

Old fashioned identity theft alive and—unfortunately—well

Did you hear about the family of five in Florida? Unfortunately, this is not a joke. It turns out they were involved in an identity fraud ring for more than three years. The family, with ages ranging from 24 to 37, had filed at least 130 fraudulent applications, using more than eight Social Security numbers and 11 dates of birth during a three-year time period.

Such is an example from an extraordinary effort by ID Analytics. According to a recent release, the company not only identified more than 10,000 identity theft rings in the United States, but set up a proprietary database showing the conspirators' locations, ages, and relationships. What it goes to show is that identity theft continues to be the major headache it has been for decades and is something financial institutions must continue to guard against. This is true even as the banking industry gears up to counter other and increasingly more sophisticated threats, such as the distributed denial of service attacks that have been much in the news.

Back to the study and some interesting observations:

- Hotbeds for fraud rings—States with the highest numbers of fraud rings include Alabama, the Carolinas, Delaware, Georgia, Mississippi, and Texas. The three-digit ZIP codes with the most fraud rings observed are areas around Washington D.C.; Tampa, Fla.; Greenville, Miss.; Macon, Ga.; Detroit; and Montgomery, Ala.
- Fraud in the countryside—While many fraud rings occur in cities, a surprisingly high number were also found in rural areas of the country.
- Bonding over identity theft—A large number of families are working together in fraud rings, even using each other's Social Security numbers and dates of birth. However, rings made up of friends are more common, with the majority of fraud rings made up of members with different last names.

The company says it determined this information by looking at approximately 1.7 billion identity risk events including applications for credit cards, wireless phones, payday loans, utilities, and other financial services credit products. It also examined changes in personal identifying information among accounts. This information was supplemented with authorization requests and other third-party data. The study examined data in the ID Network from January 2009 to September 2012. That's kind of looking at the problem from the outside in. EMC collaborated with the National Cyber Security Alliance to develop a tool that looks at the problem from the inside out. They created a free Online Identity Risk Calculator that provides a user with a sense of how vulnerable he or she is to identity theft—and more important, provides a quick tutorial about the risks. Located at www.emc.com/fraudgame, it's an ingenious 10-question quiz in which the user remains anonymous. It asks the user such questions like how much he or she accesses an online banking account, downloads apps, plays online games, uses social networks, and more. The lower the score, the better. The good news is that, in evaluating the first 2,000 people to take the quiz (only the scores and general demographics being recorded) the average score was 33 out of 100.

Along the way one learns such interesting facts as:

- More than 50% of phishing emails in 2011 were targeted at online banking users.
- Credit card fraud cost merchants \$100 billion a year.
- One out of every 300 emails sent in 2011 was malicious.

A word to the wise: EMC notes that online banking was a common risk activity for both males and females alike, with 60% of respondents accessing their banking online once a week or more. That customers use online banking is something that banks generally like, but it also means that associated security measures are that much more important in this channel. "The good news is that initial data from the nearly 2,000 people who used the Online Identity Risk Calculator seems to indicate a low overall exposure to online threats based on their behaviors tied to many basic things most of us do online every day. But no one should be complacent since cybercriminals are constantly evolving their attacks through more sophisticated phishing emails and websites, rogue mobile apps, and trojans that can expose consumers to identity fraud, malware infections, and even the takeover of online bank accounts," says Michael Kaiser, executive director, National Cyber Security Alliance. It seems that concern about identity protection, particularly as it relates to banks, is spreading. Just recently, a handful of companies that specialize in security products for financial institutions have felt motivated to issue releases saying, in effect, just that. Examples:

- FIS announced that it has experienced strong growth for its QualiFile deposit account risk scoring solution among its ChexSystems network members. "In 2011, FIS' risk management products saved our clients an estimated \$1.3 billion in fraud and abuse losses for demand deposit accounts. Our internal research shows a typical fraud loss averages \$1,200, and typical abuse loss is about \$400."
- FICO announced the availability of the latest version of Falcon Fraud manager, which has been around for 20 years. The new version protects consumers' card and demand deposit accounts from various forms of payment fraud, including e-payments fraud. "As customers bank across many different channels, it is essential for financial institutions to assess and confront account risk based on the transaction request and method by which the transaction is initiated," says Jason Malo, TowerGroup research director, in commenting on the FICO release.
- Finsphere Corp. announced results of a proprietary survey which concludes that nearly 75% of respondents would sign up for a debit or credit card featuring the company's security protection solution if it were offered by their financial institution. "The study exposes a clear opportunity for financial institutions to attract and retain customers," the survey report said.
- NICE Actimize recently touted the installation of its 360-degree view of enterprise risk into Metabank, located in Storm Lake, Iowa. It's a means to "ensure compliance with the Bank Secrecy and U.S. Patriot Act requirements and to reduce its operational expenses. Actimize's Suspicious Activity Monitoring and Customer Due Diligence Anti-Money Laundering solutions will support Metabank's efforts to protect consumers."
- Easy Solutions, Inc announced a major product enhancement of Detect Monitoring Service, intended for financial institutions as a proactive, cloud-based solution for phishing, pharming and malware. It provides 24/7 monitoring in real time to rapidly identify, shut down, and recover from online scams that mislead customers through fraudulent use of corporate identities.

It remains a jungle out there, with—as the ID Analytics database shows—a lot of predators. As with any safari, safety depends on personal responsibility—keeping one's eyes open—and professional help—responsible and effective security systems by trusted agents, namely banks. "By now, most online consumers hear a regular drumbeat about computer viruses and hackers, but it's not always clear how each of us, through our own everyday use of the web might be affected by online threats. Usually that understanding happens only after we personally experience something

bad," says David Martin, chief security officer, EMC Corp. ## Sources used in this article include: EMC and NCSA Offer Free Online Identity Risk Calculator ID Analytics Uncovers More than 10,000 Identity Fraud Rings in the U.S. Demand for FIS' Risk Solutions Soars as Banks Combat the Multi-billion Dollar Issue of Demand Deposit Account Loss FICO Falcon Fraud Manager 6.3 Prevents Electronic Payments Fraud on Demand Deposit/Current Accounts Independent Study Validates Strong Consumer Confidence and Demand for Finsphere Card Protection Solution That Improves Verification and Security of Credit and Debit Card Transactions NICE Actimize Solutions Implemented by MetaBank to Support Financial Crime Risk Strategy By Providing a 360-Degree View of Enterprise Risk Easy Solutions Launches a New Version of Detect Monitoring Service - Proactive Cloud Based Protection against Phishing Attacks.

About the Author

John Ginovsky is contributing editor of ABA Banking Journal and TechTopics e-newsletter. For more than two decades he has written about the commercial banking industry. In particular, he's specialized in the technological side of banking and how it relates to the actual business of banking. He previously was senior editor for Community Banker magazine (which merged with ABA Banking Journal) and was a staff writer for ABA's Bankers News. You can email him at jginovsky@sbpublish.com