations provide that verification is required under certain circumstances that involve a greater risk of fraud. For example, when a financial institution receives a credit report with an address discrepancy, it is now required to undertake an analysis that provides a “reasonable belief that a consumer report relates to the consumer about whom it has requested the report.”<sup>19</sup> In addition, when a card issuer receives a request to issue a credit card that is made within 30 days of a change of address, the issuer is required to undertake verification measures to form a “reasonable belief” that the address change is valid. To do so, the card issuer is required to have reasonable policies and practices, such as notifying the cardholder by the means agreed upon, permitting the cardholder to validate the address change and credit request, or for the issuer to otherwise assess the validity of the change of address.<sup>20</sup> Furthermore, the Program must take into account the risk of fraud for other types of transactions specific to the services offered, and must be periodically updated to include this information. Therefore, the Program will, if compliant, continue to provide insight into transactions or practices with increased risk of fraud, and may require validation for a variety of additional transactions.<sup>21</sup> The regulations leave open the potential of using third-party services to assist in establishing a reasonable belief about the validity of the requested transaction.<sup>22</sup>

Interagency guidelines offer assistance on the formulation and maintenance of a Program that satisfies the requirements of the “Red Flag” regulations.<sup>23</sup> The governed entities must include in their Programs relevant identity theft “Red Flags” from applicable supervisory guidance, their own experiences, and methods of identity theft that the entity had identified that reflect changes in identity theft risks.<sup>24</sup> The final version does not prescribe specific practices but relies on a risk-based, nonprescriptive approach regarding the identification of identity theft “red flags.”<sup>25</sup> The Agencies promulgating the rules describe their approach as broad enough to cover a wide variety of financial institutions and creditors that offer and maintain many different products and services, including the potential for medical identity theft for the purpose of obtaining

medical services.<sup>26</sup> Further, the rules require that the Identity Theft Prevention Program be “periodically” updated to reflect the financial institution’s “own experiences with identity theft, changes in methods of identity theft, changes in methods to detect, prevent and mitigate identity theft, changes in accounts that it offers or maintains, and changes in its business arrangements.”<sup>27</sup> The lack of specific methods that must be employed to validate subject transactions is designed to provide the flexibility to permit the financial services provider to adapt to rapidly changing practices and risks of identity theft.

## IDENTITY FRAUD PRACTICES

Assuring that the identity theft prevention program complies with the “Red Flag” regulations requires an understanding of identity fraud practices. In general, most identity fraud involves new account openings and/or account takeover. New account fraud occurs when the thief opens a new account in the victim’s name. According to the FTC’s 2006 Identity Theft Survey, approximately 1.8 million U.S. consumers were the victims of new account fraud. Once the identity thief has compromised the victim’s credentials, such as name, Social Security number, date of birth, or other identifying information, it is relatively easy to open a new account in the name of the victim, satisfying the customer identification program requirements of the Bank Secrecy Act. The element the thief will typically manipulate is the access points, that is, mailing address. Changing the address ensures that statements, credit cards, and purchased merchandise<sup>28</sup> will be delivered to the address listed on the credit application, and not the address of the victim.

When the credit issuer obtains the new account application, it is sent to a consumer reporting agency<sup>29</sup> (“CRA”) to determine credit eligibility. The CRA provides credit information, and, as applicable, information of the address discrepancy. The credit issuer then must determine whether to issue credit. Financial services providers report that in the new account opening process, approximately 20 to 40 percent of all creditworthy new applications have an address discrepancy, most of which are related to legitimate household moves. Prior to the “Red Flag” regulations, the

credit issuer needed only to decide whether to deny the credit pending verification, and risk losing the credit or sale opportunity until the identity of the customer can be verified, or grant the credit in the face of the address discrepancy. Because the overall incidence of fraud is typically low on transactions with an address discrepancy, the typical issuer would approve these transactions. Practices utilized to verify customers typically include documentary evidence, third-party database verification services, and authentication or “out-of-wallet” solutions, such as quizzing the applicant as to who holds their mortgage and the amount of the monthly payment. Documentary evidence practices, such as asking for a utility bill, involve time delays (and the potential loss of the relationship), cost, and often do not provide an assurance of the customer’s identification. Third-party database verification methods can assist in verifying the name at the address for a portion of the transactions, but provide no greater insight beyond this. In addition, “out-of-wallet” solutions can be feigned, and typically produce many false positives. The end result is a Program that falls short of its objective of identifying fraudulent activities. While these processes can be unreliable and costly, they would be considered “reasonable” under the law. A financial institution is not obligated to do more than satisfy compliance with its Identity Theft Prevention Program.

## **THE LEADING SOURCE OF IDENTITY THEFT**

Account takeover has exploded as the current leading source of identity theft. According to the FTC’s 2006 Identity Theft Survey, 6.5 million U.S. consumers reported misuse on an existing account, or account takeover. A common account takeover scheme in financial services is for the identity thief to request an address change from that of the victim to an address of which the identity thief has access. Historically, CIP programs did not focus on account address changes and there was no mandated verification of address change requests. Once the account address change was accomplished, the identity thief then requested new checks, debit cards, credit cards, or other credit authority. Once in hand, the identity thief is permitted to empty the accounts and utilize the credit obtained.

In the case of new account fraud or account takeover fraud, the thief will change the address to hide the fraud and receive credit, financial instruments, and documentation. In new account fraud or account takeover fraud, validating the address change is the key to preventing the fraud.

The validation requirements of the FACT Act regulations require the financial institution to form a “reasonable belief” as to the validity of the identity of the customer. How does the financial services provider form a “reasonable belief” of the identity of a customer? Documentary evidence, third-party verification, and “out of wallet” solutions have been the traditional methods of verifying customer data that are currently being used, but they are problematic as the sole method of verification. For example, documents can be easily forged. Even an ambitious teenager is able to create or obtain a photo identification with a fraudulent birth date. Utility or phone bills are also easily forged, or alternatively can be legitimately set up at the thief’s address with a fraudulent name. Also, each of these methods has a manual component that delays credit decisions, aggravates customers, and involves labor costs. These most common methods of customer validation, which meet the requirements of the Bank Secrecy Act and PATRIOT Act customer identification programs, have significant potential for fraud and provide little to alleviate the risk of identity fraud.

## **CONFIRMING IDENTIFYING INFORMATION**

Another method to form a reasonable belief of the identity of a customer is to use third-party databases to confirm identifying information. For example, if a consumer report indicates an address discrepancy, the financial institution may elect to check other third-party databases to determine if there is other evidence of the named consumer at the alternate address. Third-party databases are typically compiled from public information, such as U.S. Post Office records, phone directories, utility companies, consumer reporting agencies, or other public records or records available for purchase. If the customer identification inquiry is the result of an address discrepancy, there is a significant possibility that

third-party databases will provide the same address discrepancy as the credit report or other source of the discrepancy. Many common data sources are slow to update their databases, so they cannot be relied upon for recent mover information. However, identity thieves do indeed attempt to manipulate these databases by filing change of address forms with the Post Office, and taking other fraudulent steps to complete their crime. Address changes that can be verified through third-party databases have a higher likelihood of legitimacy, but not certainty, and addresses that cannot be verified may be legitimate, but further information is required to form a reasonable belief of the identity of the customer.

A more reliable method of validating customer information focuses not only on the third-party verification information but also on the address-related information to provide a fraud risk score. Address-related information includes critical demographics, such as the type of dwelling, ownership status, and market value. Looking at the previous address demographics, compared to the demographics of the address change, can show discrepancies that are predictive of identity theft. The logic is simple. Using just economic information, it is accepted that most address changes do not involve significant economic changes. In short, people move in predictable ways. Statistically significant changes, especially adverse changes, in income levels, neighborhood crime statistics, or changes in dwelling type correlate highly to identity theft. It is likely that the address change may not be that of the creditor, but rather someone else who may be an identity thief. When the analysis is extended to a variety of data points that can be correlated to the risk of fraud, an algorithm can be developed that will produce an actionable, decisive result — or score, that predicts the risk of fraud. For example, an address change from an owned home in rural Iowa to an urban residence 2,000 miles away that happens to be a vacant lot in a commercial area indicates a much higher incidence of fraud and identity theft. The score would reflect this high likelihood for fraud. Using data from a variety of financial service providers to validate additional statistical correlations between the risk of fraud and information derived from publicly available address-based data, empirical data shows that address information can be predictive of fraud.

## **CUSTOMER ADDRESS INFORMATION**

The scoring model utilizes customer address information provided by the subscribing financial services provider to obtain information about the risk of fraud associated with the address change, or address discrepancy, from public records and proprietary statistical analysis. The risk of fraud is quantified as a score provided to subscribing financial service providers, who then makes validation decisions based on the risk of fraud.<sup>30</sup> Blind analysis of data that includes known fraud undertaken by the provider suggests that the risk analysis is significantly more predictive of fraud than was actually identified by other manual processes or third-party database verification. It is logical that a method of evaluating the risk that an address is fraudulent that utilizes multiple data sources to assess the risk of fraud will be more predictive than a single data point verification method.

Using statistical analysis to analyze risk is not new in the financial services industry. Statistical analysis of risks associated with behavior changes can be predictive of fraud in credit card transactions. The Falcon product from Fair Isaac Corporation has been a standard fraud detection system for credit card transactions. Falcon examines differences in transactions to identify the risk of fraud. For example, if a consumer who always transacts in his home state of Tennessee, and never for more than \$500, suddenly makes a \$5,000 purchase from the Ukraine, Falcon identifies the transaction as high risk. Once the risk is identified, the card is blocked and the consumer is contacted to make sure that the potential transaction is not fraud.

As the provider of identity fraud risk scores broadens its own subscriber base and analyzes customer data including known identity fraud from a variety of subscribers, the service provider is able to enhance its knowledge base of statistical correlations and incorporate additional correlating metrics in its analysis. In this way, the predictive feature of the service keeps pace with trends in identity theft.

## **THE ROLE OF SCORING**

Assuming the validity of the statistical analysis to predict the risk of fraud, the issue is the role of scoring in an Identity Theft Prevention

Program. The FACT Act regulations require the credit issuer to form a “reasonable belief” of the identity of the customer. It cannot be an accident that the authors of the regulations selected “reasonable belief” as the standard of care. Legal case law has abundant references to “reasonable belief.” *Black’s Law Dictionary* defines “reasonable belief” as follows:

“Reasonable belief” or “probable cause” to make and arrest without a warrant exists when facts and circumstances within arresting officer’s knowledge and of which he had reasonably trustworthy information are sufficient in themselves to justify a man of average caution in belief that a felony has or been or is being committed. [references deleted] The words “reasonably believes” are used throughout the Restatement, Second, Torts to denote the fact that the actor believes that a given fact or combination of facts exists and that the circumstances which he knows or should know, are such as to cause a reasonable man so to believe.<sup>31</sup>

The definition of “reasonable belief” requires the actor to form the belief based on the facts and circumstances. This standard corresponds with the overall reading of the “Red Flag” regulations and guidelines, which requires that the Program utilize a risk-based analysis considering the types of products, demographics of the institution and its customers, and available verification information. A “reasonable belief” cannot be based on unreliable information that the financial provider knows, or should know, may not provide valid information about the identity of the customer. At the other end of the spectrum, “reasonable belief” does not require establishing customer identity to an absolute 100 percent certainty. In the face of a facts and circumstances analysis of what may constitute “reasonable belief,” the decision maker must use the methods that provide reliable verification.

The relative ease of obtaining the scoring information also contributes to the fact that it is a reasonable method of customer verification under the circumstances. Score-based solutions provide more immediate information about the likelihood of fraud than processes that require contacting the customer and waiting for information to be returned. In addition, if the finan-

cial provider verifies an address change when requested using the address score, it can immediately respond to credit card requests using the validated address.<sup>32</sup> In an environment of fierce competition for customer credit where delays in making credit decisions are costly, there is a significant value to the ability to obtain information about the likelihood of fraud without delay may be considered reasonable under the circumstances.

Credit providers and financial institutions that verify address changes and address discrepancies using address-scoring information are able to limit the number of applications that require further manual verification practices and make credit and account information almost immediately with scoring information which is highly predictive of fraud and identity theft. In the case of account openings and account address changes where the customer is not present, online scoring provides some immediate information upon which the financial services provider can form a reasonable belief about the identity of the customer and the validity of the proposed transaction. With the ease of use, ease of access response time, and other circumstantial factors, it is reasonable to use the method that is most predictive of fraud. Recognizing the inherent shortfalls of traditional methods of verifying information to form a reasonable belief of the identity of the customer, it may be far more “reasonable” to utilize fraud risk scores to determine whether to proceed with a transaction. Using address-based scored transaction information to form a reasonable belief about the validity of a transaction not only complies with the FACT Act “Red Flag” regulations but is also a valuable tool in complying with the customer identification program requirements of the Bank Secrecy Act, and can significantly reduce the risk of identity theft for the financial institution and its customers. From a compliance perspective, the financial services company is also able to easily document and audit its process, which is not the case when using manual processes.

Furthermore, the FACT Act guidelines require the Program be periodically updated to include additional red flag factors and to formulate and implement changes to address such changes.<sup>33</sup> The provider of the fraud risk score perpetually advances its knowledge base and incorporates analysis of relevant trends in its scoring algorithm. As the provider continues to examine fraud data from its subscribers to improve and validate the scoring

algorithm, it will be in a position to identify emerging trends and additional predictive factors and can incorporate this information in product offerings or for fraud practices that are not addressed by its products, to provide information from its broad base to subscribers. Most smaller financial institutions and small bank associations will not have adequate resources or data bases to maintain a Program that keeps pace with current trends in identity fraud. In addition, in the current economic environment, financial providers may want to take advantage of the research undertaken by third-party providers across a large segment of subscribers. While the use of a third-party provider does not completely eliminate the need to periodically assess fraud risks and improve an Identity Theft Prevention Program, a third-party provider that monitors volumes of data and seeks to improve its service by meeting the changing environment will be an important source of updated service and information.

## CONCLUSION

Identity risk scoring, which accurately predicts the risk of fraud, is an important tool in an Identity Theft Prevention Identification Program. Utilization of address-based fraud risk scoring for account openings and address changes has been shown to reduce the occurrence of fraud. The reduced risk of fraud resulting from the use of scored information establishes this as an acceptable method of validating information for purposes of compliance with “Red Flag” regulations and others. Scored information is a valuable source to form a “reasonable belief” of the validity of a transaction and should be an integral part of an Identity Theft Prevention Program, as well as Customer Identification Programs.

## NOTES

<sup>1</sup> 31 U.S.C. 5311 *et seq.*, 12 U.S.C. 1829b, and 1951 – 1959. See also 12 U.S.C. 1818(s) (federally insured depository institutions) and 12 U.S.C. 1786(q) (federally insured credit unions).

<sup>2</sup> Under the Bank Secrecy Act, as implemented by 31 C.F.R. 103.11, the term “bank” includes each agent, agency, branch, or office within the United States of commercial banks, savings and loan associations, thrift institutions,

credit unions, and foreign banks. The requirement to identify customers undertaking certain types of transactions and requiring records of financial transactions was extended to banks of all charters by the Money Laundering Control Act of 1986 and certain sections of the Federal Deposit Insurance Act (“FDI Act”), which sections apply equally to banks of all charters. The Money Laundering Control Act of 1986 precludes circumvention of the BSA requirements by imposing criminal liability on a person or financial institution that knowingly assists in the laundering of money, or that structures transactions to avoid reporting them. The 1986 statute directed banks to establish and maintain procedures reasonably designed to ensure and monitor compliance with the reporting and recordkeeping requirements of the BSA. As a result, on January 27, 1987, all federal banking agencies issued essentially similar regulations requiring banks to develop programs for BSA compliance. 12 U.S.C. 1818(s) and 1829(b).

<sup>3</sup> See 12 C.F.R. 208.63(b), 211.5(m), 211.24(j) (Board of Governors of the Federal Reserve System); 12 C.F.R. 326.8(b) (Federal Deposit Insurance Corporation); 12 C.F.R. 748.2(b) (National Credit Union Administration); 12 C.F.R. 21.21 (Office of the Comptroller of the Currency); 12 C.F.R. 563.177(b) (Office of Thrift Supervision); and 31 C.F.R. 103.121 (FinCEN).

<sup>4</sup> *Bank Secrecy Act/Anti Money Laundering Examination Manual*, Federal Financial Examinations Council, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, and State Liaison Committee, 2007.

<sup>5</sup> *Id.*

<sup>6</sup> Public Law 107-56.

<sup>7</sup> 68 C.F.R. 103.121 (b) (2) identifies the elements of a mandated customer identification program (CIP): “The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. The procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer. These procedures must be based on the bank’s assessment of the relevant risks, including those presented by the various types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the various types of identifying information available, and the bank’s size, location, and customer base. At a minimum, these procedures must contain the elements described in this paragraph....”

<sup>8</sup> Section 111 of the FACT Act defines “identity theft” as “a fraud committed using the identifying information of another person, subject to such further definition as the [Federal Trade] Commission may prescribe, by regulation.” 15 U.S.C. 1681a(q)(3).

<sup>9</sup> Pub. L. 108–159.

<sup>10</sup> 15 U.S.C. 1681 et seq.

<sup>11</sup> The FACT Act required establishment of guidelines and regulations to identify possible risks to account holders and for the following specific situations determined to be at greater risk for identity fraud (“red flags”):

[I]f a card issuer receives notification of a change of address for an existing account, and within a short period of time (during at least the first 30 days after such notification is received) receives a request for an additional or replacement card for the same account, the card issuer may not issue the additional or replacement card, unless the card issuer, in accordance with reasonable policies and procedures —

(i) notifies the cardholder of the request at the former address of the cardholder and provides to the cardholder a means of promptly reporting incorrect address changes;

(ii) notifies the cardholder of the request by such other means of communication as the cardholder and the card issuer previously agreed to; or

(iii) uses other means of assessing the validity of the change of address, in accordance with reasonable policies and procedures established by the card issuer in accordance with the regulations prescribed under subparagraph (B).

(2) Criteria

(A) *In general*. In developing the guidelines required by paragraph (1)(A), the agencies described in paragraph (1) shall identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft.

(B) *Inactive accounts*. In developing the guidelines required by paragraph (1)(A), the agencies described in paragraph (1) shall consider including reasonable guidelines providing that when a transaction occurs with respect to a credit or deposit account that has been inactive for more than 2 years, the creditor or financial institution shall follow reasonable policies and procedures that provide for notice to be given to a consumer in a manner reason-

ably designed to reduce the likelihood of identity theft with respect to such account.

(3) *Consistency with verification requirements.* Guidelines established pursuant to paragraph (1) shall not be inconsistent with the policies and procedures required under section 5318(1) of title 31, United States Code.

<sup>12</sup> 72 Fed. Reg. 63772-74 (11/09/07), Subpart J, §41.90 (b)(9) definitions defines the term as follows: “*Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.”

<sup>13</sup> 72 Fed. Reg. 63772-74 (11/09/07), Subpart J.

<sup>14</sup> 72 Fed. Reg. 63772-74 (11/09/07)Subpart J.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> 72 Fed. Reg. 63772-74 (11/09/07), Subpart J, See also Joint comments of the Department of the Treasury, Office of the Comptroller of the Currency, Federal Reserve System,, Federal Deposit Insurance Corporation, Department of the Treasurer, Office of Thrift Supervision, National Credit Union Administration, and Federal Trade Commission, Section by Section comments, § \_\_.90(d)(2)(iv) Element IV of the Program: Updating the Program.

<sup>18</sup> 72 Fed. Reg. 63772-74 (11/09/07), Subpart J.

<sup>19</sup> 72 Fed. Reg. 63772-74 (11/09/07), Subpart I.

<sup>20</sup> 72 Fed. Reg. 63772-74 (11/09/07), Subpart J, §\_\_.91.

<sup>21</sup> For example, issuers of Internet credit may find greater risk of fraud with transactions a “ship to” address that differs from the address on the credit billing statement, warranting validation of the credit holder and recipient identity.

<sup>22</sup> 72 Fed. Reg. 63772-74 (11/09/07), Subpart J requires the financial services provider to “[e]xercise appropriate and effective oversight of service provider arrangements.”

<sup>23</sup> 72 Fed. Reg. 63772-74 (11/09/07), Appendix J.

<sup>24</sup> 72 Fed. Reg. 63772-74 (11/09/07), Appendix J (II)(b).

<sup>25</sup> 72 Fed. Reg. 63772-74 (11/09/07), Appendix J.

<sup>26</sup> 72 Fed. Reg. 63772-74 (11/09/07), Section \_\_.90(d)(2)(i) Element I of the Program: Identification of Red Flags.

<sup>27</sup> Joint comments of the Department of the Treasury, Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit

Insurance Corporation, Department of the Treasurer, , Office off Thrift Supervision, National Credit Union Administration, and Federal Trade Commission, Section by Section comments, § \_\_.90(d)(2)(iv) Element IV of the Program: Updating the Program.

<sup>28</sup> Where billing address and the “ship to” address differ, certain merchants may seek additional verification of customer identity. Eliminating any address discrepancy reduces the risk that such transactions will be flagged.

<sup>29</sup> 15 U.S.C. 1681(a)(f) provides: “The term ‘consumer reporting agency’ means any person which, for monetary fees, dues, or on a cooperative non-profit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.”

<sup>30</sup> The financial services provider will likely define the threshold score, indicative of the risk of fraud, for which accounts or credit will be approved, and either rejecting other high risk scored applications or leaving open the opportunity for applicants with scores predicting a higher risk of fraud to provide other verifying information.

<sup>31</sup> Black’s Law Dictionary, 8th Edition (2004).

<sup>32</sup> 72 Fed. Reg. 63772-74 (11/09/07), Subpart J, provides in part:

*Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

<sup>33</sup> 72 Fed. Reg. 63772-74 (11/09/07) Section \_\_.90(d)(2)(iv).