Secretaries of State Confront the Growing Problem of Business Identity Theft

By Kay Stimson

Secretaries of state are warning about the increasing risk of business identity theft as the problem spreads across the states. Criminals have been altering online business records housed by their offices and using them to open up phony lines of credit to illegally obtain valuable goods and services. Secretaries of state are working to establish new safeguards against such fraud, as they alert state legislators and other key stakeholders about the magnitude of the issue.

Secretaries of state are preparing to take on a new threat that has emerged during the nation's economic downturn. The officials who oversee corporate registrations and other business filing processes on behalf of the states say that business identity theft—a criminal mutation of classic identity theft—is on the rise and spreading across states. Computer-savvy thieves are literally hijacking business entities from their owners, leaving behind a digital vapor trail of fraudulent credit purchases and other damages. Several states have already adopted new or improved safeguards for protecting the state-held data that offers a potential gateway to this type of crime, and they are warning others to do the same.

"This can explode quickly and become a big problem," said Colorado Secretary of State Scott Gessler, who noted that his state has already registered 85 victim entities with total losses of approximately $3.4 million. "We are committed to making Colorado a hard target for identity thieves, and that means identifying new policies and protections for state-based businesses as well."

National numbers on business identity theft are virtually impossible to calculate; federal law enforcement agencies typically haven't kept such statistics. However, Dun & Bradstreet, a leading provider of business credit information in the United States, has reported documented cases of business identity theft in at least 22 states.

"What is particularly disturbing about this trend is the significant dollar amounts involved," said Robert Strezze, a senior risk analyst with Dun & Bradstreet. "It's not unusual for the losses to be in the mid-six figures by the time the criminal activity is detected, and it's a lot more lucrative than stealing individual identities."

That sentiment is echoed by Colorado's Gessler, who added that one business in his state suffered a loss of at least $250,000 at the hands of corporate identity thieves.

The cost to state and local governments is harder to determine, but just as with regular identity theft, costs add up for law enforcement and other government officials who investigate and help remediate damages from the crime. Plus, few dispute that a state with a reputation damaged by repeated or large-scale fraud of this type could see damage to its economic development plans.

Methods of Deception

According to the experts, the process of business identity theft is very similar to regular identity theft, only on a more complex scale. Criminals look for ways to steal a legitimate business identity, securing lines of credit with banks and retailers at the expense of the unsuspecting victim entity. Once the fraudsters get the money or goods involved, they leave the legitimate business owners steeped in debt and typically unaware that a crime has occurred until creditors come calling—giving the bad guys ample time to find new victims and evade detection.

Enterprising thieves are stealing business identities in a number of ways. In California, they have rented virtual office space, sometimes in the same building as the victim entity, ordering everything from corporate credit cards to electronics and hot tubs.[1] The crooks then sell the illegally obtained merchandise, shut down the virtual office and move on to the next victim as quickly as possible.

In other states, thieves have been able to carry out their scheme by gaining access to legitimate business records. This happened in Colorado, where criminals were able to exploit the state business registration website, altering the names of company officers and addresses for at least 85 victim entities.

Once the criminals were able to change the corporate registration information for each business that became a victim of the scam, they were able to use the business's corporate registration history—along with additional false documents—to establish lines of credit with banks or retailers. Identity thieves then purchased items that could be bought and exchanged for cash or sold with relative ease.

"Make no mistake about it, this is organized crime," warned Georgia Secretary of State Brian Kemp, who has implemented new protections in his state to curb business identity theft. "And there is more than one victim—it's actually much larger than some might think."

Kemp pointed to a whole chain of victims who must clean up in the wake of such fraud. Beyond the business which has its identity stolen, the crime affects the companies that have received the orders for stolen goods and services, the banks or lending companies that have issued any credit and entities like state governments that house business filings and related documents to provide confidence in commercial transactions.

Businesses of all sizes are being victimized by identity theft, but small and midsize companies are most often targeted.[2] Experts say this is mainly because they have extensive credit lines and cash reserves, but fewer legal and financial protections at their disposal than larger corporations.

In Georgia, Kemp noted he has also seen cases of such fraud related to churches and family-owned businesses at the center of divorces or disputes between relatives. Dun & Bradstreet's Strezze has also seen thieves taking on the identity of dormant or well-aged shelf companies whose owners are no longer doing business.

State Solutions

In order to make it more difficult to perpetrate corporate identity theft, secretaries of state are urging states to take action. For them, it often means ensuring that state safeguards keep pace with advances in online services for the business community.

Nevada, which is home to one of the largest numbers of corporate registrations in the nation, is unveiling its Nevada Business Portal this spring. The unique, new one-stop shop for business/government transactions will help guard against business identity theft by incorporating single sign-on and identity management elements in the online service. When fully launched, the portal will dramatically streamline the processes for establishing and maintaining corporate entities in the state.

Meanwhile, Colorado is establishing an optional password system for businesses on its corporate registration website, along with an e-mail alert system that will send electronic notice whenever a company's information is changed online. Georgia has already established a similar system for e-mail alerts.

The real challenge that lies ahead, secretaries of state said, is ensuring that business owners are aware of the relatively new risk of corporate identity theft, and getting them to sign up for e-mail alerts or password protections while checking their filings regularly.

"We are trying to protect businesses in every way that we can," said Nevada Secretary of State Ross Miller, "but this type of crime is relatively new and the methods of fraud are constantly changing. States need to engage multiple partners in their efforts, including the business community and registered agents, law enforcement, financial institutions and other industry stakeholders. Otherwise, the criminals will just figure out new ways to pull off this crime."

Miller pointed out that because catching the perpetrators of business identity theft can be difficult—and sometimes impossible if they are based overseas or moving from state to state—it is a wise investment strategy for states to focus on preventing such fraud.

Since nearly every state offers a searchable database that can tell users whether a company is in good standing and can identify the names and addresses of registered agents, Miller and his colleagues at the National Association of Secretaries of State are looking to form a business identity theft task force to focus on this issue.

"These business records are supposed to be used as a tool for commerce," says NASS Executive Director Leslie Reynolds. "While banks and other entities can use the information available on state websites for legitimate purposes in business transactions, the number of would-be criminals who are looking to exploit this information appears to be rapidly growing. It has raised some important policy implications for state officials."

Reynolds added states want to work together to combat corporate identity theft crimes, share strategies for communicating with the business community and others who deal with state business registrations and reporting, and discuss ideas for engaging law enforcement in helping to prevent or detect this type of fraud.

With an estimated 2 million corporate entities being formed in the U.S. each year, secretaries of

state have a compelling reason to work together on this issue. They will also look to state legislators, governors, attorneys general and other state leaders for assistance in protecting businesses and conducting proactive outreach on the risks of business identity theft.

"No state wants to become known as an easy target for corporate identity fraud when they are already facing financial hardships. Having a thriving business climate is vital to their economic health," Reynolds said.

Notes

[1] Greg T. Spielberg, Bloomberg Businessweek, "Taking on Small-Business Identity Theft," July 9, 2009, available at *http://www.businessweek.com/bwdaily/dnflash/content/jul2009/db2009079_858536.htm*.

[2] Dun & Bradstreet White Paper, "Tackling Corporate Identity Theft with a Public-Private Partnership," submitted to the National Association of Secretaries of State, February 2011, available at *http://www.nass.org/index.php?option=com_docman&task=doc_download&gid=1097*.

About the Author

Kay Stimson is director of communications and special projects for the National Association of Secretaries of State in Washington, D.C. A former television news reporter who covered the state legislatures in Maryland and South Carolina, she frequently writes about state and federal policy issues for lawmakers.