Look Out for Identity Scams

By Philip R. Wahl II

Identity theft victimized 12.6 million adults in the United States last year. The theft equated to one case every three seconds and a cumulative plundering of more than $21 billion, according to the “2013 Identity Theft Report” by Javelin Strategy & Research, a privately funded firm specializing in customer transactions. Consumers ranked this business as their No. 1 problem for the 13th consecutive year, the Federal Trade Commission announced in February; 18 percent of 2 million-plus complaints “were related to identity theft.”

No matter the source, recent findings cause concern. Seven percent (8.6 million) of all U.S. households in 2010 “had at least one member age 12 or older who experienced one or more types of identity theft” that collectively cost $13.3 billion, tallied Lynn Langton of the Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, in November 2011. And in 2004, for example, this looting of consumers reached an all-time high at $47 billion, per Javelin. That same year, a survey by the nonprofit Identity Theft Resource Center estimated for each incident, 330 hours (mean) to repair the damage, including but not limited to $4,000 in lost wages (mean), $851 in out-of-pocket expenses (mean), and $614 in medical and emotional health-related costs (average).

The consequences of identity theft also affect the government. Last November, Ericka Crickowski, a contributing writer at DarkReading.com, a news and information portal about information technology security, compiled the most egregious breaches of government data in 2012; the worst entailed the stealing of more than 3.3 million unencrypted bank account numbers and 3.8 million tax returns from the South Carolina Department of Revenue. Andrew Shain at The State daily newspaper in Columbia, S.C., in January put the figure at “6.4 million consumers and businesses” and the tab at “$20 million and counting.”

Even the Internal Revenue Service has not escaped the enormous impact of ID theft. Treasury Inspector General for Tax Administration Judd R. Geiger testified as much at a May 2012 “Identity Theft and Tax Fraud” joint hearing before the Committee on Ways and Means, Subcommmittee on Oversight and Social Security, U.S. House of Representatives. “For processing year 2011, the IRS reported that of the 2.2 million tax returns that it identified as fraudulent, approximately 940,000 tax returns with $6.5 billion in associated fraudulent tax refunds involved identity theft,” he said.

No wonder the DOJ website introduces its discussion of identity theft and identity fraud by quoting Iago from Shakespeare’s Othello: “But he that filches from me my good name / Robs me of that which not enriches him / And makes me poor indeed.”

The definition of identity theft and identity fraud varies, with some authorities distinguishing between the two, others interchanging the phrasings, still more fusing one onto the other; and alternatives conveying that the latter occurs as a result of the former. For instance, the Westfield Bank of Ohio interprets identity theft as “fraudulently obtaining a person’s confidential identifying information” and identity fraud as “abusing this stolen information to falsely transact personal business in the victim’s name.” The DOJ explains, “Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception, typically for financial gain.” Unlike your fingerprints, which are unique to you and cannot be given to someone else for their use, your personal data — especially your Social Security number, your bank account or credit card number, your telephone calling card number, and other valuable identifying data — can be used, if they fall into the wrong hands, to personally profit at your expense.” All parties agree that the crime “can wreak havoc with your finances, credit history, and reputation,” in the FTC’s words, “and can take time, money, and patience to resolve.”

ID predators employ many devious tactics. Data phishing, social engineering, and hacker attacks are especially prevalent in the digital era. Other ploys include soliciting “customers” via email, text, and phone, creating fake websites, and mailing phony preapproved credit cards. Schemers also sift through garbage for paperwork that hasn’t been shredded, sort through coworkers’ desks, search public records, “shoulder surf” or watch and eavesdrop from nearby, steal or redirect mail, and submit false job, loan or credit card applications and otherwise assume the guise of the prey.

To reduce the risk of identity theft and identity fraud, pay attention to what the DOJ calls the SCAM, which requires taking proactive steps against possible swindling. Specifically: “Be stingy about giving out your personal information to others unless you have a reason to trust them. … Check your financial information regularly, and look for what is out of place and what shouldn’t. … Ask periodically for a copy of your credit report. … Maintain careful records of your banking and financial accounts. … If you’ve suffered identity theft or identity fraud, immediately freeze your accounts, notify credit bureaus, establish fraud alerts, contact law enforcement, report the crime to the FTC, acquire other applicable entities such as the IRS, Social Security Administration and the department of motor vehicles, and consult advisory websites including the Privacy Rights Clearinghouse at privacypolicies.org.”

Philip R. Wahl II (Georgia Regents University) is the Augusta market president for Savannah River Banking Company in Augusta, Ga. He earned a B.B.A. in management from GRU and serves as chair of the board of trustees of the Augusta State University Foundation.

Other outreach includes being on GRU’s Hull College of Business board of advisors and on the GRU Consolidation Working Group. Wahl’s past chairmanship spans the Augusta Metro Chamber of Commerce, Augusta Convention & Visitors Bureau, and the Downtown Development Authority of Augusta. Email him at phil.wahl@savannahriverbanking.com.