Tackling Corporate Identity Theft With a Public-Private Partnership

Decide with Confidence

Executive Summary

Corporate identity theft is on the rise. This crime, which entails the unauthorized use of a company's name and information to perpetrate fraud, is often more lucrative than stealing individual identities. Thieves alter company information, such as registered agent names and addresses, and use the falsified information to obtain commercial credit lines and order hundreds of thousands of dollars in merchandise in the name of the legitimate business; and then they disappear with the goods weeks and months before the fraud is discovered. Businesses of all sizes are being victimized.

The good news is we have developed a solid understanding of the schemes fraudsters use to perpetrate corporate identity thefts. In addition, businesses themselves are overcoming their reluctance to acknowledge and address this problem. Equally important, state governments are starting to take corrective actions. In our view, the time is ripe for government and business to join forces in a comprehensive partnership that enables them to share information, identify best practices, and collaborate in combating corporate identity theft.

The Rise of Corporate Identity Theft

Corporate identity theft is similar to personal identity theft. Criminals steal the identity of a legitimate business, trading on its good name to secure or use an existing line of credit or otherwise obtain goods and services from unsuspecting companies. The fraudulent business may also use the stolen identity as a tool to help steal large numbers of individual identities. It may be weeks or months before a company discovers that it has shipped hundreds of thousands of dollars worth of goods to a fraudulent business, or that criminals gained access to its networks and data by posing as a legitimate business. And by that time, the criminals are long gone, carrying out the same scheme in another city or state.

What's alarming about corporate identity theft is its rapid spread across many states. At Dun & Bradstreet, where we closely monitor business activities, we have seen a growing business trend of corporate identity theft in just the last 12 months. Media reports of the crime are growing as well:

- In Colorado, identity thieves exploited minimal controls on the state's business registration website, which allowed anyone to go onto the website and change corporate information. The thieves would alter information such as company addresses or officers, and then used the falsified information to order merchandise and secure credit lines, in one case bilking a medium-sized retail company of $250,000. Police investigators said they identified 48 companies affected by the crime and expected to find dozens more.[1]

The Many Victims of Corporate Identity Theft

1. The company that has its identity stolen – usually a small or medium-sized business.
2. The company that receives an order for goods or services and delivers them to the fraudulent company – often a large business.
3. The bank or lending institution that issues credit to the fraudulent company.
4. The entities that provide confidence in commercial transactions, such as a credit bureau, government business registration agency, or even an unrelated company whose identity is stolen and used by a fraudster to provide a positive reference, such as a prompt payment experience.
5. The commercial jurisdiction where repeated fraud is perpetrated, undermining the "good-name" of a county, state, or even country.

[1] Joseph Boven, "New scam takes advantage of Secretary of State's business filing system," *The Colorado Independent*, July 16, 2010; and David Migoya, "Corporate ID thieves mining the store: Net-based swindle surprisingly easy," *The Denver Post*, September 23, 2010.

- In California, a common scheme has seen criminals assume the name of a business located at the same address where they rent

  virtual office space. They will then order corporate credit cards and merchandise ranging from computers to hot tubs. Because these fraudulent charges are often mixed in with legitimate business expenses, the corporate victims may not detect the fraud for six months or more. "It's easier and safer to pretend to be a corporation," said Robert Morgester, a California deputy attorney general who specializes in identity theft and computer crime.[2]

- In Canada, criminals have found numerous ways to steal corporate identities of small businesses, which are especially vulnerable because they lack the resources to implement needed controls. In one instance, a fraudster falsified company minutes and made himself the CEO, which allowed him to sell a company-owned building and abscond with the proceeds.[3]

The consequences of such crimes can be devastating, especially for small businesses that can't afford to simply write-off $250,000 in unpaid merchandise. And a business that's had its identity stolen may find itself embroiled in legal battles and demands for payment of goods it did not purchase or bank loans it did not receive. "About 7 percent to 15 percent of all commercial credit losses are due to corporate identity theft, fictitious companies or related fraudulent activity," said Bob Beckett, of Dun & Bradstreet. "And no business is immune. The victims range from small, single-store businesses to large multinational corporations."

A variety of factors have spurred the rapid increase in corporate identity theft. Successful crackdowns on consumer fraud have caused many criminals to target businesses instead. New online services also make it easy to create businesses that appear to have legitimate addresses, phone numbers and credit histories, thus enabling criminals to set up shop quickly and begin their con. At the same time, safeguards have not kept pace because businesses are only beginning to realize their vulnerability to this crime. In particular, the necessary collaboration among businesses and law enforcement agencies—such as sharing information and developing best practices and approaches to combating identity theft—has just started. These factors translate into a low prosecution rate, making corporate identity theft an attractive criminal enterprise.

Patterns of Deceit

When banks or corporations evaluate a business seeking credit, they often look for evidence—for a "Proof of Right"—demonstrating that the company is who it says it is, and that it has the resources and capabilities it claims to possess. A proof of right can be a financial statement, business address, phone number, government business license, credit history and other business record. Confidence in the legitimacy of a business is increased with each proof of right that is verified.

Unfortunately, fraudsters are finding ways to mimic or illegally obtain traditional business records that provide proof of right. Moderately skilled individual fraudsters have gained knowledge on how to fool automated credit-decisioning tools; and the Internet enables them to perform their scams from afar, including outside the country, making them difficult to uncover or trace and ultimately prosecute. Our experience shows that fraudsters are circumventing traditional business verification methods using tactics that are common to a variety of fraudulent activities, including corporate identity theft:

- ***Falsify business registration documents and updates.*** Thieves exploit the lack of password controls or PINs to change business information on Secretary of State or other licensing websites, adding false addresses or reinstating a previously dissolved company; or they might register in one state as a foreign corporation that is related to a legitimate company in a different state, thus getting the "standing" and corresponding credit history of the legitimate corporation.

[2] Greg T. Spielberg, "Taking on Small-Business Identity Theft," *Bloomberg Businessweek*, July 9, 2009.
[3] Sharda Prashad, "Identity theft strikes small businesses," *The Globe and Mail*, Jan. 18, 2010.

- ***Falsify credit reporting profiles.*** Thieves have tried to use loopholes that would enable them to request "updates" to information in credit bureau files, thus legitimizing false business information, such as an address or phone number.
- ***Falsify financial statements.*** Using information gathered from public documents available on the Internet, such as annual reports, thieves can recreate financial statements for fraudulent purposes.
- ***Purchase "shelf" corporation.*** Thieves can purchase a 40-year-old corporate charter off the shelf, making them look well established and low risk. Creating and purchasing these aged shelf corporations, which adds creditor confidence and often drives automated decisioning rules, is legal. Using them with the intent for fraudulent purposes is not.
- ***Create a website for business.*** Business websites are easy to create, including websites that mimic those of well-known corporations. Additionally, fraudulent use of the D&B, Better Business Bureau® and VeriSign® symbols is on the rise.
- ***Obtain a verifiable office location.*** Thieves rent office space in the same building as a legitimate business, which enables them to obtain credit cards or merchandise on credit because the business address is verified as legitimate.
- ***Obtain a virtual and in some cases well known and established office location***. Virtual offices are on the rise, often with little or no vetting. Even places such as the Chrysler Building, Rockefeller Center and Madison Square Garden in New York offer virtual offices, mailbox, telephone answering services, etc.
- ***Obtain a verifiable phone number***. Phone services allow a number to appear as local or as a landline when it is not, or provide a professional answering service and even forward the call to a prepaid mobile phone.

Criminals may use these deceptions for a quick swindle that allows them to get the goods and then get out; or they may use them as part of a complex scheme to build credibility for a big score. Complex schemes often go on for months with a number of well-organized steps that might include multiple players spread across the country, or even outside the country, all with a big score in mind. In either case, these deceptions provide criminals with multiple ways to fraudulently demonstrate proof of right, leaving banks and businesses vulnerable to corporate identity theft.

Next Step: Public-Private Sector Partnership

Despite the rise in corporate identity theft, businesses have been reluctant to adopt stricter controls because they don't want to drive away legitimate customers. They want to make it easy—not difficult—to do business with them. State and local governments face the same dilemma: If businesses have to navigate what seems to be a bureaucratic maze simply to do business in a particular city, state or even country, they may take their business—and jobs—elsewhere. Consequently, the chief problem in addressing corporate identity theft is: How can we implement effective safeguards that don't slow or discourage the free flow of legitimate commerce?

We believe that government and business must band together in partnership to exchange ideas and best practices for combating corporate identity theft. We are already seeing some states taking steps to protect businesses. Some states, like Colorado, are setting up toll-free numbers for victims to report theft and fraud. Also, the Colorado Secretary of State's website provides warnings and tips to help businesses avoid identity theft.[4] In California, the state legislature strengthened law enforcement by expanding the definition of "person" in identity theft cases to include associations, organizations, partnerships, businesses, trusts, companies, and corporations.[5] The U.S. Small Business Administration

> "Both law enforcement and the business community need to be willing to share information and work in collaboration on these cases. This is a new type of crime and it will take both groups time to recognize and learn how to identify these criminal activities."
>
> *Kevin Hyland*
> *Agent, Colorado Bureau of Investigation*

[4] See www. protectyourbusiness.us
[5] Greg T. Spielberg, "Taking on Small-Business Identity Theft," *Bloomberg Businessweek*, July 9, 2009.

also provides educational materials and tools for fighting identity theft. These are all great steps. But if states and businesses act independently or with little coordination, criminals can quietly move into a new city or state without fear that their methods and activities will be known to their new marks.

The time has come to create a public-private task force on corporate identity theft. Task force members can exchange lessons learned and identify emerging trends and best practices among corporate and government agencies. The task force also can help identify available tools and techniques that reduce the risk of corporate identity theft without placing a burden on legitimate businesses to register, apply for credit, receive credit or update their credit reports. Ultimately, combating identity fraud will require the combined efforts of business entities monitoring their business registrations and credit reports; vendors and suppliers leveraging red-flags; and government having the statutes in place to prosecute offenders. Together, we can stop corporate identity theft before it happens.

About Dun & Bradstreet

Dun & Bradstreet (NYSE:DNB) is the world's leading source of commercial information and insight on businesses, enabling companies to Decide with Confidence® for 169 years. D&B's global commercial database contains more than 185 million business records in over 190 countries. The database is enhanced by D&B's proprietary DUNSRight® Quality Process, which provides our customers with quality business information. This quality information is the foundation of our global solutions that customers rely on to make critical business decisions. D&B provides solution sets that meet a diverse set of customer needs globally. Customers use D&B Risk Management Solutions™ to mitigate credit and supplier risk, increase cash flow and drive increased profitability; D&B Sales & Marketing Solutions™ to increase revenue from new and existing customers; and D&B Internet Solutions™ to convert prospects into clients faster by enabling business professionals to research companies, executives and industries. For more information, please visit **www.dnb.com**, or call **800.424.2495.**