BUSINESS IDENTITY THEFT

IN THE U.S.

2018 REPORT

THE NATIONAL CYBERSECURITY SOCIETY

Prepared By:

The National Cybersecurity Society
1215 31st Street, N.W. #3921
Washington, D.C. 20027

EXECUTIVE SUMMARY

The National Cybersecurity Society (NCSS) has prepared *"Business Identity Theft In The U.S."*, to lay the foundation for an effective and sustainable national program to assist victims of business identity theft. The study presented in this report analyzes the current ecosystem of participants – federal, state and the private sector; defines types of business identity theft; the mechanisms in place to define the identity of the business; how vulnerabilities are exploited; and recommendations to improve victim resources.

The analysis uncovered there is no standard set of information used by all credit reporting agencies, or federal and state governments that define the identity of a business. Without a standard set of data elements, it is difficult to definitively recommend which data needs to be protected. Coupled with the fact that today all business identifying information is public, the real question emerges…..what should be the ***standard*** for identity data and will protecting it safeguard identity?

The types of business identity theft addressed are: financial fraud, tax fraud, trademark ransom and website defacement. While some business identity data can be found in paper records, the majority of the data stolen or compromised resides in online systems – and it is easy to find data on businesses. Various online systems maintain information on where a business is located, the name of the business owner, revenue, number of employees, their Tax ID number, credit worthiness and registered agent. State registries found an increase in business identity theft after business records became electronic. Criminals are changing business records to their advantage – even as simple as a change of delivery address so that illegally purchased goods can be ordered and delivered without an owner's knowledge until of course -- the bill arrives. Consequently, the fraudulent purchase remains on the business' line of credit and requires a significant investment in time and resources to reverse the charge.

Current statutes such as the Fair Credit Reporting Act -- protect consumers, not businesses. No single government agency is in charge of collecting statistics on this type of crime, nor is their consistent guidance on "who to call when you become a victim". While commercial credit reporting agencies are motivated to collect and provide the most accurate information available -- given the dynamic nature of commercial data -- the inaccuracies are almost a certainty. Moreover, there is no easy or systematic way for a business entity to address issues related to accuracy, completeness or relevancy in the reported information.

For 2016, the Internet Crime Complaint Center reported identity theft as the seventh largest crime type based upon the number of victims, at 16,878 victims and with extortion ranking sixth at 17,146 victims – and the victim loss for identity theft was reported at $58.9 million[i]. These statistics address consumer identity theft and while the identity theft resources for consumers are significant, there are few resources for businesses. From interviews conducted by the NCSS for this report, several agencies indicated that they believe business identity theft crime data is included in the total numbers of identity theft maintained by the FTC and the FBI.

Business identity theft involves a complex set of players, systems, processes and statutes. It appears a national level forum or task force with participants from government (federal/state/local/tribal/territorial), the financial services industry and the private sector might be created to discuss solutions. Improved coordination methods among the states and the federal government would play a significant part in thwarting crime – just like the Social Security Administration shares identity data with the Department of Motor Vehicles. Another suggestion would be to improve verification and validation of business identity data through a national business registry similar to what is occurring in Canada. However, finding support and the resources to tackle this threat may be a hurdle too difficult to achieve given the many needs facing the business community today. What is needed is an industry leader with the resources to sustain a multi-year task force effort – to mobilize all the players in this space.

During our discussions, many leaders indicated that they had seen an increase in the crimes involving business identity, but did not have a sense of how bad it is. The IRS stated that identity theft is "big business" for criminals. Combining stolen data from data breaches with business intelligence to create large tax returns; wire transfers and ransoms are fueling an underground economy of organized crime. In the state of Ohio, the business registry office found instances where criminals are selling business identity data as a "package". The opportunity cost of allowing this crime to go unabated is not an option. We believe changes in state business registry processes; a more informed and proactive business community; and an interagency task force might be the leading elements of change needed. The NCSS looks forward to continuing the dialogue with our partners to find ways to protect businesses from this type of cyber crime and increase victim services throughout the U.S.

1 IRS has recently initiated efforts to redact EINs on some tax records.

TABLE OF CONTENTS

BACKGROUND

In October 2017, the Identity Theft Resource Center selected the National Cybersecurity Society (NCSS), as one of six sub-grantees, to lead a national coalition under the auspices of the National Identity Theft Victims Assistance Network (NITVAN). NITVAN is a network of coalitions across the country engaged in creating, enhancing and delivering identity theft and identity-related cybercrime victim assistance training and outreach to improve the ability to provide direct victim assistance services. The program provides resources to establish and augment the work of regional, statewide and community-based coalitions, with an emphasis on threats from cyberspace. Through a national network, the ultimate goal is to provide training, technical assistance and policy guidance to victims of identity theft and cybercrime. Funding for this award is derived from the U.S. Department of Justice, Office for Victims of Crime, through the Crime Victims Fund. This unique fund is financed by fines and penalties paid by convicted federal offenders, not from tax dollars.

As a coalition leader for small business, the NCSS project plan includes collaborating with others in the ecosystem to design a long-term business identity theft and cybercrime resource system encompassing training, outreach and best practices. While the focus will be on small business – businesses of all sizes will benefit from the resources that will be provided. All educational materials and related tools developed will be widely available to the public and through coalition members to assist victims of cybercrime. This paper, Business Identity Theft in the U.S., analyzes the current ecosystem; the issues surrounding business identity theft; how vulnerabilities are exploited; and recommendations to improve the resources to support victims. Intended outcomes include education and outreach, improved victim services and identification of best practices.

PURPOSE

The National Cybersecurity Society (NCSS) has prepared this report to lay the foundation of an effective and sustainable national program to assist victims of business identity theft. Through the grant, the NCSS plans to identify victim assistance services at the state, federal and national level; to educate the business community on how to protect themselves; and to share information on how to respond in the event they become a victim. The intent of this effort is to increase victim resources and to expand the network of coalition partners who can assist victims.

The project will include: analyzing available resources to support businesses; identifying what gaps exist in victim assistance services; developing resources for businesses; building a coalition and delivering educational content. Resources will include information about the types of business identity theft; protection measures and steps to take in the event the business falls victim to this type of crime.

BUSINESS IDENTITY THEFT

WHAT IS IT?

The Federal Trade Commission defines identity theft as a fraud that is committed or attempted, using a person's identifying information without authority[ii]. The Department of Justice's Office for Victims of Crime, defines business identity theft as a type of identity theft committed with the intent to defraud or hurt a business (e. g. financial business identity, extortion[iii]). Similarly, the Internal Revenue Service (IRS) defines business identity theft as creating, using or attempting to use businesses' identifying information without authority to obtain tax benefits[iv].

Through research and analysis, four types of business identity theft emerged:

A. Financial Fraud – obtaining new lines of credit, loans or credit cards; UCC fraudulent filings;

B. Tax Fraud – filing fraudulent returns using tax subsidies or obtaining refunds from federal and state governments;

C. Website Defacement – by manipulating a business's identity on the web;

D. Trademark Ransom – registering the business name as an official trademark and demanding a ransom for release of the trademarked business name.

In 2010, state officials in Colorado and Georgia began warning business owners about an increase in unauthorized changes that were accessible online as part of the business filing 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.

Using credit reporting agency data the thieves easily target businesses with good credit ratings and/or find businesses that are no longer in operation. Unlike consumer credit card fraud, the payoff for stolen business credit is huge – in one case criminals used forged business identities to obtain bank loans and lines of credit allowing them to make a number of large and expensive purchases, including high-end automobiles[v].

Another type of financial fraud includes fraudulent Uniform Commercial Code (UCC) filings. Criminals and activists file bogus financial statements and real property liens impacting a business entity's credit rating. Activists target government officials, corporations, and banks (or their employees) as a response to a perceived injustice. Victims may spend years battling these false claims, and some may not even realize they have been targeted until they attempt to conduct a property transaction, or open a line of credit. Financing statements filed to harass a target victim often falsely indicate that the "debtor" owes large sums of money to the filer or purported "secured party." Harassment filings have become more common in the past decade as more criminals have learned about these tactics and adopted them in large numbers[vi].

At the IRS, business identity thieves file fraudulent business returns to receive refundable business credits or refunds. In November 2014, the IRS Advisory Council raised concerns with business identity theft and issued the following statement:

> "Business identity theft can be more complex than individual identity theft and….. can occur in many ways. A fraudulent business entity tax return can be filed that generates a larger refund than would be obtained on an individual income tax return due to available refundable tax credits, or fraudulent W-2 forms with fictitious withholding may be filed and the information subsequently used to file multiple fraudulent individual income tax returns claiming refunds. Similar to individual identity theft, business identity theft also impacts the banking and business communities. Because of the potentially larger payoffs available, business identity theft is on the rise[vii]."

BUSINESS IDENTITY THEFT CONTINUED

The IRS provided these examples of business identity theft to include:

- Using the EIN of an active or inactive business without permission or knowledge of the EIN's owner to obtain a fraudulent refund;
- Using an EIN of an active or inactive business without permission or knowledge to file fraudulent Forms 941, Employer's Quarterly Federal Tax Return, or Forms W-2, Wage and Tax Statement, to support bogus Forms 1040, U.S Individual Income Tax Return, claiming a fraudulent refund;
- Applying for and obtaining an EIN using the name and Social Security Number of another individual as the responsible party without their approval or knowledge to file fraudulent tax returns (e.g. Form 941, Form 1120 or Form 1041, U.S. Income Tax Return for Estates and Trusts), avoid paying taxes, obtain a refund, or further perpetuate individual identity theft or refund fraud;
- Filing an individual return claiming refundable business credits which increase the amount of the refund[viii].

The IRS logged 4000 business identity theft cases in 2016, and through June 2017, it logged 10,000 cases. Although 10,000 may seem like a low number, business identity theft caused $268 million in damages for 2016, up $122 million from 2015, and by 2017 damages were approximately $137 million[x].

State tax authorities report similar frauds, and state tax systems were built for speed and efficiency of processing tax refunds, not to screen for fraud or fabricated identities. The state of Indiana testified before Congress in 2015, that tax ID theft had escalated dramatically over the last two years, and through their investigative efforts stopped more than $88 million in fraudulent refunds[xi].

The third type of business identity theft is through spoofed or compromised websites. Cyber criminals steal or hack a business's website – in essence their identity on the Internet. Compromised websites are used for a number of reasons – to redirect traffic to a hacker's spurious website; steal customer data including payment and email information; host malware, spam pages, and/or porn; advertise illicit products; or simply vandalize the site. Ransomware, a type of malware, has become the latest threat to the business community - whereby criminals lock or vandalize the website and demand a ransom before the website can be put back into use. In this case, malicious actors make it plainly obvious through pictures and threatening text, which warn users that the site has been "hacked", impacting the business's ability to conduct business via the web as well as damaging their reputation.

In some cases, the compromised websites go undetected for months. An experienced hacker will work hard to ensure the infected site goes undetected for the longest possible period in order to leverage the good name and identity of the business. Some businesses do identify a hacked website earlier, and when it comes to mitigating the damage, knowing you are a victim as early as possible is critically important.

IRS notes in the past year (2017), they have seen a 250% increase in the number of fraudulent returns to include filings for partnerships, estates and trusts. The IRS commented in a recent article published during National Tax Security Week:

> "Small business identity theft is a big business for identity thieves. Just like individuals, businesses may have their identities stolen and their sensitive information used to open credit card accounts or used to file fraudulent tax returns for bogus refunds[ix]."

BUSINESS IDENTITY THEFT CONTINUED

When Commtouch, a cloud based security firm, surveyed businesses to understand the scope of website defacement and fraud, nearly half of respondents were notified about the compromise when they tried visiting their own sites[xii]. Business owners who have been the victim of this type of crime can submit a complaint to the Internet Crime Complaint Center (IC3) of the FBI, however website compromise or defacement is not listed as a separate crime from ransomware or misrepresentation.

The fourth type of business identity theft involves the business name. Fraudsters identify businesses that have not adequately protected their company's name by filing with the U.S. Patent and Trademark Office. Criminals file the requisite application, obtain the trademark, then notify the company that they are using their trademark illegally, and demand a ransom to release the trademark. Interviews with state officials identified this crime and it is unclear how prevalent this activity is.

In 2016, IC3 reported a new crime called business email compromise or BEC. Business email compromise is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments[xiii]. This type of fraud (a type of phishing threat) involves compromised email accounts of company officials to convince employees to take a specific action, such as send employee W-2s, wire transfers to offshore accounts or send account information. The latest statistics report a 270% increase in identified victims and total exposed loses, at $1.2 billion[xiv]. In a way, this type of crime is using the known identity of an organization's leadership, their habits and established relationships with their employees to entice employees to take action. Using a CEO's known traits, practices and work schedule, these fraudsters leverage the known identity of the person and the business to craft their exploit. Emails lure employees to quickly respond to the boss, often without questioning the direction given. While not true business identity theft, BEC leverages known "identity" traits and mannerisms of the business and its leadership to conduct the crime.

HOW BAD IS IT?

Everyone we interviewed indicated business identity theft is on the rise, due to the lucrative financial rewards for the criminal. Interviews with a large U.S. financial institution's fraud department indicated they have seen a 200% increase in wire transfers through business email compromise. Business email compromise losses in 2018 exceed several billion dollars -- a rise in the number of businesses falling victim to this type of phishing scam.

In the 2015 Treasury Inspector General for Tax Administration (TIGTA) report, the IRS had identified 233 business tax returns that were filed using known or suspicious EINs of which 97 claimed refunds exceeding $2.5 million. Recognizing that the IRS has identified over 6,175 suspicious EINs in its registry, the audit team recommended that better processing filters be developed to identify more suspicious returns. Moreover the audit recommended additional work was needed to alert the public and state offices of the rise in business identity theft.

In 2018, Dun & Bradstreet reported a significant increase in business identity theft for the six-year period starting in 2007 and peaking in 2012; with a decline during the years of 2013-2015. Yet in 2016, increases began again, with a sharp increase in 2017 -- up 46% year-over-year which represents the largest increase of any year since tracking began in 2005. The cities where the largest number of business identity theft occurred were: Las Vegas, Los Angeles, Miami, Atlanta, Houston and New York (2013-2015). The most frequent types of businesses impacted by business identity theft included: business services, management consulting, health and allied services, accounting and bookkeeping, elementary and secondary schools and construction firms. While most business identity thefts tracked by Dun & Bradstreet are for active companies, inactive, or dormant entities are often targets as well. In discussions with representatives from International Association of Commercial Administrators, IACA, and the IRS, they noted dormant or defunct businesses represent a significant opportunity for criminals. In one case, a criminal stole an identity of a business that had been defunct for over 15 years – submitting a business application for reinstatement to a state registry. Under the Model Business Corporation Act (MBCA), state registries cannot reject a reinstatement application.

Commercial credit reporting agencies play a unique role in the ecosystem because of their trusted broker role between businesses and financial institutions.

BUSINESS IDENTITY THEFT CONTINUED

Credit reporting agencies facilitate commerce across the U.S. and hold critical data on business history, identity data and financial stability. Business credit reporting agencies help not only in reviewing and assessing the creditworthiness of a business, but can also help in identifying appropriate data elements to define business identity as well as assist in supporting victims of identity theft.

Over the years, Congress has reviewed the Fair Credit Reporting Act and has never found the need to expand the law to cover commercial credit reporting agencies because of the trusted broker role.

The FBI collects data on consumer identity theft, not business identity theft. We have learned that the FBI won't investigate a business identity theft unless it involves organized crime or exceeds $100,000. Similarly, the U.S. Secret Service (USSS) did not provide data on business identity theft, even though OVC-TTAC states they are the lead agency charged with investigating identity theft that impacts the nation's financial systems. The USSS investigates criminal violations such as computer fraud, access device fraud and computer based attacks on financial banking systems and telecommunications infrastructure[xv].

As part of the National Association of Secretaries of State, (NASS) report in 2012, Georgia officials began alerting businesses due to the rise of the number of cases of business records being modified. In one case, criminals used nearly 3,900 individuals and businesses to conduct more that $5 million in fraudulent transactions. In another case, over 200 companies were compromised and over $1.2 million of goods stolen[xvi]. The State of Colorado reported similar losses and had over 300 businesses with loses over $3.5 million[xvii].

The IC3 collects complaints on Internet crime, which includes BEC, ransomware, tech support fraud, and extortion. In 2016, the IC3 received 298,728 complaints with reported losses in excess of $1.3 billion[xviii]. For 2016, the IC3 reported identity theft as the seventh largest crime type based upon the number of victims, at 16,878 victims and with extortion ranking sixth at 17,146 victims. The victim loss for identity theft was reported at $58.9 million and business email compromise at a loss of $360.5 million[xix]. IC3 does not collect data on business identity theft.

Currently, there is no central law enforcement agency collecting data on business identity theft, nor a central agency for victims to report or complain their business has been the victim of identity theft. Dun & Bradstreet reports that business identity theft cases seldom get the necessary attention of law enforcement and almost never are prosecuted.

The IRS has recognized business identity theft as a significant issue and plans to continue to audit this area to uncover any new trends and patterns.

Previous IRS audit recommendations have included:

1. Defining business identity theft;
2. Educating the public and tax preparers;
3. Improving filtering mechanisms;
4. Collecting and tracking metrics;
5. Implementing EIN e-authentication systems to verify the identity of a person requesting an EIN.

Lastly, federal law enforcement includes business identity theft under the crime category of identity theft. Without hard data on this type of theft, it is unclear "how bad it is". Yet, ask any small business owner how destructive it is to lose their hard-earned good credit standing – which has taken years to build – it's devastating. Goods purchased through stolen credit can take months to resolve, at which time the business has to carry the debt – either pay the balance to maintain their credit rating or not pay it, impacting their company's credit worthiness. In interviews with small business owners, business credit plays a major role in financing and sustaining their livelihood.

IDENTITY MANAGEMENT FOR BUSINESS

In terms of IT security, identity management is the organizational process for identifying, authenticating and authorizing individuals or groups of people to have access to applications, systems, networks and/or physical assets. The elements that define user identity are based on the system or systems to be accessed, and include both sensitive and non-sensitive data. Sensitive data or Personally Identifiable Information, (PII) is data that is unique to the individual – that if combined with non-sensitive data can distinguish one person over another. Unauthorized release and compromise of sensitive PII data is what defines a data breach.

Data used to identify a business's identity contains public, non-sensitive data. Examples of identity data for businesses are fictitious name, or "doing business name", or DBA, owner's name, legal entity type, address, county, state, registered agent, effective date of establishment or website address (url). Identity data for businesses is publicly available through a variety of means, such as state records, Dun & Bradstreet and other online search engine resources such as Google or Yellow Pages. State and private sector systems often provide access to the data if a user has in his/her possession some business data elements. Often these "known" data elements are used to verify the identity of the user. Moreover, the ability to change the data is considered by state officials as an effective and efficient manner to manage these public records -- as businesses often change ownership, move or change registered agent. Even though these records are public, one measure many states have implemented is restricting access to those wishing to update these records by requiring user name and password[xx]. Some state systems send a notification email to the owner of the record notifying them that the business record has changed[2]. Adding an email "alert" to the owner of the record provides a layer of additional protection, but requires the business owner to opt in for the service. Business owners need to informed and encouraged to take proactive steps to manage these records.

The state of Colorado has added two-factor authentication to verify users, which acts as a second means to authenticate users. Two-factor authentication is recognized as an industry cybersecurity best practice.

EMPLOYER IDENTIFICATION NUMBERS (EINs)

The Internal Revenue Service issues Employer Identification Numbers (EINs) or Tax IDs and the primary purpose of the EIN is for tax administration. EINs are not required if a person operates a sole proprietorship or any limited liability corporation without employees. In the case of a sole proprietorship, the owner uses his or her social security number.

Once an EIN is assigned to a business entity, it becomes the permanent Federal taxpayer identification number and is never cancelled, reused or reassigned to another business entity.

Under certain circumstances, the IRS requires businesses to obtain a new EIN when ownership or the structure of the business has changed. The IRS states that although changing the name of the business does not require a new EIN, owners may wish to contact the IRS or visit the Business Name Change on their website to find out what actions are required if the name of the business has changed.

EINs are printed on all Forms 1099 used by vendors, investors, individual's and/businesses as well as on each employee W2. Free EIN lookups are available on the Internet. EINs are used to open bank accounts, file and obtain business licenses or obtain a line of credit. EINs are not identified as sensitive data that needs to be protected like social security numbers.

If an owner obtains an EIN but later determines it is no longer needed (e.g. the business never materialized or the business is inactive or defunct); a request can be made to the IRS to close the account. Closing an account requires the complete legal name of the entity, the EIN, the business address and the reason for divestiture. Many businesses fail to contact the IRS that their business is no longer active and IRS personnel indicated that this is a significant area of concern.

The IRS has found that identity thieves apply for and/or obtain an EIN using the name and social security number of another individual as the responsible party. In many cases identity thieves use the EIN of an inactive business without the permission or knowledge of the EIN's owner. The IRS maintains a cumulative list of suspicious EINs and as of December 2017, the list contained over 6000 suspicious EINs. IRS indicates that the reuse of inactive or defunct EINs is a significant issue that needs addressing, and in the Treasury Inspector General Report of 2015[xxi], one of the key recommendations was to implement procedures that a taxpayer must surrender an EIN no longer in use because the business is closed or no longer in service.

2 NASS reports nearly 30% of state business registry offices restrict access to business records via username and password.

STATE BUSINESS REGISTRATIONS

In 2014 alone, the IRS identified over 225 returns that had used suspicious EINs to file fraudulent returns and of these 97 claimed refunds totaling over $2.5 million[xxii].

Since many other organizations use EINs for registration and identity purposes, it is unclear if there is a central reporting mechanism for individuals, businesses, states, banks, and/or credit reporting agencies to report suspicious EINs to the IRS.

Typically, the state business services division, under the Secretary of State office, manages the registration, licensing and filings of businesses as well as the paper and online processes of business registration.

Many state offices operate under the Model Business Corporation Act (MBCA), a law used as a basis for their statutes. This law defines the business filing and company formation process as well as the duties of the Secretaries of State. The duties under the MBCA limit the responsibilities of these offices to "ministerial," meaning the function is administrative with little to no ability for the office to challenge the validity of the filing. Moreover, these offices have no authority to control who can view or gain access to the state filings, as they are a public record[xxiii].

State statutes differ in terms of registration processes and Florida is the only state that uses EINs for registration. Most states have a method to check name availability[3]. However, there is a no validation in the registration process to determine if a similar named entity exists in another state. Additionally there is no interstate process for sharing registration information across state lines. An IACA official reported that in some cases criminals obtain the approved entity certificate from one state; cross state lines and open new accounts and lines of credit in another state; as well as sell these new fraudulent business identities on the dark web. Without the use of a unique identifier, and a method to cross reference business identity across state lines, it appears it would be nearly impossible to track fraudulent business identity in the U.S.

In 2012, the National Association of Secretaries of State reported that criminals look to exploit the state filing systems and business registration websites for financial gain[xxiv]. NASS found that criminals file bogus reports with the Secretary of State offices or manipulate online business records – such as change the business address; list new officers; or change the registered agent; income levels and number of employees. Using these altered records, the hackers apply for credit. When the retailers check with the credit reporting agencies to verify the information, the check involves verifying the data that resides at the state. State officials who oversee business filings indicate business identity theft is of great concern.

Based upon these inconsistencies in registration, name change and identity management, it appears that thieves could easily create a new business without an EIN or steal the identity of a business they find through online research. It appears protecting business identity in the near term will be a challenge without significant commitment and sustained improvements.

3 http://www.sos.ca.gov/business-programs/business-entities/name-availability/

BUSINESS CREDIT FILE

All businesses rely on a business credit file to sustain their ability to conduct day-to-day operations. The business credit file or report is used to apply for a loan, credit card, process a merchant account, set insurance rates, lease office space and/or provide credit to other business partners in the supply chain.

Good credit is probably one of the most coveted assets a business has, especially a small business. The business credit or FICO score is a numeric representation of a company's creditworthiness. While consumer credit reporting agencies (CRAs) use a standard algorithm to calculate a score for an individual, business scoring doesn't follow an industry standard and varies among the agencies. The algorithm calculates a company's creditworthiness based on information supplied by the business owner and gathered from the business's vendors, suppliers, trade associations, data mining research entities and financial institutions. While consumer credit uses an individual's social security number to verify identity; CRAs used different methods to verify identity. All business credit information in the file is public, and anyone can obtain the file as long as they are willing to pay for it.

In the U.S., the three commercial credit reporting agencies for businesses are:

1. Experian
2. Equifax and
3. Dun & Bradstreet

CRAs collect information from a variety of sources and use a number of methods to verify the data is current and accurate, but admittedly the information may contain a degree of error. On the consumer side, the FTC found 25% of consumer credit reports contain errors[xxv], and mainly because of the degree of inaccuracy in consumer credit reports, the Fair Credit Trade Act, provides consumers the ability to get free copies of personal credit reports. Unfortunately, the same consideration is not afforded businesses.

Commercial CRAs work in a different framework than consumer CRAs. Dun & Bradstreet, Experian and Equifax are motivated to keep the data as accurate as possible or suffer the risk of losing business from their customers. Yet the ability for customers to verify and correct the data held on their behalf varies dramatically among the entities. Each has varying degrees of approaches for businesses to correct or update their data. All three CRAs use different methods and data sources to score creditworthiness.

The table below provides an overview of the data collected and the approaches used to calculate the score.

CRA	Product	Cost	Data Sources/Elements[4]
Dun & Bradstreet	Credit Decision - based on payment data, a "commercial credit score" & financial stress score	$61.70	Company profile: Tax ID/SSN, business type, date established, ownership, location, number of employees, annual sales, SIC/NAICS, address, parent organization Inquiry Information: number and type of inquiries made on the credit file. Credit Report Summary: number of accounts, total past due, most severe status, single highest credit extended, total current credit exposure, average open balance, number of accounts delinquent Paydex Score: includes commercial credit score and financial stress score
Equifax	Equifax Risk Rating	$99.95	Payment Index: on-time payment history from vendors/creditors Business Credit Risk Score: evaluates the likelihood of payment delinquency. Includes company size, available credit limit on revolving credit card; length of time oldest financial account opened; evidence of nonfinancial transactions such as invoices from vendors Business Failure Score: age of oldest financial account, amount of credit limits used; number of delinquent accounts; evidence of nonfinancial transactions
Experian	CreditScore	Free	Completely different approach from Equifax and Dun & Bradstreet. Business Credit Score: Credit information from suppliers & lenders; legal filings from local county and state courts, company background information from independent sources such as public records from collection agencies; balances from outstanding loans, payment habits, size of business and age of business.

BUSINESS CREDIT FILE CONTINUED

Identity theft resources recommend data breach victims (consumers) monitor their credit reports to determine whether their identity has been stolen and used to obtain new lines of credit or use existing lines of credit to purchase goods and services. Given that all three consumer credit bureaus use the same data and scoring methodology, correcting data on one file is automatically shared with the other remaining agencies and is a fairly easy task to accomplish. Unfortunately for business owners, monitoring their identity via the three CRAs who use different data to assess creditworthiness, and business solvency, makes this a difficult task.

For a fee, Dun & Bradstreet, Experian, as well as several other commercial vendors provide business credit monitoring services. These entities provide several types of monitoring – of the business itself, and for the business to monitor the credit activity of their business partners, customers, and suppliers. It is unclear whether the business credit file monitoring is worth the cost (upwards to $150/month), however does provide the business the opportunity to track data on the business and to correct erroneous data quickly that may affect their credit profile, as well as alert the business of potential business identity theft.

BUSINESS CREDIT REPORTING AGENCIES

A. Identity Verification and Authentication

Dun & Bradstreet. Dun and Bradstreet issues a unique nine-digit number identifying number called a D-U-N-S (Data Universal Numbering System) number to establish a business credit file. A DUNS number is required to bid on government contracts or receive a grant or loan and requires an address. To initiate a DUNS application online, an applicant is required to provide their name and other details associated with the business to establish a login and password. The application is submitted to Dun & Bradstreet who uses the self-reported information to check for consistency and curates this information with other data including but not limited to, government and other private institution data, and to ensure accuracy of the business information. The applicant is then notified when the application is approved. The data elements required on the application include legal name (DBA) of the business, headquarters physical address, mailing address if different, type of business operations, telephone number, CEO/principal contact name and title, number of employees and whether the entity is a home-based business. Dun & Bradstreet also provides free support for businesses who suspect or have had their identity stolen. To report a business identity theft to Dun & Bradstreet businesses can call: 800.895.7262.

Equifax. Equifax's identity verification approach uses EFX ID®, by securely linking all data using randomly issued "keys". EFX ID® is used in place of SSN or EINs, and is a nine digit number. Equifax's EFX ID® is a registered trademark for a service Equifax designed in 2009 which provides business information based on a tracking system that allows users to identify and track businesses as they are bought and sold, change names or locations. Equifax provides information regarding the inter-related and inter-dependent nature of businesses, a feature not found elsewhere in the review – which could facilitate safety, security and efficiency.

4 Selected sample of data presented in report. See endnotes for urls of sample reports.

BUSINESS CREDIT REPORTING AGENCIES CONTINUED

Experian. Experian issues an Experian Business Identification Number (BIN), also a nine-digit number. To ensure data accuracy, Experian uses industry technologies to format, cleanse and load data that is acquired directly from government sources and industry vendors. Experian collects legal filings from various local, county and state courts across the United States. Company background information is collected from a variety of independent firms. Experian does not display information directly from a company about its business, unless that information has been verified.

In researching sample business credit file processes, use of EINs or SSNs were not utilized as identifiers, for the three CRAs. It did not appear that there is an industry norm or standardized process used by the CRAs to verify or authenticate business identity, however elements of each process could provide promise for improvement. Dun & Bradstreet's application process appears to provide a method to verify authenticity of the application through hands on review, all provide a unique identifier to the business's identity, yet all rely on "other data" as undefined to verify.

B. Access and Changes to the Business Credit File

Dun & Bradstreet. Companies can request to see a self-report credit and payment history via a secure online portal, called iUpdate, and can recommend changes or updates to information in the D&B database for free.

Additionally, Dun & Bradstreet offers monitoring services which allow a business to stay informed about any and all changes made in the D&B database. These services can be found online or by calling 877.763.3044. D&B encourages businesses to be proactive in monitoring and updating their business credit file and to notify D&B about any potential errors. D&B notes they will promptly investigate the issue, confirm the information in question, and correct verified inaccuracies. In many cases, D&B will research and make appropriate changes and in some cases may apply for a "stop distribution" order regarding the business credit file until the matter is resolved. When resolved, D&B will send a correction notice to businesses or others who they know have received the inaccurate data.

Equifax. Requesting a copy of a business credit file can be done by locating the entity in question, paying the fee of ($99.95). A free report can be obtained if the company has been denied credit by calling their toll-free number at 1.800.797.8495. As in the case of Experian, the business credit file cannot be frozen but a dispute can be made through their toll-free number.

Experian. Companies can initiate an update to their Experian business credit file by completing a submission to Experian's website at www.BusinessCreditFacts.com, or by calling their toll free number at 1.800.727.8495; if information about the company is inaccurate or outdated.

Companies can easily access their D&B file to verify information and make changes. This flexibility comes with a cost – thieves can use the DUNs search function to find and locate businesses with good credit rating; manipulate the data to impersonate; or defraud the business. As previously noted, Dun & Bradstreet reported business identity theft to NASS, in 26 states.

STATUTES – VICTIM'S RIGHTS

In order to appreciate the ecosystem of resources for victims a review of the legal framework was conducted. The statutes presented below cover the statutory framework of identity theft and describes the resources available for victims. The legal framework presented below is from the Office for Victims of Crime, Department of Justice, and "Identity Theft Supporting Victims' Financial & Emotional Recovery" online resource guide.

A. Identity Theft and Assumption Deterrence Act (1998)

- Makes identity theft a federal crime
- Defines identity theft
- Defines the means of identification

Identity theft occurs when a person…."knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law…"

B. Identity Theft Enforcement and Restitution Act

- Allow victims of identity theft to recover restitution for time spent repairing their credit.

C. Identity Theft Penalty Enhancement Act (2004)

- Imposes tougher penalties for identity thieves that commit terrorism
- Defines a new crime – aggravated identity theft
- Addresses sentencing issues for underlying crimes
- Allows for consecutive sentences for identity theft

D. Internet False Identification Act (2000)

- Prohibits the possession, production or transfer of identification documents (false or real) that were not legally issued to the possessor.

E. Justice for All Act (2004)

- Affords victims of federal crimes certain rights
- Provides federal victim services and mandates notification to federal victims to include status of investigation, resource information, and right to an attorney
- In case of indictment, provides information to the victim about the court process, victim impact, right to restitution, attendance at proceedings, sentence notice, and prison release information.
- Also provides victim assistance for cases under investigation

F. The Fair Credit Reporting Act (FCRA)

- Comprehensive Statute that governs Consumer Credit Reporting Agencies (CRAs)
- Contains many protections for identity theft victims – to include steps a victim should take in order to clear his or her credit report.
- Mandates consumer CRAs block the first five digits of a consumer's SSN from credit reports at the consumer's request; block items on credit report that are disputed due to identity theft within 4 days of receipt of written notice.
- Requires consumer CRAs to notify information furnishers that items are disputed due to identity theft
- Allows a consumer to request copies of documents related to fraudulent accounts

G. Fair and Accurate Credit Transactions Act (FACTA)

Amended the FACA to add important consumer rights to victims of identity theft and to outline a procedure for victims, consumer CRAs and businesses to follow when disputing fraudulent accounts.

- Requires consumer CRAs to provide consumers one free credit report per year
- Allows consumers to request that the first five digits of their SSN be blocked from their credit reports;
- Requires creditors and other businesses to take reasonable steps to protect consumer information from unauthorized access
- Allows identity theft victims to place a fraud alert on their credit reports for 90 days extendable to 7 years
- Allows personal identity theft victims to block any portion of their credit report attributable to identity theft
- Allows active duty military to place an alert on their accounts and credit reports renewable yearly while serving outside the U.S.
- Requires consumer CRAs to give identity theft victims a written summary of their rights upon request

STATUTES – VICTIM'S RIGHTS CONTINUED

- Requires businesses that issued accounts or credit to an imposter to provide account documentation to the identity theft victim if requested in writing
- Requires collection agencies to report identity theft to creditors and provide information about the alleged debt to the identity theft victim
- Prevents a creditor from placing a debt for collection after being notified that the debt was incurred through identity theft.

To dispute a fraudulent credit report entry under FACTA, a victim must contact the consumer CRA in writing and provide a copy of the victim's police report, identity affidavit[5] (if not included in the police report), government issued identification card (driver's license), complete description of the items that the victim is disputing and a statement that the information does not relate to any transaction initiated by the victim.

To dispute a fraudulent account under FACTA, a victim must contact the creditor in writing and provide a copy of the victim's police report, identity theft affidavit, government issued identification card, and relevant information about the transaction being disputed.

H. The Fair Credit Billing Act

Provides a procedure for consumers and businesses to follow in order to dispute billing errors in credit cards and revolving charge accounts.

- Allows a consumer to dispute billing errors such as wrong dates, wrong amounts billed, or unauthorized charges
- Specifies a procedure for financial institutions to follow to investigate and respond to billing errors identified by consumers;
- Limits a consumer's responsibility to pay unauthorized charges if the consumer notifies the financial institution of the unauthorized charges within 60 days of the consumer's receipt of the statement containing the unauthorized charges.

I. The Fair Debt Collection Practices Act

Prohibits unfair, abusive, or deceptive debt collection practices. The law prohibits debt collectors from:

- Contacting the debtor before 8 a.m. or after 9 p.m. unless the consumer consents;
- Contacting the debtor at work after receiving notice that the debtor cannot receive such calls at work
- Contacting a debtor except to inform that the debtor of an action being taken such as the filing a lawsuit, after the debt collector has received written notice from the debtor requesting that the collector cease contact;
- Harassing, threatening or lying to a debtor in order to collect a debt
- Giving false information about a debtor to third parties.

J. Electronic Funds Transfer Act

Governs how electronic transfers are made.

- Governs use of ATM, debit cards, telephone transfers, pre-authorized account deposits and debits and wire transfers;
- Gives consumers the right to dispute errors or unauthorized transfers within 60 days of the date that the unauthorized transfer or error appears on the consumer's account statement;
- Limits a consumer's loss due to unauthorized activity to $50 if reported within 2 days of the loss or to $500 if reported more than 2 days after the loss but less than 60 days after the account statement shows the loss.

K. State Identity Theft Laws

Identity theft may be a misdemeanor or a felony. Prosecution is conducted by the local District Attorney Offices and investigations are done by the local police or sheriff offices. Laws vary by state.

L. Regulatory Agencies

Regulatory agencies play a role in investigations such as:

- Social Security Administration investigates identity theft crimes involving the buying and selling of Social Security cards.
- Internal Revenue Service handles identity cases involving a victim's tax records or business identity theft of business returns.
- Federal Trade Commission collects information on consumer identity theft and conducts investigations on unfair business practices affecting consumers.
- These laws were established to protect the consumer and unfortunately the provisions afforded victims do not include protections for business.

5 No identity theft affidavit exists for business identity theft

VICTIM RESOURCES

Through the review, there are limited resources for victims. The majority of the laws as currently written protect consumers, however an argument can be made that business identity theft is still identity theft. By law, identity theft is a federal crime and it appears many of the provisions under the federal statute - Justice for All - would apply to victims of business identity theft. Limits on loss under the Electronic Funds Transfer Act apply to consumers, not businesses. FACA and FACTA apply to consumers, not businesses, however CRAs will provide a free report if the business has been the victim of identity theft.

The IRS provides several resources for business identity theft victims. The IRS has developed Form 14039-B, Business Identity Theft Affidavit, which victims can use to notify the IRS of suspected identity theft. In addition, the IRS has prepared the "Tax Preparer Guide to Identity Theft" for tax practitioners that lists warning signs for business clients and "Tax Practitioner Guide to Business Identity Theft", however some of the information provided is not consistent with our research[6]. In the beginning of each tax year, the IRS disseminates information through its month-long program -- National Tax Security Awareness. A helpful article was published in 2017, titled "Small Businesses: Be Alert to Identity Theft."

To crack down on fraudulent returns for 2018, the IRS has instituted the following measures to make it harder for identity thieves to impersonate the business.

These new requirements include:

- Requiring the company executive that signs the return to provide their full name and SSN;
- Requiring the preparer to provide payment history of estimated payments made during the year;
- Requiring the entity to provide the parent company information if applicable;
- Requiring additional information concerning deductions;
- Requesting information on whether the business has filed other forms, such as 940, or 941;
- And in some cases, requiring the sole proprietor to provide additional identifying information, such as driver's license.

Many states have provided resources via their websites for business identity theft victims. Colorado has a subpage on its website devoted to business identity theft and has produced a guide: "Business Identity Theft Resource Guide".

The National Association of Secretaries of State has been a leader in the area of business identity theft. Recognizing the problem, they formed a Business Identity Theft Task Force that developed proactive strategies for combating this new type of crime. The first report, "NASS White Paper on Business Identity Theft, Prevention and Protection in State Policy Making Efforts" published in 2012, established steps for victim assistance and education. This organization continues to champion improvements in the state business filing systems to prevent and thwart this type of crime.

As part of the research, the NCSS identified two resources – Business Identity Theft.org and Identity Theft Protection Association, 2012. Neither organization would respond to our requests for validation of their organizational status and whether they currently support victims.

Additionally, contact with law enforcement (FBI, USSS) did not identify any resources for victims of business identity theft.

Contact with the FTC revealed that while consumers can report identity theft to the FTC and the organization has many helpful resources for consumers, the agency does not provide victim resources for business identity theft.

6 Inconsistencies include: placing a fraud alert on CRA accounts (applies only to Experian) and TransUnion does not maintain business credit files.

VULNERABILITIES AND GAPS

Several vulnerabilities were identified that if corrected could strengthen the system and make it harder for thieves to exploit. Criminals look to capitalize on these vulnerabilities to gain access to systems and processes. The IRS has been proactive in that they have investigated business identity theft through yearly audits, and identified measures to make it harder to impersonate the business and file fraudulent returns.

Gaps were identified in victim resources, reporting mechanisms and understanding of the crime. No federal agency is actively evaluating or reporting statistics on this type of crime.

The goal for this work effort is to increase awareness, identity system improvements and work with coalition partners to increase the current level of victim services.

VULNERABILITIES/GAPS/ AREAS FOR IMPROVEMENT

EINs and SSNs. EINs and business owner SSNs aren't used consistently as a means to verify identity. Inactive or stolen EINs are used to register fraudulent businesses. EINs are not protected data like SSNs. Identity theft of an individual, using their SSN can result in business identity theft. EINs are widely available on the Internet for lookup. No visible process was found to report defunct or inactive EINs to IRS and it appears that many businesses fail to contact the IRS that the business is no longer viable. There is no visible or well-known process to report suspicious EINs to the IRS.

Compromised Websites. Compromised websites go undetected for months. Unpatched vulnerabilities in websites and limited web application firewall protections make websites vulnerable. Businesses don't monitor the status of their websites to determine if they are still safe for users. No federal agency lists website defacement as a crime – even though hijacked websites can be held for ransom. IC3 does not list website defacement as a separate crime from ransomware or misrepresentation.

Federal Resources. No federal agency is collecting statistics on business identity theft. There is no central federal agency for businesses to report business identity theft. Federal victim resources are limited. No identified business identity affidavit form is available as there is for consumers; however, IRS has provided one for tax fraud. No defined process on documenting and reporting the crime or means to recover. It appears the current laws do not provide the same protections for businesses as consumers – FACA, FACTA and Fair Credit Billing Act, Fair Debt Collection Practices Act or the Electronic Transfers Act.

State Resources. It is unclear if state identity laws cover business identity theft. Unclear if state offices coordinate with each other – Tax, Attorney General, Business Services Division and what coordination occurs with the federal government.

Awareness. There is a lack of public awareness; lack of resources for victims; lack of defined processes for victims to use to repair their business identity. Unclear if businesses realize that their credit profile is a critical asset that needs to be protected.

State Registration Systems. There is an easy ability to change state business records, without challenge. States don't restrict access to business filings, or challenge the change. Not all states have implemented a change notification email to the business owner of record. No authentication method used to validate the user is legitimately the appropriate user to change the record. No validation in the registration process to determine if a similar named entity exists in another state. There is no verification method to verify registrations -- EINs aren't used for state registrations. There are inconsistencies in state registration processes. There appears to be limited coordination between state offices; limited coordination between state and federal.

Identity Verification. Commercial CRAs use multiple publicly available sources, curated with private sources, to verify a business's identity. Unclear what that process is. Use of EINs or SSNs are not consistently used in the business credit file report process. There appears to be a lack of cross-reference to standard identification methods used by other agencies as well as coordinated with the other CRAs. All three CRAs use different identification verification and authentication processes.

VULNERABILITIES AND GAPS CONTINUED

Business Credit Scoring Methodology. Business credit scoring is inconsistent between commercial CRAs, nor is there any visibility in the process. It is unclear how the business owner can challenge the validity of the data that is being used to assess credit worthiness and solvency, if the process is not transparent to the users.

Data Validity/Accuracy. Commercial CRAs collect information from a wide variety of sources and use a number of methods to verify if the data is current and accurate. It is unclear the accuracy of the business credit file.

Business Credit File. No standard process to challenge data on the business credit file. There is an inability for businesses to monitor their credit without signing up for an expensive monitoring service. CRAs reference that "other data and other sources" are used to determine business credit score. Lack of visibility into the data and sources makes it difficult for a business owner to challenge or correct bad information if these sources aren't shared.

Data Availability/Data Access. DUNs search function can be used to find businesses with good credit standing. This free search can be exploited. Dun & Bradstreet allows direct access to the business credit file, if the user has the login credentials. Criminals can gain access through compromised credentials and easily change the records.

Fraud Alerts/Freeze Files. Businesses can't freeze a business credit file after a business identity theft. Not all commercial CRAs provide an ability to place a fraud alert in the file.

Business Credit File Restitution. Dun & Bradstreet provides a detailed accounting of the process used to restore the business credit file after being notified by the business of erroneous errors. The other CRAs provide no visibility into the process used to correct errors, nor indicate what data/documents are required to be provided by the business entity. It is unclear if D&B restitution outcomes (corrected business files) are shared with the other CRAs.

RECOMMENDATIONS/NEXT STEPS

The NCSS team used interviews, past reports, audits and online research to analyze business identity theft in the U.S. and prepare this report. Many players in the ecosystem were given the draft report and asked to comment.

Through this process, the NCSS has developed the following set of recommendations:

1. **National Business Identity Task Force** – establish a working group/task force aligned with other private sector communities to discuss the study findings and identity opportunities for improvement. Suggested representatives for this group include: federal and state law enforcement; federal and state governments; all three commercial credit reporting agencies; large national banks or financial institutions; Better Business Bureau and leaders in identity theft. The task force can be used to create communication tools/strategies and assist in disseminating the information to the business community. Additionally, identify a sponsor for the task force who has the resources and commitment to lead the work effort.

Several contributors to this study recommended a task force – similar to the one established by the IRS Security Summit -- which was created to address tax fraud. The model brought key industry players together to identify data elements, coordination methods and criminal tactics in order to develop ways to prevent and thwart tax fraud. The National Business Identity Task Force could be a working group appended to the Tax Security Summit.

2. **Guidebook to Protecting Business Identity** – Leveraging the Task Force, develop a guide that can be shared nationwide about techniques to protect, prevent and respond to business identity theft. It is envisioned the guide would establish the steps businesses should use on a quarterly/annual basis to protect critical business identity data.

RECOMMENDATIONS/NEXT STEPS
CONTINUED

3. **Awareness** – Build an awareness program to reach businesses across the U.S. to communicate prevention methods that can be implemented to protect their identity. Leverage partners to identity opportunities to present study findings and recommendations developed through the Task Force.
4. **State Registration Systems** – Coordinate with NASS, IACA and state officials about the need to restrict the ability to change business records and to verify the user before the record is changed. Additionally, recommend the owner be notified when the record has been changed. The goal would be to achieve 100% online identity verification and authentication before a record can be changed.
5. **Credit Reporting Agencies** – Coordinate with CRAs to determine the data sources used for identity verification and whether adding fields could improve identity management. Coordinate with CRAs to determine methods used to verify data accuracy and identify means for the business owner to have more visibility into the process as well as have the ability to provide updates. Coordinate with the CRAs to address fraud alert mechanisms. Determine whether correction-notice processes can be disseminated industry wide to ensure inotices are provided to the other CRAs.
6. **Statutes** – The Fair Credit Reporting Act, as well as many other statutes concerning identity theft provide protections for consumers. Leveraging the task force, advocate that similar provisions be afforded businesses.

In closing, there needs to be a better understanding of the scope and depth of the crime. Without a single federal agency tracking statistics on this type of crime, it is still unclear "how bad it is". As identity theft affects 7% of the U.S. population, an argument could be made that we could see a similar impact to the small business community. With 28 million small businesses in the U.S., could there be 2 million small businesses affected? How would we know? With the increase in data breaches targeting financial data, it is safe to assume that the breach involves some level of data on the business owner, and as IRS reports – identity thieves are displaying a sophisticated knowledge of the tax code and industry practices to obtain valuable data to impersonate the business. Crime data is useful for operational and resource allocation decisions by law enforcement, government agencies and businesses. Without this data, victim advocates have a difficult time lobbing for attention from policy and lawmakers in order to provide needed reforms to support businesses and thwart this type of crime.

Law enforcement needs to start collecting data on business identity theft and assisting in defining the data required to conduct the investigation. While the instructional aids developed for this effort will include "notify local law enforcement", what data should be provided to law enforcement? When should the business report the theft? How will the commercial CRAs be involved in the investigation? What tactics do criminals use? Is the average financial loss $100K, therefore an insurance policy can be priced accordingly? What credit monitoring measures should be instituted to provide an early warning signal and used to inform the investigation?

Since this is a crime that isn't tracked; there isn't the requisite victim services available. The IRS has done a commendable job producing a number of resources about tax fraud to include dedicating an entire month to improving tax security awareness. The Office for Victims of Crime, DOJ, and the Identity Theft Resource Center have taken the first steps to recognizing the need for improving victim resources by funding this grant – but more work needs to be done – to better inform policy makers, influence federal and state leaders and educate the business community.

Lastly, improving outreach to the business community is desperately needed so owners can be informed of preventive measures to protect their identity. Updating and validating business information with the states where they are registered is an important once a year task -- as well as checking their line of credit. Obtaining credit monitoring and/or identity monitoring services are also important if available and cost effective. Insurance coverage is another prudent measure the business can take to protect against loss. These steps coupled with good cybersecurity practices (protecting access to critical files, keeping software up to date and changing login and passwords) are effective tools for business identity theft.

The NCSS would like to acknowledge the support received from the following organizations that contributed material for this study:

National Association of Secretaries of State (NASS)

Treasury Inspector General for Tax Administration

Identity Theft Resource Center

Office of the Victims of Crime, Department of Justice

Dun & Bradstreet

State of Ohio Business Services

State of Colorado Business Services

International Association of Commercial Administrators (IACA)

ENDNOTES

i Internet Crime Complaint Center, 2016 Internet Crime Report, 2016.

ii Federal Trade Commission, FTC Issues Final Rules on FACTA Identity Theft Definitions, Active Duty Alert Duration, and Appropriate Proof of Identity, https://www.ftc.gov/news-events/press-releases/2004/10/ftc-issues-final-rules-facta-identity-theft-definitions-active

iii Department of Justice, Office for Victims of Crime, Training and Technical Assistance Center, "Identity Theft Supporting Victims' Financial and Emotional Recovery.

iv Treasury Inspector General for Tax Administration, "Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection", September 2015.

v Vijayan Jaikumar, "Corporate ID theft hits Georgia businesses," Computerworld, July 16, 2010.

vi NASS, State Strategies to Subert Fraudulent Uniform Commercial Code (UCC) Filings, A Report for State Business Filing Agencies, 2014.

vii Treasury Inspector General for Tax Administration, "Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection", September 2015.

viii Treasury Inspector General for Tax Administration, "Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection", September 2015

viv Internal Revenue Service, "National Tax Security Week No. 5 – Small Businesses: Be Alert to Identity Theft", December 1, 2017

x Dornbrook, James, IRS: Business Identity Theft Cases Jump 250% so far in 2017, 2017.

xi Alley, Mike, Indiana Department of Revenue's Testimony presented U.S. Senate Committee on Finance, 2015.

xii Commtouch, "Compromised Websites – An Owner's Perspective – Stop Badware", February 2012.

xiii Internet Crime Complaint Center, 2016 Internet Crime Report, 2016.

xiv Krebs, Brian, FBI, $1.2 billion lost to Business Email Compromise, August, 2015.

xv Department of Justice, Office for Victims of Crime, Training and Technical Assistance Center, "Identity Theft Supporting Victims' Financial and Emotional Recovery.

xvi NASS White page on Developing State Solutions to Business Identity Theft, January 2012.

xvii NASS White Paper on Developing State Solutions to Business Identity Theft, January 2012

xviii Internet Crime Complaint Center, 2016 Internet Crime Report, 2016.

xix Internet Crime Complaint Center, 2016 Internet Crime Report, 2016.

xx NASS White page on Developing State Solutions to Business Identity Theft, January 2012.

xxi Treasury Inspector General for Tax Administration, September 9, 2015, "Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection."

xxii Treasury Inspector General for Tax Administration, September 9, 2015, "Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection."

xxiii NASS White Paper on Developing State Solutions to Business Identity Theft, January 2012

xxiv NASS White Paper on Developing State Solutions to Business Identity Theft, January 2012.

xxv Hephner, Lisa, "How to Review Your Small Business Credit Scores"

xxvi Tsosie, Claire and Nicastro Steve, "Business Credit Score 101", October 6, 2017.

xxvii Internal Revenue Service, "Key IRS Identity Theft Indicators Continue Dramatic Decline in 2017, Security Summit Marks 2017 Progress Against Identity Theft," February 8, 2018.