

BUSINESS IDENTITY THEFT:

The Latest Twist

Judith M. Collins

Identity theft is rapidly becoming the most pervasive financial as well as brutal crime to occur in the history of the United States. Identity theft crimes undermine business and the economy of the entire U.S. and facilitate acts of terror against U.S. citizens. Identity theft is directly related to drug trafficking, money laundering and organized crime (Collins & Hoffman, 2003a). Indeed, identity theft and not terrorism may be called the crime of the 21st Century.

The most common definition of Identity theft is the unauthorized use of another person's "personal identifying information" to obtain credit, goods, services, money, or property, or to commit a felony or misdemeanor. "Personal identifying information" means a person's name, address, telephone number, driver's license number, Social Security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings or checking account number, or credit card number. The definition in recent months, however, has taken a new twist: the latest trend is "business" identity theft (Collins & Hoffman, 2003b).

"Business identity theft" is the unauthorized use of a business's business identifying information to obtain credit, goods, services, money, or property; or to commit a felony or misdemeanor.

"Business identifying information" means a business's name, address, telephone number, corporate credit card numbers, banking account numbers, federal employer identification number (FEIN), Michigan Treasury Number (TR), electronic filing identification number (EFIN; Internal Revenue Service), electronic transmitter identification number (ETIN; Internal Revenue Service), e-business websites, URL addresses, and e-mail addresses (Collins & Hoffman, 2003b). Business identity theft also includes account numbers known to employees, such as passwords and codes that provide access to buildings, offices, departments and locations where proprietary and financial records are processed or maintained (Collins & Hoffman, 2003b).

Personal identity theft is a \$100-billion per annum industry worldwide; however, for at least four reasons, the cost of stolen business identities can be expected to be even greater. First, business bank and credit card accounts are often reconciled less frequently than most personal accounts; second, business statements usually contain many more entries and charges made from numerous geographical locations, national and international; third, business accounts also usually contain larger amounts of funds relative to personal banking accounts; and, fourth, business "store fronts" are now located in cyberspace

The author is Associate Professor and Director, Identity Theft University-Business Partnerships in Prevention at Michigan State University, School of Criminal Justice in East Lansing, Michigan.

on e-commerce websites. For these four reasons, “business identity theft” has become an attractive crime for the knowledgeable criminal.

For example, one business identity theft case involved the cloning of a legitimate e-commerce website in which the International Chamber of Commerce (ICC) uncovered a global Internet banking scam involving about \$3.9 billion (ICC Commercial Crime Services, 2001). The identity thieves set up fake websites that were identical to the sites of original businesses. By mimicking legitimate banking businesses, the criminals obtained customer Social Security Numbers and bank and credit account numbers. At least 29 fraudulent websites, all hosted in the U.S., mimicked websites of either Euroclear Bank, the international clearing system for securities transactions, or Bloomberg, the information services provider. The perpetrators published fake European banking guarantees worth nearly \$4 million and validated the documents on the websites. The crime involved a network that operated in the United States and the Far East, however, the fake guarantees were cashed at banks in the UK and other countries. This example illustrates how “business identity theft” is not only the latest twist but has also become a criminal trend that expands the jurisdiction of identity theft crimes far beyond the cities and counties of the United States.

In another “business identity theft” case, the owner of Omega Financial began receiving calls from “customers” who said they had sent his company a \$900 loan commitment fee and wondered why their loans had not been processed (Associated Press, 2001). Omega Financial was the victim of “business identity theft.” The company had never received any commitment fees.

What’s more, the company had been out of the loan business for over a year. The perpetrators had placed newspaper ads in several states that included a toll-free number to apply for a loan, using the Omega Financial name. This identity theft network operated in the U.S. and Canada.

Other “business identity theft” examples include the owner of a company who received advertising bills from the Verizon communications company totaling over \$24,000 – someone had placed ads in the Verizon yellow pages using the legitimate business name and address but another telephone number (Slattery, 2002); in Colorado (People vs. Joseph Finley, et al, Case Nos. 01 CR 2356 through 2366, Denver District Court), seven members of an identity theft network were convicted for stealing and using a business bank account number to create and cash bogus payroll checks; in Florida, three men obtained temporary employment at several businesses where they, too, stole business bank account numbers, which they used to print counterfeit checks. Finally, a criminal stole and used the federal employer identification number (FEIN) of a legitimate, 25-year Michigan business to obtain a \$480,000 Small Business Administration (SBA) loan. The company owner learned of this “business identity theft” when he received a notice of default on the SBA loan, applied for by the perpetrators (Identity Theft University-Business Partnerships in Prevention, 2003).

There are solutions to identity thefts. Contrary to common thought that most identity thefts occur online by hackers, the majority of identity thefts emanate from the workplace. Recent research on 1,037 cases indicated that as much as 70% of all identity thefts are committed in the workplace by

employees or by people impersonating employees (Collins & Hoffman, 2002). These employees, often contract or temporary workers, obtain employment for the sole purpose of personal or business identity thefts. The source for prevention is therefore the workplace.

Beginning with (1) personnel selection for security, managers can secure business borders by (2) conducting “information” process risk assessments to secure the personal and business information as it is processed through sequential job tasks, (3) conduct e-business website risk assessments to identify susceptibilities to theft, (4) require that documents containing personal or business identities be cross-shredded before disposing, (5) develop ‘red flags’ to identify potentially bogus credit card, bank, retail account or other applications, (6) train employees to recognize bogus applications, (7) generate random numbers for use as personal identifiers, for both customers and employees, in place of Social Security numbers, (8) develop and emphasize ethical company cultures, and (9) reinforce and reward employees who promote honesty in the workplace. Thus, identity theft can be prevented at its source in the workplace by implementing a four-factor model that focuses on a business most valued assets: people (employees, customers and other stakeholders, processes (information throughput within departments), proprietary information (personal and business) and property—virtual and actual (Collins, 2000).

In summary, identity theft has expanded beyond the theft of “personal” identities to include “business” identities. What’s more, the jurisdiction of identity theft has also expanded beyond the counties and cities of the U.S. to include countries worldwide. Most alarming perhaps is that

the majority of identity thefts occur in the workplace, making identity theft a far more serious and costly crime than shrinkage ever was and an especially egregious form of workplace aggression. But identity thefts can be prevented, by securing four business assets: people, processes, proprietary information and property.

References

Associated Press (2001). N. H. businessman latest victim of fraud ring. In *Foster's Daily Democrat*. Retrieved December 4, 2001, from <http://www.fosters.com/citizennews2001/Dec/03/ap1203e.htm>.

Collins, J.M. (2000). Preventing identity theft in the workplace using the four-factor model to secure people, processes, proprietary information and property (virtual and actual). Presented by Collins, J.M. and McGinley, T.G. at the *Academy of Criminal Justice Sciences 38th Annual Meeting*, in Panel Session 132, “Identity Fraud Profit and Predictions,” Wash., DC. April 5, 2001.

Collins, J.M. & Hoffman, S.K. (2003a). Identity theft legislation for the State of Michigan. Bill proposal September 29, 2003, for Sponsorship by Senator Beverly S. Hammerstrom, District 17, State of Michigan. Contact: Judith M. Collins, Ph.D., judithc@msu.edu, 540 Baker Hall, Michigan State University, E. Lansing, MI 48824-1118.

Collins, J.M. & Hoffman, S.K. (2003b). *Identity theft first responder manual for criminal justice professionals: police officers, attorneys and judges*. Flushing, NY: Looseleaf Law Publications, Inc.

Collins, J.M. & Hoffman, S.K. (2002, January). Identity Theft: Perpetrator (n = 1,037) profiles and practices. Case study conducted in preparation for grant funding, submitted January 2003 to the National Institute of Justice, U. S. Department of Justice, Office of Justice Programs. Contact: Judith M. Collins, Ph.D., judithc@msu.edu, 540 Baker Hall, Michigan State University, E. Lansing, MI 48824-1118.

Colorado Attorney General (2001, December 21). Moving business operator and associate indicted on insurance fraud, forgery, weapons & other charges. Press Release. Retrieved July 2, 2002, from <http://www.ago.state.co.us/PRES-REL/presr12001/prsr1116.stm>.

Identity Theft University-Business Partnerships in Prevention (October, 2003). Report by a business owner victim of the theft of a federal employer tax identification number. E. Lansing, MI: Identity Theft Crime and Research Laboratory. Contact: Judith M. Collins, Director, judithc@msu.edu, 540 Baker Hall, Michigan State University, E. Lansing, MI 48824-1118.

International Chamber of Commerce (ICC) Crime Services. (April 11, 2001). CSS foils multibillion multi-billion internet banking fraud. Retrieved August 8, 2003 from: http://www.iccwbo.org/ccs/news_archives/2001/fraud.asp.

Slattery, J. (2002). The problem of business identity theft. CBS 2, New York. Retrieved March 31, 2003, from: http://www.cbsnewyork.com/investigates/local_story_297105022.htm