

Piggy-Back Identities

How can your credit union mitigate the risk that your member will present you with someone else's Social Security number as they apply for a loan?

By Lisa Hochgraf

August 2010

If someone doesn't like their credit history these days, it's surprisingly easy for them to buy themselves an alternate Social Security number that links to a better score.

In fact, Jim McCain told attendees of a recent CUES Webinar that when he googled for "credit profile number," a term given by potential fraudsters to a nine-digit number "that has the same genetic makeup as a Social Security number," he got hundreds of hits, including one ad that promised such things as: "Numbers are clean and ready to be used." "We guarantee no one else is using the CPNs." "We'll validate as being issued by the Social Security Administration." And, "We guarantee that you or your clients will be able to start new profiles."

One of the greatest risks that credit unions face, McCain told attendees of "The Hidden Threat: The Integrity of the Social Security Number," is making sure real identifiers for the member you are serving are being presented.

McCain, certified trainer and general manager of [Computer Information Development LLC](#), Arcadia, Calif., said synthetic name fraud—in which an identity is fully or partially fabricated—is not new, but it is on the rise. When this type of crime is committed, the fraudster might provide his real name, date of birth and address, and someone else's Social Security number—someone with a way better credit score than the fraudster's.

"This fraud might be perpetrated by a relative," McCain said, "but there are businesses out there selling these Social Security numbers, too."

During his presentation, McCain described elements of the current environment that support the rise of this type of fraud, and suggested a key way to mitigate this risk for your credit union and its members.

Rising Threat

According to a 2007 Federal Trade Commission study cited by McCain, there are tens of millions more credit profiles than there are consumers. How did this happen?

"When the Social Security Act was created, the government never intended the Social Security number to be an identifier," McCain said. "Now it's the primary link to address, date of birth and name information."

Fraudsters are smart about how Social Security numbers are generated and this helps them find groups of numbers they can use or sell. For example, a list of "high group numbers" (the middle two numbers in a Social Security number) is issued every month by the Social Security Administration. This is a good starting place, according to McCain. Then, such Internet sites as [ssnvalidator.com](#) and [usinfosearch.com](#) can be used to confirm whether the fraudster's guess at a full Social Security number is in fact valid.

According to a Carnegie Mellon University study cited by McCain, Web users have a one in 10 chance of getting a valid Social Security number on one of these sites simply in guessing.

Information issued by "the Social Security Administration and the Internet provide the platform for those (fraudsters) to learn how to decode a Social Security number and how to use it in ways not in your best interest," McCain said. "These sites allow anyone to go to them and put in Social Security numbers and see if those are in the range of those issued by the Social Security Administration."

Many times fraudsters will present a child's Social Security number, McCain said. That's because parents often elect to get a Social Security number for their child in the hospital, as part of the Social Security Administration's "Enumeration at Birth" program. These numbers appeal to fraudsters not only because they are valid, but also because they have room for someone else to build a credit history on them.

So how does this apply to credit unions?

"Lenders don't understand that when they pay money to go through a service (for identity verification that) they may be receiving false information," McCain said, noting that every time a fraudulent Social Security number is

added to the credit reporting systems with someone's correct name, address and date of birth, another credit profile is created. "They think that when they order the information from credit bureaus, it must be true. Without special scrutiny, special profiles created within the scheme are not immediately distinguishable from other newly created, legitimate files.

"If we are inputting a Social Security number that belongs to a child in conjunction with someone's name, and date of birth and address that we're getting off their ID (card) then we are part of the problem," McCain continued. "We have cross-polluted that trusted authority with that information."

Mitigating the Threat

Of course, the government has tried to put legislation in place to help limit this type of fraud. In 1971, the Fair Credit Reporting Act was enacted, which created the credit report as a primary vehicle for consumers to display their credit histories. The FACT Act in 2003 created a mechanism that consumers could use to dispute information on their credit reports. Most recently, the Red Flag rules have "put the onus back on the financial community or any business that uses personal identifiers" to have an identity theft prevention program to detect, prevent and mitigate the risk, McCain noted.

McCain expressed concern about financial institutions' use of automated loan decisioning in the context of synthetic identity fraud. "They allow us to validate a lot of loan applications very quickly, but they're not very good at picking up the vulnerability" of a fraudulent Social Security number, he said. "Current validation methodologies rely on algorithms and address histories, leading to major increases in synthetic name fraud."

Instead, McCain and Chuck Salvia, regional manager of Computer Information Management, recommend the Social Security Administration's [Consent-Based Social Security Number Verification](#) program, through which enrolled companies can match the Social Security number and accompanying identifiers they're being presented to the administration's master files.

According to Salvia, this program, launched in 2008, provides instant verification of a person's name, address, gender and whether the person who corresponds with the number is deceased. In addition, testing a Social Security number requires written consent of the holder of the Social Security number.

According to Salvia, credit unions can access the service in one of two ways. They can enroll directly, paying the \$5,000 one-time fee plus \$5 per verification request, or use the services of a company already enrolled in the program, such as Computer Information Management.

Salvia said experience confirms that CBSV verifies more personal identifiers directly to the official governmental source than any other verification. And, the program can handle large volumes of verifications for any legitimate business reason—from credit decisions to hiring processes to tenant screening.

Compared to other government identity theft prevention offerings, "it's the cream of the crop," Salvia said.

Having worked in this industry since 1971, McCain said extra caution is called for to make sure the risk of synthetic identity theft is managed both for your credit union and its members.

"As technology advances, it becomes more difficult to perform our functions (of mitigating risk)," he said. "This threat is huge. We haven't seen the end of it. I urge you to do the extra due diligence so you can sleep at night."

Lisa Hochgraf is a CUES editor.