

Developing State Solutions to Business Identity Theft



Assistance, Prevention, and Detection
Efforts by Secretary of State Offices

January 2012

National Association of Secretaries of State
444 North Capitol St., NW – Suite 401
Washington, DC 20001



Introduction

In October 2011, the National Association of Secretaries of State (NASS) held a national forum on business identity theft in Atlanta, Georgia, bringing together top advocates and experts from government and the private sector. The event was part of a NASS Business Identity Theft Task Force plan to develop proactive strategies for combating this relatively new type of crime. Secretaries of State and state business division directors attended the forum to learn how they could better protect the state-held information that offers a potential gateway to business identity theft. They wanted to discuss how they could work with law enforcement, financial institutions and business leaders in their state to educate all of the stakeholders about this type of crime. They were also interested in hearing about tools and technology that would aid in the detection and prevention of business identity theft, with best practices from private sector experts familiar with the issues.

Some states were already aware of the increasing number of business identity fraud cases involving unauthorized changes to business records on file with Secretary of State offices. Georgia and Colorado had both spent considerable time and effort implementing comprehensive response and prevention measures, and these offices had plenty of substantive advice to share with their peers. The resulting discussions provided forum participants with a better understanding of business identity theft, as well as fraud detection and prevention techniques. They also laid the groundwork for the development of a white paper that all Secretaries of State could use as a resource in combating business identity theft.

In keeping with this framework, this paper focuses on the establishment of business identity theft assistance, prevention, and detection efforts by Secretary of State offices through recommended policies and practices. It proposes a comprehensive approach to the growing problem of business identity theft, while highlighting the strategies that states can use to effectively protect entities from this type of fraud. One of the main goals of the NASS Business Identity Theft Task Force is to assist Secretaries of State and other public officials throughout the nation who want to get out in front of this emerging issue. By working with key stakeholders to develop an effective strategy that works for the specifics of each state, we can leverage our collective will and expertise to articulate the need for state action and public awareness. The key is finding the right balance between providing convenience to business owners as they update their business filings and hindering unauthorized access to such records.

Secretaries of State have good reason to work together to protect commercial documents and educate business owners on how they can reduce their chances of falling prey to identity thieves. By providing states with a resource that offers a greater understanding of the scope of this growing threat, we are confident that we can help make a difference.

Hon. Scott Gessler, Colorado

Hon. Elaine Marshall, North Carolina

Our Sponsors

NASS would like to recognize the following sponsors, whose support enabled the association to host the October 2011 Business Identity Theft Forum in Atlanta, which served as the basis for this white paper.



[CT Corporation](#)



[DataStream Content Solutions](#)



[Dun & Bradstreet](#)



[Identity Theft Protection Assoc.](#)



[INVISUS](#)



[Kaspersky Lab, Inc.](#)



[LifeLock, Inc.](#)



[NIC](#)



[Shred-it](#)

Contents

I. The Scope of Business Identity Theft for State Business Filing Offices.....	5
General Overview of Business Identity Theft	5
NASS Approach to Business Identity Theft	7
Role of Secretary of State Offices in Combating Business Identity Theft	8
Challenges in Tracking the Issue	9
II. Issues for Policymakers: Adopting Assistive and Protective Measures	10
A. Role of the Secretary of State	11
B. Issues Under State Law	11
C. Information Security Policies/Protocols	13
D. Other Issues	15
III. Recommendations & Integrated Approaches: Establish Best Practices & Increasing Awareness	15
Recommendation #1: Establish a Statewide Task Force on Business Identity Theft.....	16
Recommendation #2: Develop a State Action Plan	16
Recommendation #3: Establish a Notification Process for Businesses in Your State	17
Recommendation #4: Establish Clear Steps for Victim Assistance and Education	18
Recommendation #5: Conduct Outreach to Raise Awareness and Urge Preventive Action	19
IV. Summary.....	19
APPENDIX: NASS Business Identity Theft Forum Participants	21
Endnotes	23

I. The Scope of Business Identity Theft for State Business Filing Offices

General Overview of Business Identity Theft

As cases of personal identity theft have increased to record levels during the past few years, clever thieves have come up with newer, more lucrative tactics for carrying out identity fraud. One of these relatively recent tactics that is of great concern to Secretaries of State, the officials who oversee business filings on behalf of most states, is business identity theft. While business identity theft is a broad term that encompasses a wide variety of crimes involving the unauthorized use of a business' identity, the role of records housed by the state in carrying out this type of fraud are of paramount concern to this audience. As a result, this white paper seeks to shed light on the problem, highlight key issues for policy makers in confronting business identity theft, and promote recommended approaches and best practices for increasing public awareness.

As already noted, business identity theft is not just endemic to state business filing offices. The term "business identity theft" is frequently used to describe a wide variety of scenarios involving the fraudulent or unauthorized use of a company's identity, including the following:

- Identity thieves in New York used financial information obtained from corrupt bank employees to cash counterfeit payroll checks that were designed to look like they belonged to the victim organizations, which included corporations, hospitals, and government agencies.¹
- In California, criminals rented office space in the same building as a legitimate business, ordering corporate credit cards or retail merchandise in the businesses' name, and then disappeared by the time the business realized that its identity has been stolen.²
- A Nevada man claimed that the identity of his business was stolen after a company changed the name of the businesses' officers through filings with the Secretary of State's office, then sold the business to a third party.³
- In New Jersey, a company accused a former employee of corporate identity theft after the employee posed as the company on various social networking and business-related sites, all the while posting negative information about the company.⁴
- Large companies such as eBay, Microsoft, and VISA, have dealt with business identity theft carried out through "phishing" schemes where fraudulent emails purporting to be from legitimate, recognizable businesses seek personal or financial information from recipients.⁵
- In Tennessee, criminals have been creating phony web sites that impersonate the identity of legitimate car dealerships and advertise low prices in order to scam people into making deposits for vehicles that do not exist.⁶
- In Georgia, criminals purchased a cell phone, registered it under the name of "Georgia Powers" (which showed up on caller ID), and convinced a number of elderly people – who thought they were speaking with the utility company "Georgia Power" – to divulge their credit card data.⁷

All of these examples represent schemes that can be labeled business identity theft. However, the scope of this white paper is focused on business identity theft involving *the unauthorized alteration of business records filed with the Secretary of State's office in order to carry out fraudulent acts using the identity of the affected business.*

State trends make it very clear that criminals are looking to exploit state filing systems and business registration websites for financial gain. Typically, they try to file bogus reports with Secretary of State offices or manipulate online business records in order to steal sizeable amounts of cash and property using fraudulently obtained lines of credit. These fraudsters attempt to change the registered business address, appoint new officers, or change registered agent information on file with the state. Using altered records, which appear to indicate that they have the authority to act on behalf of a victim entity, the criminals can then apply for credit accounts with various retailers. While retailers will often check with business credit ratings agencies to verify that the information in an application is correct, it can be difficult to immediately detect that a crime has been committed because this information is based on the same Secretary of State business records that have been altered by the criminals.⁸

To date, Dun & Bradstreet has confirmed cases of business identity theft in at least 26 states. However, the exact number of business identity thefts involving altered state business records is not clear. There is currently no central repository for collecting this information. While the U.S. Federal Trade Commission does offer help for some business identity theft victims, it does not keep statistics on this specific problem. Even if the federal government did seek to do this, most states do not have a standardized method for reporting and tracking this type of crime, and businesses often fail to report it.

Thanks to the input of private sector experts and law enforcement representatives who are familiar with this issue and have shared their knowledge with NASS, it is possible to identify some of the characteristics that identity thieves look for in choosing their victims. Criminals tend to target small and mid-sized businesses with strong credit ratings, which can be easily identified through credit agencies. Businesses that are no longer in operation, often referred to as “dormant” or “dissolved” entities, are particularly vulnerable to this type of crime because their owners are less likely to be monitoring state-held business registration information. With the economic downturn that many states are currently facing, there are also more dormant companies to target.

It is also important to point out that not all instances of unauthorized changes to state business records are instances of business identity theft. Sometimes, a business or domestic dispute will lead one party to attempt to change filing records in order to establish authority over the business or another type of entity. Secretary of State offices have dealt with such disputes involving church parishes leaders, divorcing spouses and relatives with a stake in the family business. Changing entity ownership information on file with the state when there are questions about authorization to do so may not be criminal in nature, but instead the result of genuine disagreements about business ownership.

NASS Approach to Business Identity Theft

In the summer of 2010, Colorado officials started warning business owners about a sharp increase in business identity thefts involving altered business records that were accessible online as part of the Secretary of State office's business registration system. In a number of these cases, criminals 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 from various retailers, including Home Depot, Office Depot, Apple and Dell. Colorado authorities became aware of the 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 from Boulder to a virtual office in Aurora, where the fake business owners were forwarding the company's mail to another virtual office in California.⁹ By the time authorities were able to get a handle on this situation and others like it, the state had more than 300 businesses that had fallen victim to identity thieves, with total losses exceeding \$3.5 million.

Meanwhile, Georgia officials were also grappling with this issue. The Secretary of State's office began alerting businesses to the risks of business identity theft in 2010, after several cases in which state business records available online were altered and used to open fraudulent lines of credit. In one case, criminals used the identities of about 3,900 individuals and businesses to conduct more than \$5 million in fraudulent transactions. Another case involved the theft and misuse of identities for 149 individuals and nearly 200 companies in carrying out more than \$1.2 million in stolen goods. In both cases, criminals used forged business identities to obtain bank loans and lines of credit that allowed them to make a large number of expensive purchases, including high-end automobiles.¹⁰

Georgia and Colorado took swift action to address these crimes, developing task forces and working relationships with law enforcement that have served as a model for other states. The Secretaries of State also brought the issue to the attention of their colleagues.

As Secretaries of State collectively became aware that state-held business records were being used to perpetrate business identity theft, often with devastating consequences for victims, the members of the National Association of Secretaries of State (NASS) decided to take action against this growing threat. In April 2011, NASS announced the formation of the NASS Business Identity Theft Task Force, a major association initiative designed to study the issue of business identity theft and develop prevention strategies and practical, cost-effective tools and guidance for states. NASS President Beth Chapman of Alabama appointed North Carolina Secretary of State Elaine Marshall, a Democrat, and Colorado Secretary of State Scott Gessler, a Republican, to serve as task force co-chairs. The nineteen-member body, comprised of Secretaries of State who volunteered to be part of the association's work on this issue, represents all regions of the United States.

The idea of holding a national forum on business identity theft took hold during a task force meeting at the NASS 2011 Summer Conference in West Virginia. Members were eager to provide an opportunity for participants to hear about business identity theft from a wide variety of experts, including victims, private sector experts, and law enforcement officials. They also wanted to exchange ideas for improving intergovernmental coordination in the battle against this crime, and talk about issues that should be kept in mind when developing state identity theft prevention and assistance policies. Overall, the goal of task force members was to get out in front of the problem by developing a collective framework for state government action and awareness on this issue.

In October 2011, the task force hosted the first-of-its-kind NASS Business Identity Theft Forum in Atlanta, Georgia. The two-day event featured panels on the nature of business identity theft and how it occurs, trends in cyber crime, and risks to businesses. The importance of the business credit reporting process and the parameters of corporate law were covered, along with tips for assisting victims of identity theft. Participants learned about challenges for victimized businesses and law enforcement, outreach to the business community, methods for correcting fraudulent state business registrations, and private sector innovations to assist states. Fostering intergovernmental coordination, as well as sharing information on data access and security, were also major topics of discussion. The ideas and strategies discussed at the forum provide the basis for this white paper.

Role of Secretary of State Offices in Combating Business Identity Theft

Secretary of State Business Filing Duties

In most states, the Secretary of State is responsible for overseeing corporate registrations and other business filings, which is often done through the state business services division. These offices also manage the operation of state online business registration systems, which allow businesses and other entities to submit formation documents, review their records, and file updates and periodic reports via the Internet. While state law often restricts the Secretary of State's office to serving only as the official repository for state business documents and other filings, state business divisions and their online tools help to facilitate state commerce, provide significant convenience to businesses, and increase the efficiency of the filing process. These offices also work closely with the State Attorney General's office and other law enforcement officials when there is suspected fraud or other types of criminal wrongdoing that must be investigated and prosecuted.

One of the biggest challenges that Secretaries of State face when it comes to educating the public about business identity theft is explaining their legal limitations regarding reports of suspected criminal activity. As long as a document meets certain basic requirements, the Secretary of State's office often has little or no authority to question or reject its contents, to include changes that are made to business filings. Under the Model Business Corporation Act (MBCA), a model law that many states have used as a basis for their specific statutes that regulate business filing and company formation processes, the Secretary of State's corporate filing duties are part of a "ministerial" role with very limited discretion in

reviewing the contents of documents.¹¹ These offices also have no authority to control who can view or gain access to state business filings, which are public record.

While most state corporations divisions typically do not have statutory authority to investigate consumer complaints or allegations of criminal activity, including business identity theft, these officials cooperate with federal, state, and local law enforcement agencies that request their assistance.

Challenges in Tracking the Issue

While the NASS Business Identity Theft Task Force has focused on ways to prevent the alteration of business records by business identity thieves, members have discovered that developing prevention strategies can sometimes be a challenge without reliable data and statistics. Obtaining information on the prevalence of this type of crime, including the frequency with which it is reported and/or prosecuted, can be difficult. As a result, the task force has identified the following issues as potential challenges to fully understanding the scope of business identity theft:

Lack of Reporting

For starters, instances of business identity theft are difficult to track, in part because victims are reluctant to come forward and report this crime to authorities. Companies may be hesitant to talk about fraud due to the potential impact on brand image or shareholder reaction, and larger companies may be able to treat losses due to business identity theft as a bad-debt write off. As noted in a 2009 *Businessweek* article on this topic, “companies are required by federal law to notify consumers if their data have been breached, but not if the identity of the business itself was stolen.” That article also noted that “without laws and penalties for business identity theft, companies simply have no incentive to admit they've been defrauded.”¹²

Lack of Clear Data

Since crimes that might be considered business identity theft are often lumped in with other types of criminal fraud for reporting purposes, available statistics usually do not provide a clear picture about the frequency—or the pervasiveness—of business identity theft itself. This issue is further complicated by the fact that where any statistics on business identity theft are available, they are unlikely to separate out those schemes involving the use of altered business records held by the state.

Lack of Penalties / Regulations to Prosecute Business Identity Theft

Unlike consumer identity theft crimes, there are few statutes at the state or federal level that specifically target business identity theft. Business identity theft crimes involving interstate activity may be prosecuted at the federal level under various fraud statutes, but these laws may not adequately address the circumstances of business identity theft victims.¹³

Lack of Prosecution/Reporting

Few business identity theft cases are prosecuted because of a lack of state statutes. The fact that business identity theft crimes typically involve multiple law enforcement jurisdictions that may not be sharing relevant information with one another is another hindrance to this process. Additionally, the issue is difficult to track because there is no central repository for data on this type of fraud.

Tracking Activity Originating Outside the US.

Federal law enforcement authorities have reported to the NASS Business Identity theft Task Force that many business identity theft cases originate in countries outside of the U.S., making it more difficult for investigators to track and prosecute these crimes. Gathering evidence and even establishing jurisdiction can be major efforts when the perpetrators are based overseas. This issue underscores the reality that authentication and security features that Secretaries of State implement on the front end of the filing process will likely be more effective at combating the problem of business identity theft than some limited number of prosecutions that can be made in state or federal courts.

II. Issues for Policymakers: Adopting Assistive and Protective Measures

If there was one recurring piece of advice that participants from all backgrounds stressed during the NASS Business Identity Theft Forum, it was that Secretary of State offices would be well-served by focusing their attention and resources on business identity theft prevention and assistance measures above all else. With many state business services divisions constantly looking for new ways to enhance their processes for renewing an existing corporate entity, forming a new corporate entity, and communicating with corporate entities, it is only logical the these efforts might be carried out in conjunction with this work.

With many states now facing severe budget shortfalls and agency cutbacks, taking steps to determine the most practical, cost-effective strategies up front can yield important benefits. Preparation is key to engaging key stakeholders who can assist the Secretary of State's office in fighting business identity theft crimes and assisting victims. As busy legislatures grapple with a range of proposed identity theft laws and protections each session, they may not be thinking about the role of business entities in this legislation.

While there are specific questions that each state must ask in adopting new laws and policies to curb business identity theft, leaders should be prepared to identify the top issues under state law, examine information security policies and protocols, and identify other state-specific concerns that exist. These basic considerations could include the following:

A. Role of the Secretary of State

The role of the Secretary of State's office is important, particularly in light of any laws that limit the Secretary of State's discretion and authority over the business filing process. The ability of Secretaries of State to implement new policies and procedures to detect and prevent business identity theft will be dictated, to a large degree, by the state's legal parameters. Changing the law to expand the authority of the Secretary of State's office may be no easy feat, and in many states, this would be a radical change requiring significant financial resources and added personnel.

B. Issues Under State Law

State Law Definitions

Under the Model Business Corporation Act, the definition of "person" includes both an individual and a business entity. However, there are few state and federal laws that extend fraud protections to business entities. In 2006, California became the first state in the nation to expand its legal definition of "person" to apply to corporations and other business entities, giving law enforcement officials a new tool for prosecuting business identity theft cases. The new law helps facilitate investigations of business identity theft and provides a base for prosecution of these crimes.¹⁴

Treatment of Dissolved Entities

Given the frequency with which dissolved businesses are targets of business identity theft, states may want to evaluate their processes for reinstating dissolved entities. These are companies that have been legally dissolved, either voluntarily, or for failure to comply with state law. Dissolved entities can include businesses that simply decided to discontinue business operations, or entities that have failed (knowingly or unknowingly) to comply with ongoing reporting requirements, such as the filing of annual reports. Regardless of the circumstances that led to their dissolution, these entities seem to be particularly vulnerable to business identity theft. In Colorado, 80 percent of the state's 356 reported identity theft victims were delinquent or dissolved entities.

As a result of these issues, some states have sought to make the process of reinstating a dissolved entity more rigorous. For example, a corporation that was registered in North Dakota can only be reinstated by a court order after one year of being dissolved.¹⁵ Other states have prohibited the online reinstatement of dissolved entities.

However, states also need to keep in mind that some businesses simply forget to file annual or periodic reports, and may unwittingly end up with a dissolved entity designation. Additional requirements may create unnecessary burdens on those businesses that policy makers will need to consider.

Where the law permits, it may also be advantageous for a Secretary of State to conduct periodic reviews of these filings. The North Carolina Secretary of State's office recently learned of attempts to perpetrate

business identity theft involving unauthorized reinstatements of previously dissolved entities. Staff noticed that a number of revocation of dissolution filings included identical fax numbers and email addresses, sending up red flags. After reviewing four months' worth of voluntary dissolutions on file with the state, they contacted each person who filed the original dissolution papers and discovered that eight cases of business identity theft had, in fact, occurred. The Secretary of State's office took swift action to mitigate damages to potential victims, sending interrogatories to the officers of the newly-reinstated entities that must be answered and formally notarized. If the entity fails to respond, the Secretary of State has grounds for dissolving the entity.¹⁶

Review of Filings During Formation and Reporting

Some states may want to consider legislation giving the Secretary of State's office more discretion over the contents of a filing during the submission process, which is generally limited to ensuring that certain basic requirements are met (such as verifying that all lines on the form have been filled). Many Secretaries of State have long argued that they are not in a position, legally or resource-wise, to review or verify information that is provided in information documents and reports. Implementing new review procedures will likely require significant budgetary and personnel increases for the Secretary of State's office, which could be an unrealistic option for states facing budget shortfalls and staffing shortages. Additionally, some Secretaries of State point out that these new processes would also add to the time it takes for a business to file formation documents and annual reports.

Collection of Email Addresses for Notification Program

Email notification programs, which have been implemented in both Colorado and Georgia, enjoyed broad support at the NASS forum. Some Secretaries of State may need to seek legislative support to authorize an electronic contact (usually email) notification program, whereby an electronic notification is sent to anyone associated with a corporate entity each time some type of change is made to that entity's records. The notification typically asks each entity contact with an email address (or other type of electronic contact information) on file to review the entity's information, and ensure that the changed information is authorized and correct. In Georgia, a backup security feature permanently stores every email address added to an entity's record, ensuring that a person who attempts fraud cannot delete email addresses to block receipt of the notifications by the rightful entity contact. Colorado's Secretary of State has predicted that 97 percent of the state's active businesses will be signed up for the email notification program in that state by January 2012.

Reporting of Instances of Business Identity Theft

Secretaries of State may want to consider a standard reporting mechanism for business owners who suspect that their records have been illegally altered. This process may require legislation to implement a prescribed form or some other reporting procedure. Several forum participants suggested the potential benefits of developing a standard form that Secretaries of State could utilize for business identity theft reports, similar to what the Federal Trade Commission (FTC) currently provides for victims of consumer identity theft.

Process for Correcting/Restoring Business Record

Secretaries of State may want to pursue the adoption of legislation to establish or streamline the process for correcting or restoring business records that have been altered. During the NASS forum, many state officials expressed frustration with their lack of a clear mechanism for making changes to a record or correcting information.

Public Access to Email Addresses Collected Under Notification Program

Policymakers may need to establish how email addresses or other electronic contact information collected for the purpose of an electronic notification program will be treated under public records laws and other statutes. Some forum participants expressed concern about the collection of email addresses, because they would be considered public information and would, therefore, become publicly available.

Ability to Share Data with the Public, Other States, Federal Agencies (FTC)

State laws may need to be altered if they prevent or restrict a state from sharing data on business identity theft with law enforcement and other government authorities. In Georgia, for example, the Secretary of State's Office has entered into an information-sharing agreement with the Governor's Office of Consumer Protection, the state agency responsible for investigating corporate and personal identity theft. The agreement allows the Office of Consumer Protection to access corporate filing information to investigate and perform measures to proactively detect business identity theft and fraud.¹⁷

Prosecution of Business Identity Theft

Secretaries of State may want to support the creation and/or adoption of legislation to facilitate prosecution of business identity theft crimes involving business records. For example, as noted earlier, California's 2006 expansion of "person" to include corporations and business entities has helped facilitate prosecution of business identity theft cases in that state.

C. Information Security Policies/Protocols

During the discussions on state policymaking issues at the NASS Forum on Business Identity Theft, several key issues related to Secretary of State cyber and information security policies were a topic of focus. These issues include having the authority to make changes to security policies, establishing new policies and procedures designed to enhance security, and the importance of internal document security and handling practices. The fact that many state business divisions are working on increasingly limited budgets, staff size and financial resources may play a major role in the decision-making on what is cost-effective and realistic.

Authority to establish procedures and develop new processes

When considering the implementation of additional security policies or protocols, Secretaries of State must determine if the proposal is consistent with their authority and discretion to implement such

measures. The adoption of new measures to enhance the security of online records or the addition of features to reduce the potential for unauthorized access to records may be contingent upon who has authority to establish cyber and information security policies. While some Secretary offices have their own CIOs who are able to design and develop log-ins and other security features in-house, other Secretaries of State have to work with the office of the state's chief information officer, or another state-designated office, to follow the protocols of an established security framework. This may be more or less restrictive than a Secretary would like.

Establishment of cyber security policies & practices

States may need to explore ways to enhance security of online records and reduce the potential for unauthorized changes. States may want to consider implementing verification measures to prevent unauthorized access of business records, including the adoption of password protection systems, measures to confirm the identity of individuals making changes, and/or tools to verify whether an address is valid. Colorado is currently implementing a voluntary password protection system for business entities that will allow multiple users to access the business' records. The state appropriated nearly \$361,000 to implement the program, along with a full-time employee to manage the system. Forum participants noted the potential usefulness of verification programs that state filing offices could institute in order to confirm the identity of the individuals attempting to make changes to business records.

In West Virginia, business owners must enter a username and password to gain access to their business filing information and in order to update their annual reports they must enter a personal identification number issued each year by the Secretary of State's Office. And Nevada recently implemented the Nevada Business Portal, a one-stop site that will help guard against business identity theft by incorporating single sign-on and identity management elements in the online service. Additionally, discussion at the NASS Business Identity Theft Forum included the suggested practice of organizing a task force of stakeholders that use the state system and garner their input before making significant changes to their filing processes (i.e. registered agents, credit agencies, banks and other financial institutions).

Internal Information Security Policies

As increased security is applied to electronic systems and processes, criminals often modify their tactics to take advantage of weaknesses in other processes, such as physical or manual processes. Secretary of State offices may need to consider reviewing internal information security policies and protocols for the handling and access of hardcopy documents, including forms, applications, checks, and credit/debit card materials that contain sensitive personal information of business owners to minimize the risk of exposure through loss, theft, or unauthorized access. Such policies and protocols should address the complete lifecycle of the documents from initial receipt, processing and handling, retention and storage, to secure disposal. Staff whose job responsibilities include receipt, access, or handling of such hardcopy

documents should consider information security awareness training. Procedural changes to existing processes for enhanced security may require additional staff training.

Additionally, Secretary of State offices may want to consider fraud prevention training for frontline staff to assist in the detection of unusual or suspicious activity that may be an indication of attempted fraud. These red flags may include unusual forms of payment, suspicious identification, unusual filing activity in relation to previous business activity or history, or suspicious/unusual client behavior during the transaction. Forum participants noted that many attempted incidents of fraud can be stopped at the point of transaction by an alert and properly trained employee.

D. Other Issues

Data Mining, Data Matching, and Predictive Modeling

Secretaries of State may want to consider utilizing a number of data analysis tools that could provide assistance in detecting and preventing business identity theft. For example, if officials discover that a particular credit card has been used by identity thieves to alter business records, the database could be analyzed to determine if that credit card was used to make changes to other records. Also, tools could be implemented that monitor IP addresses used to change business records and identify red flags, including IP addresses from Russia or Mexico, or changes to 50 records in one day by the same IP address. Other red flags referenced at the NASS forum (but not necessarily indicative of illegal activity), include identifying address changes to out-of-state locations and identifying companies that have been reinstated with new officers after long periods of being dormant.

Provide Business Registrants with a List of ID Monitoring Services at Time of Registration

Secretaries of State may want to consider providing a list of various private companies that provide services to monitor business records for any unauthorized changes to each new business registrant. Some participants at the NASS Business Identity Theft Forum suggested that this would be an effective way to connect businesses with private companies that can provide monitoring services and other tools designed to detect and prevent business identity theft.

III. Recommendations & Integrated Approaches: Establish Best Practices & Increasing Awareness

After learning more about the issue of business identity theft and discussing various state strategies and solutions, NASS Business Identity Theft Forum participants identified several key recommendations that states could consider implementing in order to deal with this issue. These recommendations represent best practices for increasing awareness of business identity theft and instituting proactive measures to prevent it from occurring. Some of the recommendations, such as public outreach and collaboration with stakeholders, are relatively simple but effective approaches that can go a long way in helping to not only prevent business identity theft, but also by providing business with the knowledge of what to do if

they become a victim. Other recommendations may require legislation, new technology, or additional resources for implementation, and forum participants recognized that this may not be possible in some states. Regardless of which recommendations Secretaries of State are able to implement, the goal is to provide states with ideas and strategies they can utilize in crafting the most appropriate and effective approach to this issue.

Recommendation #1: Establish a Statewide Task Force on Business Identity Theft

Business identity theft forum participants really liked the Georgia Secretary of State's idea of collaborating with key stakeholders on business identity theft issues through the formation of a special task force. The Georgia office is collaborating with the U.S. Attorney's office in Atlanta and other state and local law enforcement entities as part of Northern District of Georgia Identity Theft Task Force. Therefore, another recommendation of this white paper is that states could develop a statewide task force dedicated to informing and educating the general business community about business identity theft. Activities of the task force might include the following:

- Reviewing state law and other state or local government practices to create an effective strategy for dealing with business identity theft
- Conducting joint outreach and training sessions with law enforcement
- Holding informational meetings with business organizations
- Developing informational materials for the public
- Publicizing changes to state law, or the introduction of new resources
- Establishing a Business Identity Theft Awareness Day, Week, or Month – or, conducting a business identity theft awareness campaign as part of the Better Business Bureau's National Identity Theft Prevention and Awareness Month in December, or the federal government's National Cyber Security Awareness Month in October
- Advocating for policy/regulatory changes that allow for prosecution of business identity theft crimes

Recommendation #2: Develop a State Action Plan

Secretaries of State need a clear plan of action in dealing with business identity theft, including a thorough understanding of the laws and policies that impact the state's ability to fight this type of crime. This planning process could include:

A. Legislative Action Plan

State legislation may be necessary for states to implement different tools and policies. If necessary, Secretaries of State could work closely with other state policymakers to determine how best to address these needs through legislative means.

B. Staff Training

Secretaries of State could take steps to ensure that staff members are well-versed on applicable policies and procedures concerning unauthorized changes to business records. This might include procedures for dealing with individuals who suspect they may be victims of business identity theft.

C. Data Collection/Management Procedures

States could consider various data collection tools or policies that can help prevent unauthorized changes to business records. Secretaries of State could work on developing protocols on the key areas of information that will be most needed. While the focus of most discussions at the NASS forum involved Web-based filings and online information changes, it is important to note fraudulent changes to records can also be carried out with paper forms mailed to the Secretary of State's office. Therefore, Secretaries of State should review their policies to consider paper-based fraud scenarios as well.

D. Data Sharing

Secretaries of State could consider sharing information with other states. This could include the development of a national repository or database that includes information about business identity theft victims. The FTC currently maintains a clearinghouse containing millions of individual consumer complaints about identity theft which allows law enforcement to find information about identity theft victims, identify other agencies involved in investigations, and spot identity theft trends and patterns.

F. Law Enforcement and Prosecution Contacts Lists and Training

Cooperation and communication with law enforcement is a vital aspect of preventing and responding to business identity theft cases. States could develop a contact list of all relevant local, state, and federal law enforcement agencies, and work with agencies on developing an action plan for preventing business identity theft and assisting potential victims. Consider regular training of law enforcement utilizing security experts from the public/private sectors.

Working closely with law enforcement has been a key component of efforts to combat business identity theft in Colorado, where the Secretary of State's office has partnered with the Colorado Bureau of Investigation, U.S. Secret Service, and U.S. Attorney's Office to share information and support business ID theft investigations.

Recommendation #3: Establish a Notification Process for Businesses in Your State

Notification programs that inform businesses of changes to their records can be an effective method for reducing instances of business identity theft and assisting potential victims of this crime. Participating businesses receive an email notification anytime their records are altered or updated. This step will allow them to review and detect any unauthorized changes, and potentially stop a business identity theft scheme before it unfolds. This can provide a business with an easy, yet very effective, means to prevent business identity theft. Both Colorado and Georgia implemented email notification following

business identity theft cases in those states. Secretary of State Brian Kemp of Georgia noted that the implementation of an email notification program requires a comprehensive outreach program to make businesses aware of the program and encourage them to sign up.

Prior to any email notification program, states can alert companies to the threat of business identity theft with regular filing-reminder mailings. Recently, Tennessee sent a flyer with their annual report filings reminder. The flyer, entitled "Protect Your Business from Identity Theft," included suggested practices for reviewing records, information on where to check business credit reporting records, and information about fraud liability limits and reporting requirements.

Recommendation #4: Establish Clear Steps for Victim Assistance and Education

One of the most important components of a business identity theft education programs is making sure that businesses know what steps to take if they become a victim of this crime. Businesses that find themselves in this situation will likely have many questions and concerns, including who to contact, how to correct their records, and how to repair any damage to their credit.

States may want to consider developing an informational Web page to help business owners understand the steps they need to take if they suspect that they have become a victim of business identity theft. This includes information on reporting the crime to law enforcement, notifying crediting reporting agencies, and contacting relevant financial institutions. California, Colorado, Georgia, and Ohio are among the states that currently provide a Web page with this information.

Any resources that states develop to assist businesses that suspect they have been targeted by identity thieves could include the following information:

- Notify local and/or state law enforcement officials
- Contact banks, credit card providers, and other relevant creditors to notify them of the fraud
- Report the issue to the business credit reporting agencies
- Place a fraud alert on business/merchant accounts
- Request copies of documentation used to fraudulently open or access accounts

Fraud reporting procedures

The FTC offers a complaint and affidavit form designed to assist victims of consumer identity theft in filing a report with law enforcement and dealing with credit agencies. This form may be something states could use as a guide in developing a reporting form for victims of business identity theft. NASS members may also want to consider developing a standard affidavit form that states could use for business identity theft reporting purposes.

Recommendation #5: Conduct Outreach to Raise Awareness and Urge Preventive Action

As the officials who typically oversee business filings on behalf of the states, Secretaries of State share the goal of engaging business owners in the state's processes. Education and outreach could be a key component of any business identity theft prevention plan, to include online resources, media campaigns, and meetings with chambers of commerce, rotary clubs, bar associations, and other relevant organizations. These efforts could highlight steps that businesses can take to prevent and respond to business identity theft.

Members could promote key tips for preventing business identity theft, including the following:

- File all reports and renewals with state filing offices in a timely manner
- Regularly check business records to make sure information is accurate
- Continue checking business records, even if the business is no longer operating
- Sign up for email notifications and utilize password protection where available
- Contact the Secretary of State if unauthorized changes have been made to business records
- Monitor billing records and accounts for suspicious or unauthorized transactions
- Monitor business credit information with Dun & Bradstreet and other credit reporting agencies

Recognizing that Secretaries of State can make the greatest impact by focusing on state and local stakeholders, there is also a need for coordinated education and awareness efforts at the national level that can be carried out by NASS and partner organizations. As part of these broader efforts to reach the business community and increase awareness of business identity theft, states can work with NASS and the Identity Theft Protection Association, which have developed a new website dedicated to this issue: www.BusinessIDTheft.org.

IV. Summary

Secretaries of State have the opportunity to be at the forefront of efforts to curb the recent trend of business identity theft involving altered business records. While the scope of these crimes is not clear, the damage caused by the schemes uncovered in Colorado and Georgia, and the relative ease with which these crimes were carried out, underscores the importance of taking proactive measures to prevent similar crimes from occurring in other states.

The prevention and detection measures discussed in this white paper are tools that Secretary of State offices throughout the country may want to consider in dealing with the issue of business identity theft. How each state ultimately decides to approach this issue will depend on a number of factors, including the Secretary of State's authority, legal restrictions, privacy concerns, funding availability, staff size, technological capabilities, and filing procedures. Some states may need or desire to take a multifaceted

approach utilizing email notification, password protection, and data mining. For others, the best approach might be to focus on education and outreach with the business community through direct stakeholder outreach and online resources.

By having a strategy in place, and working together with law enforcement, the business community, and the private sector, Secretaries of State can be part of the collective effort to prevent businesses throughout the nation from becoming victims of business identity theft schemes.

APPENDIX: NASS Business Identity Theft Forum Participants

NASS Business Identity Theft Task Force Members

Hon. Scott Gessler, Colorado Secretary of State - Task Force Co-Chair
Hon. Elaine Marshall, North Carolina Secretary of State – Task Force Co-Chair
Hon. Beth Chapman, Alabama Secretary of State
Hon. Debra Bowen, California Secretary of State
Hon. Kurt Browning, Florida Secretary of State
Hon. Jim Condos, Vermont Secretary of State
Hon. Jason Gant, South Dakota Secretary of State
Hon. Mark Hammond, South Carolina Secretary of State
Hon. Tre Hargett, Tennessee Secretary of State
Hon. Brian Kemp, Georgia Secretary of State
Hon. Ross Miller, Nevada Secretary of State
Hon. Charles Summers, Maine Secretary of State
Hon. Natalie Tennant, West Virginia Secretary of State

Panelists

Bruce Andrew, Vice President, Marketing, Shred-It
Michael Barnett, Executive Director, Identity Theft Protection Assoc.
Robert Beckett, Government Business Development, Dun & Bradstreet
Greg Brown, Vice President of Strategic Development, DataStream Content Solutions
Jeanne Canavan, Assistant District Attorney, DeKalb County Georgia
William Clark, Jr., Partner, Drinker Biddle & Reath LLP
Todd Davis, CEO, LifeLock, Inc.
Charlene Dawkins, Government Relations Manager, CT Corporation
Kim Duncan, First Vice President, SunTrust Bank
James Harrison, CEO, INVISUS
Brent Hoffman, General Manager, Nebraska.gov/NIC
Cindy Liebes, Regional Director, Southeast, Federal Trade Commission
Monty Mohr, Director of Criminal Investigations, Governor's Office of Consumer Protection, State of Georgia
Ray Moore, Special Agent in Charge of Atlanta Office, U.S. Secret Service
Gary Mullen, Vice President Corporate Marketing, Kaspersky Lab, Inc.
Mark Reardon, Chief Information Security Officer, Georgia Technology Authority
Bob Sullivan, Senior Writer, Technology Sector, MSNBC
Malcolm Wiley, Assistant Special Agent in Charge of Atlanta Office, U.S. Secret Service

Attendees

Scott Anderson, Deputy Secretary of State, Office of the Nevada Secretary of State
Dan Burke, Vice President, U.S. Sales, Kaspersky Lab, Inc.
Clarissa Cerda, Senior Vice President, LifeLock, Inc.
Penny Barker, Business & Licensing Manager, Office of the West Virginia Secretary of State
Tanja Battle, Director of Registration, Office of the Georgia Secretary of State
Nathan Burton, Director of Business Services, Office of the Tennessee Secretary of State
Matt Carrothers, Director of Media Relations, Office of the Georgia Secretary of State
Theresa Carter, Constituent Services Representative, Office of the Georgia Secretary of State
Jeshua Caudle, Systems Engineer, Office of the Kentucky Secretary of State
Michelle Day, Assistant Secretary of State, Office of the Oklahoma Secretary of State
Allen Eskridge, Assistant Secretary of State, Office of the Kentucky Secretary of State
Kelly Farr, Deputy Secretary of State, Office of the Georgia Secretary of State
Cyndi Festa, Global Information Services Leader, Dun & Bradstreet
Tim Fleming, Chief of Staff, Office of the Georgia Secretary of State
Beth Fraser, Director of Governmental Affairs, Office of the Minnesota Secretary of State
Don Habeger, Director of the Division of Corporations, Office of the Alaska Lieutenant Governor
Mike Hardin, Director of Business & Licensing, Office of the Colorado Secretary of State
Mona Hart, General Counsel, Office of the Tennessee Secretary of State
Chris Harvey, Chief Investigator, Office of the Georgia Secretary of State
Mike Lauritsen, Director of Business Services, Office of the South Dakota Secretary of State
Jessica Monk, Special Assistant, Office of the Georgia Secretary of State
Cheri Myers, Director of Corporations, Office of the North Carolina Secretary of State
Tom Riley, Assistant Secretary of State, Office of the Mississippi Secretary of State
Vincent Russo, General Counsel, Office of the Georgia Secretary of State
Mike Smith, Director of Communications, Georgia Superior Court Clerks' Cooperative Authority
Terry Sosebee, Special Agent in Charge, Georgia Bureau of Investigation
Ron Thornburgh, Senior Vice President of Business Development, NIC
Randy Vaughn, Chief Innovation Officer, Office of the Georgia Secretary of State
John Waters, Assistant Director, Elections Division, Office of the Georgia Secretary of State
Sheridan Watson, Communications & Outreach, Office of the Georgia Secretary of State
April Wright, Corporations Section Administrator, Office of the Delaware Secretary of State
Tom Wrosch, Commercial Registries Manager, Office of the Oregon Secretary of State

Endnotes

- ¹ Miller, Chuck. "Identity theft ring busted in New York," *SC Magazine*, May 28, 2009.
- ² Spielberg, Greg T. "Taking On Small-Business Identity Theft," *Bloomberg Businessweek*, July 9, 2009.
- ³ Norman, Jan. "Irvine businessman sues over corporate identity theft," *The Orange County Register*, May 21, 2008.
- ⁴ "David Landau & Associates, LLC Uncovers Identity Theft, Corporate Impersonation," *PR Newswire*, Sept. 8, 2011.
- ⁵ Edwards, John. "Preventing Business Identity Theft," *CFO*, May 19, 2004
- ⁶ Ransom, Kevin. "Stolen Dealer Identity Baiting Car Shoppers," *AOL Autos*, August 4, 2010.
- ⁷ Rankin, Bill. "Scams more high-tech, vicious," *The Atlanta Journal-Constitution*, May 27, 2011.
- ⁸ Migoya, David. "Corporate ID thieves mining the store," *The Denver Post*, Sept. 23, 2010.
- ⁹ Vijayan, Jaikumar. "Colorado warns of major corporate ID theft scam," *Computerworld*, July 16, 2010.
- ¹⁰ Vijayan, Jaikumar. "Corporate ID theft hits Georgia businesses," *Computerworld*, July 22, 2010.
- ¹¹ Model Bus. Corp. Act § 1.25. Comment 1.
- ¹² Spielberg, Greg T. "Taking On Small-Business Identity Theft," *Bloomberg Businessweek*, July 9, 2009.
- ¹³ Tozzi, John. "Identity Theft: The Business Bust-Out," *Bloomberg Businessweek*, July 23, 2007.
- ¹⁴ Spielberg, Greg T. "Taking On Small-Business Identity Theft," *Bloomberg Businessweek*, July 9, 2009.
- ¹⁵ See N.D. Cent. Code § 10-19.1-148
- ¹⁶ North Carolina example is based on the state's response to the January 2012 IACA survey.
- ¹⁷ Williams, Dave. "Georgia takes aim at business identity theft," *Atlanta Business Chronicle*, Dec. 2, 2011.