

Waving the Red Flag: Rules for Reducing Identity Theft¹

by **M. E. Kabay, PhD, CISSP-ISSMP**
Associate Professor, Information Assurance
Norwich University, Northfield VT

Proposed Rulemaking Against ID Theft

In July 2006 a consortium of US federal agencies published a Notice of Proposed Rulemaking (NPRM) to help protect customers of banks and other financial institutions against identity (ID) theft.²

The agencies included the Board Of Governors of the Federal Reserve System

Federal Deposit Insurance Corporation, Federal Trade Commission, National Credit Union Administration, Office of the Comptroller of the Currency and Office of Thrift Supervision.

The press release described the NPRM as follows:

The regulations that the agencies are jointly proposing would require each financial institution and creditor to develop and implement an identity theft prevention program that includes policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts. The proposed regulations include guidelines listing patterns, practices, and specific forms of activity that should raise a "red flag" signaling a possible risk of identity theft. Under the proposed regulations, an identity theft prevention program established by a financial institution or creditor would have to include policies and procedures for detecting any "red flag" relevant to its operations and implementing a mitigation strategy appropriate for the level of risk.

The proposed regulations also would require credit and debit card issuers to develop policies and procedures to assess the validity of a request for a change of address followed closely by a request for an additional or replacement card.

Additional proposed regulations would require users of consumer reports to develop reasonable policies and procedures that they must apply when they receive a notice of address discrepancy from a consumer reporting agency.

¹ Originally published as a series of three articles in Network World Security Strategies in 2007:

- Proposed rulemaking against identity theft
< <http://www.networkworld.com/newsletters/sec/2007/0319sec1.html> >
- The people's flag is deepest red
< <http://www.networkworld.com/newsletters/sec/2007/0319sec2.html> >
- Waving a red flag < <http://www.networkworld.com/newsletters/sec/2007/0326sec1.html> >

² < <http://www.fdic.gov/news/news/press/2006/pr06071.html> >

Rules for Reducing ID Theft

The report was published in three PDF files which, for reasons best known to the federal agencies involved, did not include any usable text – they are scanned from the original double-spaced paper NPRM.

The People's Flag is Deepest Red

The NPRM included a list of warning signs (“red flags”) of ID theft that financial institutions should act on to prevent ID theft.

The specific red flags are listed in Appendix J (pp 111-114) of the NPRM. The 31 warning signs including the following highlights (I am summarizing):

- Information from a consumer reporting agency
 - Fraud alert
 - Notice of address discrepancy
 - Pattern of activity inconsistent with history and usual activity of applicant or customer
 - Closure of an account for cause or abuse of privileges
- Documentary identification inconsistencies (forgeries, bad photos, wrong information)
- Personal information inconsistencies
 - Addresses don't match
 - Inconsistent Social Security Number versus date range
 - Correlation with known frauds
 - Fictitious addresses or mail drops
 - Bad phone numbers or answering services
 - Incomplete applications
- Address changes
 - Immediate change of address after establishing account
 - Undeliverable mail despite continued activity
- Anomalous use of the account
 - Bulk purchases of easily-fenced goods (TVs, jewelry etc.)
 - Failure to make payments (or to pay after first payment)

Rules for Reducing ID Theft

- Changes in payment patterns
- Major change in spending patterns
- Sudden use of a formerly-inactive account
- Notice from customer or others
 - Observed fraud
 - Failure to receive statements
 - Notification of successful phishing attacks
 - E-mail from phishing attacks returned to actual institution
- Other red flags
 - “The name of an employee of the financial institution or creditor has been added as an authorized user on the account.”
 - “An employee has accessed or downloaded an unusually large number of customer account records.”
 - “The financial institution or creditor detects attempts to access a customer’s account by unauthorized persons.”
 - “The financial institution or creditor detects or is informed of unauthorized access to a customer’s personal information.”
 - “There are unusually frequent and large check orders. . . .”
 - “The person opening an account or the customer is unable to lift a credit freeze placed on his or her consumer report.”

These guidelines are useful not only for financial institutions: they also illustrate many principles of normal operations security (OPSEC). Being sensitive to anomalous behavior is important not only for normal security but also for resource management. Look for outliers in resource utilization, outliers in the first derivative (growth rates) of such utilization and in the second derivative (changes in slope) as well.

Waving a Red Flag

There have been spirited comments in response to the NPRM published on the Federal Reserve Web site.³

Some of the early comments were from individuals at small banks; in some cases, the banking staff appeared to believe that repeating emotional expressions from multiple employees of a single bank would carry weight with the regulators. These repetitive comments were along the lines of “Financial institutions are absurdly overburdened” and were devoid of any substantiating evidence or argument. Some of the contributions were flatly unprofessional; representing expletives with punctuation marks is not a good idea for any professional at any time – and especially not when his comments will be published on a government Web site for anyone to inspect. Do people not grasp that their comments are to be made public?

In the MSIA program at Norwich University, we require students to participate in online discussions; the *Student Handbook* specifically warns, “Student discussion contributions are graded on the basis of research, articulation of rational arguments, and contributions to the class’s knowledge and understanding of the topics under discussion. Unsubstantiated opinions devoid of analysis or explanation are tolerated but not rewarded.”⁴ I wish that a similar warning were posted on all requests for comment.

Despite the agitated pawing and snorting of some of the respondents reacting to red flags, some of the comments, especially those prepared by various associations of bankers, had substantive contributions to the discussion. For example, Attorney Pat Caldwell, writing on behalf of BancorpSouth wrote a thoughtful analysis⁵ that emphasized the dangers of duplication and overlap of the proposed rules with existing regulations such as elements of the Gramm-Leach-Bliley Act (GLBA) and of the U.S.A.P.A.T.R.I.O.T. Act. In addition, the attorney raises the question of how to meet the need for interference with fraud while preserving adequate customer service.

The American Bankers Association wrote in their thoughtful response,

“[Although] the Agencies state that the proposed Regulation is intended to be flexible and reflect a risk-based approach, we conclude that the proposed regulatory language in many cases falls short of these stated intentions. Instead, we believe that the proposal runs a high risk of creating an artificial, stagnant, mandatory checklist regime that will not effectively advance the goals of detecting and preventing identity theft and fraud. We fear that unless these shortcomings are addressed, the result will be a diversion of resources from effective detection, investigation, and corrective action and will necessitate wasteful expenditure on burdensome, paperwork-laden compliance exercises. Bankers’ attention will be drawn into wasteful but obligatory drills to justify each judgment call made under a good faith effort to defeat identity thieves and fraudsters.”⁶

³ The comments were no longer online at the original URL at the time of editing in August 2009.

⁴ < http://www.mekabay.com/msia/MSIA_Student_Handbook.pdf >

⁵ < http://www.federalreserve.gov/SECRS/2006/September/20060919/R-1255/R-1255_25_1.pdf >

⁶ < http://www.federalreserve.gov/SECRS/2006/October/20061012/R-1255/R-1255_26_1.pdf >

Rules for Reducing ID Theft

They strongly urged changes, including particularly, “Regulate by objective, not prescription” and “Recognize that risk-based considerations work best as guidance and allow for appropriate judgment, rather than rely on fixed rules.”

The Missouri Bankers Association wrote,

“[W]e believe that the proposal runs a high risk of creating an artificial, stagnant, mandatory checklist regime that will not effectively advance the goals of detecting and preventing identity theft and fraud. We fear that unless these shortcomings are addressed, the result will be a diversion of resources from effective detection, investigation, and corrective action and will necessitate wasteful expenditure on burdensome, paperwork-laden compliance exercises. Bankers’ attention will be drawn into wasteful but obligatory drills to justify each judgment call made under a good faith effort to defeat identity thieves and fraudsters.”⁷

The Massachusetts Bankers Association brief included this interesting comment:

“In addition, financial institutions will incur costs to re-design identity theft and fraud programs into packages that fit into the regulatory regime examiners expect. As we’ve noted, many identity theft and fraud prevention efforts are integrated throughout the institution. An institution may be extremely adept at preventing ID theft, however if a program is not in place that has all of the required regulatory paperwork justifying each and every element contained in the regulation, the bank could come under regulatory scrutiny and criticism. Consequently, ID theft prevention will actually become less risk-based at some institutions.”⁸

Frequently Asked Questions

The Federal Reserve Board published a document entitled “Frequently Asked Questions: Identity Theft Red Flags and Address Discrepancies” which was updated in June 2009 as of this writing.⁹ This FAQ has the following structure:

- I. General FAQs
- II. Identity Theft Red Flags (Red Flags Rules and Guidelines)
 - A. Scope
 - B. Definitions
 - C. Establishment of an Identity Theft Prevention Program (“Program”)
 - D. Elements of the Program
 - Detect Red Flags
 - Respond appropriately to Red Flags detected

⁷ < http://www.federalreserve.gov/SECRS/2006/October/20061005/R-1255/R-1255_28_1.pdf >

⁸ < http://www.federalreserve.gov/SECRS/2006/October/20061012/R-1255/R-1255_33_1.pdf >

⁹ < <http://www.federalreserve.gov/newsevents/press/bcreg/bcreg20090611a1.pdf> >

Rules for Reducing ID Theft

- E. Administration of the Program
- F. Examples of Red Flags
- III. Duties of Card Issuers Regarding Changes of Address (Card Issuers' Rules)
- IV. Duties of Users Regarding Address Discrepancies (Address Discrepancy Rules)

