Small Businesses: Targets of Deception

ALLEN ANDERSON

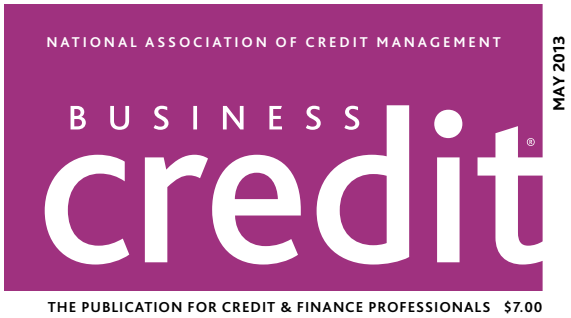
Of the many ways for a company to be robbed, some are more harmful than others. While outright shoplifting and theft, sometimes referred to euphemistically as "shrinkage," occurs in nearly every industry, stealing from a business is all the more painful when it loses its precious customers or dollars through deception. This deception takes many forms, but increasingly, the type of fraud causing small businesses the most damage is business identity theft.

Stealing a business's identity can be as simple as masquerading as a legitimate competitor in order to usurp hard-earned trust and brand awareness. A knock-off might try peddling "Kloor-ox" cleanser or "Clean-X" tissues rather than spend years building a quality product and brand name of their own. Businesses with established and recognized brands take a dim view of this type of corporate identity theft.

While outright shoplifting and theft, sometimes referred to euphemistically as "shrinkage," occurs in nearly every industry, stealing from a business is all the more painful when it loses its precious customers or dollars through deception.

Toho Pictures Ltd., the owners of the famous Godzilla name, image and roar, forced the makers of "Gabzilla," a Napa, CA, winery to remove a reptilian monster image from its cabernet sauvignon. Similarly, Toys"R"Us, Inc., has more than once taken action to discourage start-ups from being a bit too clever with their naming. Cases have been brought against Smokes R Us (a tobacco store) and Suds R Us (a coin-op laundry) to name but two. These actions may seem petty, but well-known entities facing any loss of their powerful brands are obligated to pursue any infringement, lest they diminish their identity or tarnish their image. Trademark cases such as these are often resolved based on the "likelihood of confusion" test.

This type of corporate identity theft is not limited to the best-known names, although larger entities are more likely to have the resources to fight back. In 2010, the small business Memphis Auto Sales had its name tarnished when fraudsters created numerous phony car sales websites offering steeply discounted vehicles and citing the physical address of Memphis Auto. Hundreds of unsuspecting buyers who made deposits on cars were deceived, while Memphis Auto—through no fault of its own—suffered the consequences, fielding thousands of calls from irate victims.



Even More Damaging Types of Business Identity Theft

Exploiting the name or the reputation of another's enterprise is but one form of business identity theft. Other methods are more direct. Rather than simply capitalizing on a reputation, the more sinister forms of business identity theft occur when scammers successfully convince a legitimate business's customers, suppliers or, most damaging, financial institutions that they are dealing with a genuine business's authorized personnel. "Just charge it to our account" can be costly without safeguards in place to authenticate that credit is being properly extended or withdraws duly authorized.

Stealing a business identity can happen in many ways. Both private businesses and government agencies are at risk, with all businesses ultimately suffering the consequences. Attackers may tap directly into state database systems or may simply access public records to obtain publicly held information, using that information to deceive creditors. Creative thieves have used email "phishing" attacks, malware and viruses to infiltrate business computer systems. Once installed, these systems can record every keystroke, thereby stealing

usernames, passwords and bank account numbers. The Internet and advent of electronic funds transfer offer the opportunity for these crimes to literally occur at lightning speed, with perpetrators remaining concealed behind the anonymity of an often bogus Internet protocol address.

Losing 3.8 Million Social Security Numbers

In August of last year, a malicious phishing email was sent to multiple South Carolina Department of Revenue employees. Unfortunately, at least one Department of Revenue user clicked on the embedded link, unknowingly executing malware, which caused the entire system to become compromised. The attacker used the purloined credentials to first gain access to the user's workstation and then leveraged this login to access other Department of Revenue systems and databases.

According to the *Public Incident Response Report,* commissioned by the South Carolina Department of Revenue following the breach, the attacker used at least 33 distinct pieces of malicious software and utilities to perform the attack. By the time the assault was discovered, the data theft had compromised a total of 44 systems, after installing a "back door" for unfettered admittance. Thirty-nine systems were accessed, three systems had database backups or files stolen, and one system was used to send the data back to the attacker. The Social Security numbers of millions of citizens and tax identification numbers of half a million businesses were compromised.

According to the information security analyst firm Mandiant, which conducted the incident forensics following the intrusion at the South Carolina Department of Revenue, the overwhelming majority of these targeted attacks proceed undetected. "Skilled and determined attackers can break, enter and succeed within minutes," Mandiant warned. "Other times, they spend days plotting, establishing backdoors and fortifying their positions inside a company. This sophistication and persistence presents challenges for those trying to scope, contain and remediate the threat."

Elaine Marshall, the Secretary of State for neighboring North Carolina, is keenly aware of the havoc wreaked by the data breach to her south. She is co-chair of the National Association of Secretaries of States' (NASS) Business Identity Theft Task Force, which works to bring awareness of business identity crimes and to make it harder for identity thieves to prey upon state-based businesses.

"Protecting the state-held information that offers a potential gateway to business identity theft is a critical component of our mission," she said. "Secretaries of State want to warn businesses, particularly small and midsize business owners, that this type of crime can be financially devastating. Business identities are uniquely valuable, because an established credit history can be worth a lot of money to fraudsters."

In the NASS white paper "Developing State Solutions to Business Identity Theft Assistance, Prevention and Detection Efforts by Secretary of State Offices," numerous similar data breaches are cited. In a number of these cases, criminals simply updated or altered the registration information on file with the state. After the registration information was changed, the criminals used the altered corporate identity to make online applications for credit.

The Secretary of State's offices throughout the country have alerted businesses to the risks of business identity theft after cases in which state business records available online were altered and used to open fraudulent lines of credit. In Colorado, authorities became aware of a scam after one of the targeted companies was contacted by a major retailer about nearly $250,000 in purchases made in its name. Later, it was discovered that someone had changed the company's location in state data records from Boulder to a dummy office in Aurora, where the company's mail was being forwarded to another address in California. By the time authorities were able to break the scam, more than 300 businesses had fallen victim to identity thieves, with total losses exceeding $3.5 million.

> "Business identities are uniquely valuable, because an established credit history can be worth a lot of money to fraudsters."

It Can Happen to Anyone

Perhaps the greatest misconception, and therefore the greatest threat, is a false sense of security. Unfortunately, many victims of identity theft are the very business professionals who snicker in amazement when they hear of someone responding to a phony lottery scam or a millionaire prince email. "I would never be foolish enough to fall for that," they say. While these common fraud attempts are usually the work of amateurs, there are exponentially more sophisticated swindles being perpetrated by professional criminal enterprises. These frauds, which are targeting businesses and government entities of all sizes, are often impossible to detect until after the damage has been done.

Scammers have become more discreet, and the scams more insidious. In many cases, data is breached without detection, usually as the result of malware software. It only takes a momentary lapse in judgment—clicking on an email link—to wreak havoc.

Take the case of Patco. This successful Maine-based construction firm was blindsided by a data identity theft incident, which succeeded in extracting hundreds of thousands of dollars from their corporate account. (The actual transfers totaled $588,851.26; however, the bank interceded before $243,406.83 could make it into the thieves' hands, leaving a residual loss to Patco of $345,444.43.) Much to their horror, their bank denied responsibility for the loss until after the case had gone through nearly three years of trials and appeals.

While the bank ultimately settled out of court and reimbursed Patco for its loss, the case highlights important distinctions between consumer and commercial protections. Despite the fact that Patco's losses originally occurred in 2009, it wasn't until November 2012 that the case was finally settled. Few businesses could endure a similar three-year distraction. "Three years later, after hundreds and hundreds of thousands of dollars in legal fees, deposition costs and court costs, we're to the point where we should have been before," said Patco Owner Mark Patterson in an interview with BankInfoSecurity.com.

A bank typically absorbs the risk of loss when unauthorized funds transfers occur from a consumer account. However, as Patco's bank pointed out in court, a bank may shift that responsibility to the business customer by either proving that the bank offered reasonable security procedures or by proving that it approved the fraudulent payment in compliance with security procedures noted in its contract with the customer. While Article 4A of the Uniform Commercial Code provides protections to commercial customers similar to those provided to consumers under Regulation E, the courts stressed that commercial customers bear some responsibility for their own safeguards.

Many business identity theft cases are never reported—businesses don't want the negative publicity and are too busy running their business and recovering from the damage done by the scam. They believe they can't afford the time it takes to pursue a case. Unfortunately, they're often right. "I've talked to a number of people that have had losses here in the state of Maine, and they lost $70,000 to $80,000," Patterson said. "It's a lot of money, but they have been advised by their counsel that it's going to cost more to try and get the money back. It's not worth the battle. They just wrote it off."

> While most media attention regarding identity theft has been focused on individual consumers, the risk is actually greater for small businesses.

Protect Your Business: Monitor Your Accounts

Just as small businesses have made changes to combat other forms of theft such as shoplifting, there are many simple precautions for avoiding business identity theft that are analogous to locking the door at night. Data information security professionals strongly advise small businesses to review their data handling procedures. Start with the basics of conducting background checks on employees who will have access to banking information. Make sure there is an audit and review process in place, with two parties required to authorize large debits.

To protect against external threats, it's critical to update virus protection and security software. A broad range of effective antispyware, antimalware and security software is now available, but these systems need to be installed and kept up to date on all computer workstations and laptops. In a networked environment, any infected machine can quickly spread to other workstations—it's why they're called viruses.

The use of security software is critical for any device being used for online banking and payments. In fact, whenever practical, financial transactions should only be conducted from a single machine, which might be isolated from others on the network. These precautions are echoed by the Better Business Bureau (BBB), which stresses the following additional safeguards:

- Each user should have his or her own password. Do not have several users share the same password.
- Use complex passwords: ones that contain a combination of numbers, letters and symbols.
- Consider using an additional authentication tool, such as a token or a smart card.
- Each user should change his or her password frequently, approximately every 45 to 60 days.
- Do not respond to emails or open attachments unless you were expecting the communication. Remember that phishing scam emails can come from both unrecognized and recognized sources. (You won't ever receive an authentic email asking for your online banking credentials.)
- If something appears unusual or you receive an email requesting banking credentials, call your bank, but don't use any information from the email, as it may be a phishing email.
- Do not use public computers, such as at the public library, a hotel's business center or airport computer terminals, to access online banking.

The BBB further advises its members to reconcile accounts daily. While online banking may increase threats when used to authorize debits, it is also a useful tool for spotting irregularities. When accounts are reconciled frequently against expected credits and withdrawals, any unexpected account activity can be spotted before more damage is done.

The ACH Network offers a secure and reliable network for handling billions of direct account-to-account consumer, business and government transactions annually—it's how direct deposit happens. When moving money using the ACH Network, small businesses should nevertheless be even more diligent about their security practices.

Time is of the Essence to Minimize Business Risk

No matter how vigilant your company is, a data breach can still happen. As these many victims have demonstrated, it may be impossible to completely eliminate the risk of business identity theft. Therefore, the best strategy is to be prepared to mitigate the damage. Early detection is paramount to containing the threat.

It's advisable for small businesses to be preemptive when it comes to protecting their business identity. Too often, businesses find out about ID theft after the damage has been

done. It's much better, and apt to be much less costly, to be proactive rather than reactive.

Business credit monitoring can help prevent business identity theft by monitoring inquiries into a business's file, or any unexpected credit changes. This information is available in varying levels of detail, from presenting the basic facts of a business to detailed business credit, payment and public record histories. Small-business professionals can access this wealth of data and obtain instant business credit reports online through Experian and others. With business credit monitoring, small businesses can also monitor their own business credit report and receive change alerts, as well as make more insightful credit risk decisions about prospective business partners, suppliers and customers.

Having immediate access to such data can mean the difference between profit and loss, or minor or catastrophic loss in the event of identity theft.

A credit monitoring service allows a small business to:

- Be quickly alerted to unexpected applications for credit in their business's name
- Discover if its business credit report contains errors that can negatively affect cash flow
- Review the company's credit file for completeness and accuracy
- Remain current on changes in its credit file that could negatively affect the business
- Know who is inquiring about the business

In addition to being a useful tool for monitoring one's own report for unexpected activity, a business credit reporting service is also valuable to review a potential customer or supplier's credibility when making credit decisions. This allows a business to discover in advance:

- The status of prospective customers' payment practices
- Changes in existing clients' business conditions
- Suppliers' relationships with others
- Notifications about changes to suppliers' or customers' business credit reports
- If a customer or a partner may be going out of business
- When a key account begins to get behind on payments

Identity Theft is a Risk That Can Be Mitigated

While most media attention regarding identity theft has been focused on individual consumers, the risk is actually greater for small businesses. Most small businesses barely have time to take care of their essentials, such as customers, payroll and suppliers. A baker worries about cupcakes going stale before they're sold. A builder worries about getting a roof on before the snow falls. There isn't enough cycle time to add additional worries such as who might be withdrawing funds from the corporate account. It's hard enough to earn profit, and once it's in the bank, it is presumed safe. Unfortunately, that's not always the case.

According to a recent study, small-business owners are victims of fraud at a rate of 15% more than the general population. Javelin Strategy & Research's *2011 Small Business Owners Identity Fraud Report* found that in 2010, small businesses lost about $8 billion to fraud. While the Javelin study found that the average amount of money stolen from small-business owners per incident is $4,851—only marginally higher than it is for consumers—the cost that comes with cleaning up the mess is 150% higher for businesses than it is for consumers. This is partly due to the fact that banks are less likely to cover losses for small businesses. However, small businesses also share some of the blame. The study found that small businesses were also less likely to monitor their accounts.

> "The majority of small-business owners do little to audit their business activities."

The Javelin study found that regular business account audits are rare among small-business owners. "The majority of small-business owners do little to audit their business activities," the analysts reported. "Thirty-eight percent personally examine account records on a monthly basis, and 12% use account alerts."

Businesses of all sizes have had to become more prudent about security. Physical assets, personnel safety and even a business's very name—its identity—must be protected. While nothing can guarantee that a business won't become a victim of deception, just a few simple precautions can reduce the risk of identity theft.

Allen Anderson is president of Experian's Business Information Services, where he is responsible for the strategic direction and leadership of the unit. Experian's Business Information Services is committed to helping businesses increase revenue and efficiency by making more informed decisions about their business-to-business customers. For more information, please visit www.experian.com/b2b.