

CORPORATE IDENTITY THEFT PROTECTION



Introduction

Corporate identity theft, also called business identity theft, is a growing concern for Secretaries of State nationwide. Much like individual identity theft, corporate identity theft involves the exploitation of specific weaknesses in security in order to obtain fraudulent lines of credit, gain access to corporate credit cards and purchase expensive goods – all in the corporation's name. As of the most recent economic census, there were almost six (6) million small, to mid-sized businesses across the United States, creating staggering numbers of vulnerabilities for identity thieves to exploit.¹ Further, because of the lack of statutes in many states, as well as the jurisdictional challenges facing government agencies and authorities, prosecuting the perpetrators and recuperating damages is often difficult or impossible. The purpose of this white paper is the following:



- To educate readers about the problem of corporate identity theft
- To show how corporate identity theft can be detected by the Secretary of State's office
- To explain the importance of notifying potential victims immediately.

The Problem

Most business owners are aware of the potential for personal identity theft, and take measures to protect their own personal information and the personal information of their customers. However, many business owners do not know that the identity of the business is also susceptible to identity theft. Criminals have discovered it is often easier and more lucrative to target businesses, for identity theft, specifically small to mid-size companies, because they frequently have strong credit ratings.

There are many instances when a crime falls under the category of corporate identity theft. Criminals are coming up with increasingly creative ways to defraud businesses. Listed below are three real-world examples of corporate identity theft:

- 1) Identity thieves in California rented office space in the same buildings as their targets. After ordering merchandise and corporate credit cards using the legitimate business' name, they left the building before the victim realized its identity had been stolen.²
- 2) Criminals in Georgia purchased cell phones under the alias "Georgia Powers" in order to get unsuspecting customers to disclose credit card information.³
- 3) A Nevada man had the identity of his business stolen when another company changed the names of the company's officers by filing fraudulent documents with the Secretary of State's office in order to sell the business to a third party.⁴

The primary focus of this white paper is the type of corporate identity theft described in the third example. Because Secretary of State Offices are most often responsible for business filings and records, they are a frequent target by corporate identity thieves. Manipulating official data with the Secretary of State's office – whether by hacking or through falsified filings – gives criminals control of the corporate identity, authority and financial capacity. Secretaries of State also face challenges after corporate

identity theft is detected because few statutes exist regarding corporate identity theft, and coordination between various government authorities can be difficult (particularly when the crime is committed by someone overseas).

Role of the Secretary of State

The SOS office plays an important role in corporate identity theft. In many cases, it is the starting point for thieves attempting to steal a company's identity. Criminals understand that documents and records on file with the Secretary of State are used to prove existence, obtain lines of credit and designate business officers. While this is a useful, "one stop shop" for business owners, it can also be a vulnerability to be exposed by criminals.

Secretaries of State can be hindered by the scope of their authority. Many states have adopted the Model Business Corporation Act as a foundation for statutes regulating business filings, which limits the Secretary of State to a ministerial role with little discretion to review documents. As long as basic criteria are met, the Secretary of State has little power to question the legitimacy of business filings or changes made to records.⁴ Even after corporate identity theft is detected, few cases are prosecuted because of jurisdictional limitations and a lack of statutes. Identity thieves avoid legal consequences, and victims see little or no recuperation.

Although Secretaries of State face challenges in protecting corporations from identity theft, they are not defenseless. Business owners themselves are the Secretary of State's most important ally in preventing corporate identity theft. Business owners are not limited by state statutes and can review all filings and records carefully. They can get ahead of identity thieves and freeze lines of credit. They can contact credit bureaus and government authorities before identity theft is completed. This is only possible, however, if business owners are notified immediately when there is any attempt at stealing their business' identity.

The Importance of Notification

Timely notification of the victim is critical in combating corporate identity theft. Business owners have the most power when it comes to defending their assets, credit lines and identity, and the sooner they find out about attempted identity theft, the sooner they can begin protecting themselves. Using a corporation's stolen identity for fraudulent purposes takes time – but not much. The exact time between a false corporate filing with the Secretary of State and the opening of credit lines in the corporation's name (which is just one of the many ways identity thieves can use the stolen identity) would vary from case to case. Still, there is no doubt the earlier the business is notified, the better its chances are at minimizing any damage.

The Notification Process

When and how Secretaries of State choose to notify business owners of identity theft is an important decision. One method of notification currently gaining traction with Secretaries of State across the country is an automated email or text message system. This type of system has been implemented in Georgia and Colorado, with Colorado's Secretary of State predicting as high as 97 percent businesses subscribing to the service since January 2012.⁶

Automated Notification System

Specific functionalities of the notification system would vary from state to state. Each state has unique statutes regarding exactly what the Secretary of State's office can do, what information it can collect and who has access to the information. Still many fundamental characteristics of a notification system would benefit any Secretary of State's office. Explained below is how a basic, subscription-based notification system could work.

1. Service: Customers can be notified within 24 hours of any modifications made to information connected to their business
2. Data Elements Monitored: Name and address of business, registered principal's name and address, principals' names and addresses (Directors, Officers, Secretary, etc.)
3. Subscription
 1. Customer requests notification for a business entity by providing the entity number, first and last name, email address and phone number
 2. Pay fee
4. Alerts
 1. System creates a list of entities being monitored by subscribers
 2. Finds changes made to any monitored entities within the past 24 hours
 3. Logs the changes
 4. Sends an email or text message to the subscriber monitoring any entity that changed, specifying what the changes were
 5. Provides steps for the subscriber to take if the change was unauthorized

This is one example of a system states could use to notify business owners of a potential incident, and based on the potential impact corporate identity theft could have, businesses are willing to pay for a service like this with an annual fee. On many occasions, the alert email will simply serve as a confirmation to the business owner of a legitimate change made to a corporation's records. There will be times, however, when an owner is notified of an unauthorized change. The owner can then immediately begin to take defensive steps to stop any fraudulent activity.

Conclusion

It is unlikely the problem of corporate identity theft will be eliminated; however many states are taking the right preventative steps. One major initiative was the creation of the National Association of Secretaries of State Business Identity Theft Task force in 2011. This task force is studying business identity theft, developing preventative measures against business identity theft and offering guidance to states attempting to get ahead of the criminals. With the help of this task force, as well as vigilant Secretaries of State and well-informed business owners, corporations can be better protected from the risk of identity theft.

For more information, contact Ron Thornburgh or Barrett Gilbreath:

Ron Thornburgh
Senior Vice President of Business Development
NIC Sales and Marketing
25501 West Valley Parkway
Suite 300
Olathe, KS 66061
ront@egov.com

Barrett Gilbreath
General Manager
Alabama Interactive
3 S. Jackson Street
Montgomery, AL 36104
barrett@egov.com

Endnotes

¹"Statistics About Business Size," United States Census Bureau, 2008. Web. 26 June 2012.

²Spielberg, Greg T. "Taking On Small-Business Identity Theft," *Bloomberg Businessweek*, July 9, 2009.

³Rankin, Bill. "Scams more high-tech, vicious," *The Atlanta Journal-Constitution*, May 27, 2011.

⁴Norman, Jan. "Irvine businessman sues over corporate identity theft," *The Orange County Register*, May 21, 2008.

⁵"David Landau & Associates, LLC Uncovers Identity Theft, Corporate Impersonation," *PR Newswire*, September 8, 2011.

⁶National Association of Secretaries of State. *Developing State Solutions to Business Identity Theft*. By Scott Gessler and Elaine Marshall. Washington, DC: n.p., 2012.