The American Financial System's Identity Problem

April 16, 2014

Quality Control Systems Corporation

Copyright © 2014 by Quality Control Systems Corp. All rights reserved.

The United States relies on the Social Security Number (SSN) as its de facto national identification number. What began as an account number in a federally administered "old-age benefit" retirement program is now deeply embedded throughout the public and private sectors. Usage of the SSN is widespread because it is both expedient and efficient. Nevertheless, individuals and financial institutions (FIs) are exposed to significant losses when a prospective new customer's SSN is not validated at account inception. Because inexpensive validation of SSNs can be performed without entanglement in privacy, regulatory, or security issues, many of these losses are neither inevitable nor acceptable.

Our Growing Identity Crisis

- According to the FBI's Financial Institution Fraud and Failure Report, 2006-2007, "For the period of April 1, 1996, through September 30, 2007, the FBI received 846,113 Suspicious Activity Reports (SARs) for criminal activity related to check fraud, check kiting, counterfeit checks, counterfeit negotiable instruments, and mortgage loan fraud. These fraudulent activities accounted for 27 percent of the 3,186,213 SARs filed by U.S. financial institutions (excluding Bank Secrecy Act violations), and equaled more than $21.4 billion in losses" (Reference 1).

- The Social Security Administration (SSA) reported in 2004 (Reference 2) that its earnings suspense account had $420 billion of collected FICA payments with mismatched SSNs and names. By October, 2007 the account had grown to $661 billion (Reference 3). This phenomenon may be fueled in part by FICA tax payments from undocumented workers and their employers which cannot be linked to valid SSNs with matching names (Reference 4).

- Since 1936 the SSN has demonstrated a relentless functionality creep through the accounting systems of U.S. financial institutions. FIs are generally required by law to report the use of the number and SSNs are almost always used as key field identifiers in these systems. However, in the absence of an effective procedural standard to check the validity of SSNs, the fraudulent usage of SSNs has become absurdly high.

Grant D. Ashley, Assistant Director of the FBI's Criminal Investigative Division testified to Congress in 2002 that, "Possession of someone else's Social Security Number is key to laying the groundwork to take over someone's identity and obtain a driver's license, loans, credit cards, cars, and merchandise. It is also key to taking over an individual's existing account and wiring money from the account, charging expenses to an existing credit line, writing checks on the account or simply withdrawing money (Reference 5)."

The planned use of biometric data to combat identity fraud will likely bring irresistible pressure to merge these data throughout FI and government record systems. In many instances, the easily foreseeable linkage of Person A's biometric data with Person B's bank accounts and SSN will surely be based, in part, on fraudulent and mistaken SSNs. Adding identity safeguards to biometric databases does not address the existing identity record problems. These facts give pause to anyone familiar with the absence of an effective industry identity control standard in an era of securitization.

Based on our experience testing records with SSNs over two decades, we have found that many organizations have a misplaced faith in the integrity of SSNs in their records. This faith is misplaced because it does not rest on written standards for testing these records systems, much less on the results from actual tests. Resolving these problems requires standards to be developed, maintained, and enforced at the highest levels of organizational management.

The Validation Standard: Tackling America's Identity Problem

The reluctance of the industry to strengthen validation at account inception may be a result of the unmanageable cost of third-party services that charge on a per-inquiry basis. However, an inexpensive and efficient internal application, which validates SSNs and red flags those that should be questioned, is very easy to implement without becoming mired in privacy issues or regulatory requirements.

Fraudulent transactions using SSNs are easy to expose when the perpetrator uses an SSN that: 1) has never been issued by the Social Security Administration, or 2) was issued only before the perpetrator's claimed date of birth, or 3) is known to have been issued to a person who is deceased. For applications involving use of an SSN at some time in the past, it is also possible to identify a fourth category: SSNs known to have been issued only after a perpetrator has fraudulently used the number. Identifying SSNs used in these four categories is known as Social Security Number validation.

Databases that support validation can be quite compact and are easily maintained internally because it is not necessary for the databases to contain names or any other information about individuals. When used consistently at account inception, the technique of Social Security Number validation provides a real measure of protection for customers of financial institutions against identity theft.

The first line of defense against identity fraud and mounting fraud losses should be due diligence performed internally to validate SSNs at account inception. This can be established securely and affordably across the enterprise. Such a system will effectively red flag many fraudulent, mistaken, or forgotten SSNs. Unfortunately, this procedure is frequently overlooked in a rush to assess credit worthiness, making identity validation secondary to customer profiling. We believe this practice puts the cart before the horse. First, we need to establish if the horse is really the thoroughbred he or she purports to be.

Validating SSNs not only serves as an effective means to fight fraud losses but also to clean up databases full of miscoded, mistaken, and misused SSNs (Reference 6). This goal takes on increased importance given the movement toward linkage of biometric data with financial accounting data containing SSNs.

SSN Verification through the IRS Taxpayer Identification Number (TIN) Matching Program

Many institutions (and their agents) who pay certain income subject to backup withholding provisions of the Internal Revenue Service code may check Taxpayer Identification Numbers, including SSNs, through the IRS TIN Matching Program. Partly because of cumbersome, regulatory requirements that limit users to an identified pool, TIN matching is typically performed after an account is already established, often by batch processing. This practice has many undesirable consequences for erroneous SSNs that have not been validated first.

At account inception, we recommend validating the Social Security Number before using TIN matching and while the customer is present. This avoids many simple data entry errors or misremembered numbers that should be fixed before the numbers become an indelible part of the account records and long before incurring a B notice from the IRS that will require record retrieval and additional customer contact to investigate and correct.

Consent-Based SSN Verification

Social Security Numbers can also be verified directly with the Social Security Administration using its Consent-Based SSN Verification (CBSV) Service. As with TIN matching, we recommend validating the numbers first to avoid simple errors that can be easily fixed before incurring the very high cost of CBSV.

Combined with the added compliance burdens for paperwork and audit requirements, the cost of CBSV is a considerable barrier to direct SSN verification with the SSA for most FIs. The price of verifying SSNs directly has actually risen in the recent past from 56 cents to $5.00 per verification request (Reference 7). For the foreseeable future, the proposed procedure we recommend for SSN validation will remain a much lower cost, yet very effective alternative (Reference 8).

Recommendations for Standards at Account Inception

We recommend the Financial Industry adopt a new standard at account inception to validate new customers' SSNs.

Step 1: A strong Customer Identification Program (CIP) requires that the prospective customer's SSN be validated against a table of numbers that have actually been issued on a date that is consistent with the customer's age as well as the date the SSN is used or is claimed to have been issued. To be most effective, such tables should include the dates of issuance of SSN area and group numbers (the first five digits of the SSN) since the beginning of the social security program.

Step 2: If the SSN passes Step 1, check the claimed SSN against SSNs issued to persons now believed by SSA to be deceased. These SSNs are compiled in SSA's readily and cheaply available Death Master File.

Step 3: Follow-up verification with either the IRS or SSA is only appropriate after an SSN has passed validation and cleared the Death Master File match test. The advent of biometric identification technologies makes this measure highly advisable to avoid erroneous record matching with biometric data. However, verification of SSNs that haven't been validated is inefficient, wasteful, and risky. If quick and inexpensive validation at account inception shows an SSN can't have been issued by the SSA or doesn't fit a customer's claimed date of birth or employment history, it is self-defeating to spend more time and more money to see if the number can be verified by back-end processing.

Cleaning Up Records for Existing Customers

When an institution has not previously required SSN validation in its CIP, we also recommend validation testing for all customers' SSNs. This is a best practice solution to restore database integrity – especially in view of the potential risks of linking biometric information to existing records using unproven SSNs.

Summary

Despite all of its drawbacks, the SSN will certainly continue to play an important role in the determination of personal identity long into the future. This is because – in principle – a Social Security Number is a nearly universal, unique, and invariant form of personal identification. To replace such a widely used identifier would be cost prohibitive.

It is also too expensive to continue to ignore those losses to fraud that can be simply and inexpensively stopped cold with an integrated application across the enterprise to validate a Social Security Number.

Benefits of Establishing the SSN Validation Standard

- Identity theft would be significantly reduced. Tracking and publicizing the results would be invaluable to the FI's public relations objectives.

- As fraud loss is reduced, the FI will be in a position to become more competitive with new products and services to attract new customers.

- Account records reflecting customers with apparent multiple SSNs will be steadily resolved.
- As SSN validation becomes a standard across the industry, the trusted "bank" image will be enhanced.

References

1) U.S. Federal Bureau of Investigation, "Financial Institution Fraud and Failure Report Fiscal Years (FY) 2006 and 2007," Uniform Resource Locator: <http://www.fbi.gov/stats-services/publications/fiff_06-07/fiff_06-07>, accessed October 20, 2010.

2) Hearing Before the Subcommittee on Oversight and Subcommittee on Social Security of the Committee on Ways and Means, U.S. House of Representatives, One Hundred Eighth Congress, Second Session, March 20, 2004, "Hughton and Shaw Joint Hearing on Social Security Number and Individual Taxpayer Identification Number Mismatches and Misuse," Uniform Resource Locator: <www.ssa.gov/legislation/hearings/HRpt_031004.pdf>, accessed October 24, 2010.

3) Office of Retirement and Disability Policy, U.S. Social Security Administration, "Social Security Administration's Master Earnings File: Background Information," Uniform Resource Locator: <http://137.200.4.16/policy/docs/ssb/v69n3/v69n3p29.html>, accessed October 24, 2010.

4) Office of the Inspector General, U.S. Social Security Administration, "Employers with the Most Suspended Wage Items in the 5-Year Period 1997 through 2001," Uniform Resource Locator: <www.ssa.gov/oig/ADOBEPDF/A-03-03-13048.pdf>, accessed October 18, 2010.

5) Grant D. Ashley, Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation, "Testimony Before the House Ways and Means Committee," Washington, DC, September 19, 2002, Uniform Resource Locator: <http://www.fbi.gov/news/testimony/preserving-the-integrity-of-social-security-numbers-and-preventing-their-misuse-by-terrorist-and-identity-thieves>, accessed October 20, 2010.

6) Bob Sullivan, "The Secret List of ID Theft Victims," MSNBC.com, Uniform Resource Locator: <http://www.msnbc.msn.com/id/6814673/>, accessed October 12, 2010.

7) Social Security Online, U.S. Social Security Administration, "Consent Based Social Security Number Verification Service (CBSV)," Uniform Resource Locator, <http://www.ssa.gov/cbsv/>, accessed October 25, 2010.

8) Quality Control Systems Corp., "Simulated Performance of a Technique for Social Security Number Validation in Customer Identification Programs," September 2, 2010, Uniform Resource Locator, <http://quality-control.us/fraud_detection_simulations.pdf>, accessed September 2, 2010.

Additional, related information is available on our website through these links:

Fraud Detection and Identity Validation with SecureID™ – "The best place to deploy your anti-fraud defense is to catch the offender at the door..."

Simulation Studies of Social Security Number Validation – "... This simple technique of Social Security Number validation is highly recommended for Customer Identification Programs, particularly at the time of account inception..."

"Exaggerated" Deaths in SSA's Death Master File – "... Since the 1930s, deaths of social security number holders have been reported to the Social Security Administration (SSA)."

Randomized Assignment of Social Security Numbers – "The randomized assignment of Social Security Numbers (SSNs) by the Social Security Administration (SSA) beginning in June, 2011 introduces some important changes..."

Contact Information

For more information, contact Randy Whitfield at Quality Control Systems Corp, 410-923-2411. Randy's email address is:
randy@quality-control.us