



Business Identity Theft Protection

Lurking in the Shadows:

How major American institutions are failing to publicize the threat of business identity theft

Executive Summary

Business identity theft is woefully under publicized in America today – even by major civic and private-sector institutions that are intimately aware of its seriousness.

This study by Company Alarm, the nationwide leader in business identity theft protection, sought to document both how much government agencies and private business and organizations know about business identity theft and how much they're educating the public about it. Our findings show what Company Alarm has long suspected: that business identity theft is simply not a priority for leaders in government and business.

Yes, there are some state and federal government agencies, like the Internal Revenue Service and the Colorado Bureau of Investigation, that have been sounding the alarm about business identity theft for years and have produced a steady stream of resources for businesses and potential victims. And yes, business identity theft is a frequently discussed topic among insiders, particularly members of the National Association of Secretaries of State, which published one of the nation's first white papers on the topic in 2012.

But despite this attention, few people inside or outside of government are focusing on this issue or warning the public about it. Our research finds that nearly half of nation's secretaries of state fail to publish anything about business identity theft on their websites – even though their professional organization and the association for government administrators overseeing businesses regularly discuss the topic at their conventions.

Beyond that, only a small handful of other state-level agencies seem to even be aware of business identity theft, and a large portion of them are based in Colorado, the one state that has made fighting this crime a priority.

At the federal level, the IRS and the IRS' independent watchdog, the Treasury Inspector General for Tax Administration, stand alone in the attention they've lavished upon business identity theft. However, victims of business identity theft are not likely to encounter either of those federal organizations, especially when looking for help. Rather, the nation's few experts on business identity theft recommend that victims contact the Federal Bureau of Investigation and the Federal Trade Commission for help – and neither of those organizations publish much in the way of educational information about the crime.

In the private sector, associations of government employees and the nation's three credit rating agencies (Dun & Bradstreet, Experian, and Equifax) all have tried to spread the word about business identity theft. The associations' attempts at communication, however, are limited to government officials while one of the credit rating agencies has published only a single article on the topic.

The institutions that could do the most for publicizing the problems of business identity theft – big, private businesses that handle a lot of financial transactions – are doing the least. Less than 20 percent of the 101 institutions surveyed in this report seem to have any knowledge of the problem. Yet, many of those organizations have special pages on their websites devoted to educating consumers about personal identity theft.

To rectify this situation and help educate business owner about the dangers of business identity theft, Company Alarm has several recommendations:

Recommendation 1: Every secretary of state or state-level business registration office collect annual statistics on the number of business identity theft incidents in their jurisdiction and forward that data to the Federal Trade Commission for an aggregated, nationwide report.

Recommendation 2: Every secretary of state or state-level business registration office, state tax agency and state law enforcement agency include information on their websites about business identity theft, including guidance for victims.

Recommendation 3: Private business concerns that handle more than \$10 million worth of financial transactions each year develop a plan for protecting businesses from identity theft and publish information about these programs in a prominent place on their websites.

Recommendation 4: Business organizations of all sizes and locales demand that their government representatives make business identity theft a top policy priority and develop guidance and resources for victims.

Recommendation 5: Government agencies at both the state and federal level work cooperatively to share information about business identity theft and develop policies and procedures for effectively and efficiently investigating and prosecuting criminal cases. In particular, state attorneys general and secretaries of state should be working closely together to search out and prosecute these crimes.

Recommendation 6: Laws at the local, state, and federal level be reformatted or, if needed, rewritten, to make it clear that stealing the identity of a business is as much a crime as impersonating an individual. These statutes should be clearly labelled and worded to communicate this important nuance.

Recommendation 7: State attorneys generals and/or secretaries of state track on an annual basis all pieces of state legislation pertaining to business identity theft and make that information available to business organizations in their jurisdiction. The U.S. Department of Justice should also track such proposals at the Congressional level and report it annually to national business organizations, like the U.S. Chamber of Commerce.

Business identity theft is a serious crime that can bankrupt businesses and ruin lives. But businesspeople will remain at risk until America's institutions take this threat seriously and begin educating the public about it.

Table of Contents

Introduction	5
Methodology	6
Findings	8
Discussion & Recommendations	12
Appendix 1, List of institutions reviewed	16
Appendix 2, Survey questions posed	30
Appendix 3, Survey results received	36
Appendix 4, Institutions featured on other websites	38
About Company AI	40
Endnotes	41

Introduction

Company Alarm is dedicated to combatting business identity theft, a form of identity theft in which criminals impersonate a business, rather than an individual, in order to secure illicit loans, plunder the business's assets, file fake tax returns or scam unsuspecting consumers.

By several measures, business identity theft is on the rise in the United States:

- From 2015 to 2017, the Internal Revenue Service reported a 2,757 percent increase in fraudulent tax returns filed for businesses.
- Dun & Bradstreet, the commercial reporting agency based in New Jersey, found an increase of 46 percent of business identity theft incidents from 2016 to 2017.
- The Colorado Bureau of Investigation, arguably the leading law enforcement agency fighting business identity theft in the nation, investigated more than 3,900 incidents of the crime from 2010 through 2019.

Serial entrepreneur Andy Pham founded Company Alarm after he became a victim of business identity theft. In 2015, cybercriminals logged onto the Nevada Secretary of State's website and removed Pham as the managing member of a company he was using to stash a \$5 million piece of land. With Pham out of the way, the criminals then took out more than \$2 million in unauthorized loans on the land, transferred it into another holding company and tried to sell it. Months later, when Pham discovered what had happened, he filed a lawsuit. He's been stuck in court ever since, racking up more than \$500,000 in legal fees as he has fought to regain control of the holding company and his land.

Pham's story was the focus of a 2018 front-page investigative report in the *Las Vegas Review-Journal* newspaper. The following year, that article won the top prize in business reporting in the regional Best of the West journalism competition.

Nonetheless, business identity theft is not well known in the United States, nor is it a priority for the vast majority of our nation's policymakers and law enforcement officials. As Ralph Gagliardi, the leader of the Colorado law enforcement unit focused on this crime, has said, "Business identity theft is one of the biggest problems facing American businesses today, but virtually no one knows about it."

Over the last year, Company Alarm has sought to understand just how much major American institutions know about business identity theft and are communicating to the public.

The result of that inquiry is this report.

Methodology

Over the past few years, a handful of organizations have attempted to understand the scope of business identity theft in the United States, most notably the Cybersecurity Society in its seminal 2018 report, “Business Identity Theft in the U.S.”

Our goal with this report, rather than to revisit similar themes, was simply to document how much trusted American institutions are talking about and monitoring business identity theft. To that end, we started by identifying 287 American institutions that we thought would be well positioned to know about business identity theft and spread the word about it to the public. Those institutions broke down as follows. For the full list of institutions, please see Appendix 1.

- 51 secretary of state offices or other state-level offices responsible for registering businesses. These 51 offices covered all 50 states plus the District of Columbia.
- 74 state law enforcement agencies, including state-level attorney general offices, plus, where applicable, statewide police forces. Once again, these agencies covered all 50 states plus D.C.
- 51 local tax enforcement agencies, covering all 50 states as well as D.C.
- Five federal agencies:
 - The Federal Bureau of Investigation (FBI);
 - The U.S. Secret Services;
 - The Federal Trade Commission (FTC);
 - The Internal Revenue Service (IRS); and
 - The Treasury Inspector General for Tax Administration.
- Two nationwide, private associations representing government employees responsible for business registration and organization.
- Three nationwide commercial credit rating agencies.
- 101 large, private business concerns that process a lot of financial transactions.

Using this list of institutions, Company Alarm then set out to do two things:

1. Survey each, asking them what they know about business identity theft and what, if anything, they're doing about it; and
2. Carefully reviewing the public websites for each entity to see what, if anything, they are writing about business identity theft.

For a list of the survey questions posed to the institutions, please see Appendix 2.

The surveys were e-mailed to the institutions beginning on March 4, 2020. The review of their websites began shortly thereafter.

Findings

The institutions received our survey just as the COVID-19 pandemic became a major problem in the United States. Ultimately, only one institution of the 287 surveyed responded, the Ohio Secretary of State's Office. To read its response to our questions, please see Appendix 3.

Our review of the institutions' websites was more fruitful. Overall, we found that only 57 of the 287 institutions (20 percent) included any substantive references to business identity theft on their websites. These references covered a wide gamut of content, from informational articles specifically about business identity theft and detailed guides on what to do if you become a victim, to brief, vague or glancing references in press releases and reports on other topics. For the purposes of this report, any reference to business identity theft, no matter how small or inconsequential, even if it didn't directly use that term, was counted. The institutions with business identity theft references on their websites broke down as follows.

- 29 of 51 secretary of state offices or other state-level agencies responsible for registering businesses. (57 percent)¹
- Four of 74 state law enforcement agencies. (5 percent)²
- One of 51 state tax agencies (2 percent)³
- Four of the five federal agencies (80 percent)⁴
- Two of two private associations representing government employees responsible for business registration and organization. (100 percent)
- Three of three commercial credit rating agencies. (100 percent)⁵
- 14 of 101 large, private business concerns that process a lot of financial transactions. (14 percent)

Many of these institutions included just a few, scattered references on their websites. For example, the Arizona Corporation Commission, the agency responsible for registering businesses in the Grand Canyon State, mentions business identity theft briefly, in passing, in a FAQ published on its website:⁶

Q: My company is out of business – should I let the entity be administratively dissolved?

A: No. An administratively dissolved entity is subject to being reinstated. There have been situations where an entity is reinstated by persons who are not actually associated with the entity – this is business identity theft. If you are out of business, it is recommended you voluntarily dissolve or terminate the entity so that you do not subject your entity to potential business identity theft. If your corporation is out of business, you should submit Articles of Dissolution. If your LLC is out of business, you should submit Articles of Termination.

The only reference we could find to business identity theft on the South Carolina Secretary of State's was in a 2017 press release⁷ about the secretary (Mark Hammond) receiving an award; the press release mentions that he served on a national Business Identity Theft Task Force Subcommittee.

In the private sector, American Express mentions business identity theft just once on its website – in single line on the 21st page a February 2020 report⁸ about business-to-business commerce: "Business identity theft is used to launch everything from purchasing plan scams to tax and credit card application fraud, and it caused an estimated \$137 million in damages in 2017." The Phoenix-based Western Alliance Bank mentions business identity theft in passing in a three-year-old article⁹ published by its California subsidiary, Torrey Pines Bank, about ways for businesses to prevent fraud during the holiday season. The story mentions that employees can defraud businesses by committing simple acts, including embezzlement and identity theft, but offers no other information.

Twenty-one institutions, however, stood out as having a lot of valuable information about business identity on their websites.

> *State agencies in Colorado*

Colorado's reputation as a national leader in business identity theft enforcement is well earned. The Colorado Attorney General's office has published a comprehensive, 16-page business identity theft resource guide with tips for protecting your business and recovering from business identity theft.¹⁰ The Colorado Secretary of State also publishes similar information on its website¹¹ as well as a two-page pamphlet on business identity theft.¹²

Meanwhile, the Colorado Bureau of Investigation, a statewide law enforcement agency, has a unit dedicated to fighting this crime. Business identity theft is mentioned repeatedly in its annual reports¹³ and figures prominently in educational materials the bureau has published about business fraud and cybercrime.¹⁴

> *IRS and Treasury Inspector General for Tax Administration (federal agencies)*

At the federal level, no agency has posted more warnings about the dangers of business identity theft than the IRS. At irs.gov, you can find the "Tax Practitioner Guide to Business Identity Theft"¹⁵ and at least five extensive articles on the problem,¹⁶ with practical tips for addressing it.

The Treasury Inspector General for Tax Administration, which provides independent oversight of the IRS, began investigating the IRS' approach to business identity theft as early as 2013.¹⁷ Since then, the inspector general staff has written about business identity theft repeatedly in press releases,¹⁸ reports,¹⁹ audit plans²⁰ and budget documents, and spoke about it in transcribed testimony before Congress.²¹

> *National Association of Commercial Administrators (NASS) and International Association of Commercial Administrators (IACA, associations)*

Business identity theft has been a topic of conversation for members of NASS and IACA for years. NASS, the nation's oldest, nonpartisan professional organization for public officials, published a 23-page white paper on business identity theft in January 2012,²² which sparked a national, but still trivial, conversation about the crime. IACA, a professional association for government administrators of business organization and secured transaction record systems, began surveying its members about business identity theft as far back as 2010.²³

As such, references to business identity theft appear in all kinds of documents published by both associations, from conference materials²⁴ to merit award applications²⁵ to committee and listserv descriptions²⁶ to presentations²⁷ to press releases²⁸ and reports.²⁹

> *Dun & Bradstreet and Experian (credit rating agencies)*

Two of the nation's three major credit rating agencies have published extensive postings on the dangers of business identity theft. D&B's website boasts a treasure trove of white papers,³⁰ educational articles and policy proposals³¹ and tips for business owners.³² Experian has published more than a half-dozen in-depth articles on the topic since late 2010.³³

> *Bank of America, KeyCorp and FNB Corporation (large, private business concerns)*

The overwhelming majority of the private businesses reviewed had no information on their websites about business identity theft. Nearly a dozen had either a brief mention of the topic somewhere on their site, or one or maybe two information articles about it.³⁴

However, these three companies, which provide banking and other financial services to businesses and individuals, all stood out with the sheer number of educational articles they had published about business identity theft. FNB Corporation³⁵ featured three on its site. KeyCorp, four.³⁶ Bank of America, six.³⁷

> *Secretaries of state in California, Georgia, Nebraska, Ohio and Texas*

The secretaries of state for these five states have all published information about business identity theft on their websites.³⁸ While these postings are all limited to just one (or in the case of Georgia, two) webpages, each is incredibly detailed, with specific, actionable tips for business owners.

Interestingly, of the 210 institutions that had no substantive information about business identity theft on their websites, nine institutions (4 percent) were included in stories or posts about business identity theft on other websites, including news websites. This indicates that these nine institutions are also aware of business identity theft, but haven't posted information about it on their own website.

For example, several news organizations in Wyoming³⁹ have published warnings from the Wyoming Secretary of State about business identity theft – but no corresponding warnings were found on the Wyoming Secretary of State’s own website. A 2012 story in *Governing* magazine⁴⁰ quotes North Carolina Secretary of State Elaine Marshall about how little businesses know about business identity theft. But we found no mention of the crime on the North Carolina Secretary of State’s website.

For the full list of the institutions that did not have postings on their websites about business identity theft, but are referenced in stories about business identity theft on other websites, please see Appendix 4.

Discussion & Recommendations

It is entirely possible that the COVID-19 pandemic severely impacted these institutions’ ability to respond to our survey. However, it is also true that after the first few weeks of quarantine in March and April, work did resume in both government and the private sector.

It’s also possible that these institutions did not feel like it was their responsibility to aid another private business in research. But, as we made clear in our questionnaires, the information we sought to collect about business identity theft was solely going to be used in the public interest, to further publicize its threat to business owners large and small. We would hope that all of the institutions reviewed as a part of this report would be motivated to protect businesses.

Thus, it is our view that the dismal response rate to our survey simply reflects the nation’s general disregard for business identity theft and its victims. It seems clear at this point that at least some people in many, if not most, of these institutions are aware of the problem of business identity theft. But the crime is just not a priority.

It is our view that the information posted on the institutions’ websites – or lack thereof – also reflects this general and disappointing disregard.

State agencies

At the state level, it’s unsurprising that secretaries of state and other state-level offices responsible for registering businesses are among the best sources for information about business identity theft. That’s because their industry association, NASS, published a white paper about business identity theft in 2012 and has convened a task force focusing on the issue.

That said, given the NASS’ ongoing advocacy, you’d expect *all* of the nation’s secretaries of state would post information about the crime. Yet, we found 22 offices (43 percent) had no such information on their websites. Even with the NASS’ continued attention to the issue, more than a third of the nation’s business registration agencies ignore the crime.

Beyond the business registration agencies, the other state entities reviewed were, almost universally, dismal in their reporting, with the notable exception being the Colorado Bureau of Investigation, which appears well deserving of its reputation as a national leader on this crime.

Other than the Colorado bureau, only four other state agencies mentioned business identity theft on their websites: attorney generals for Colorado and Georgia, the Alaska Department of Law and the Pennsylvania Department of Revenue. The Georgia Attorney General published a single press release warning about the business identity theft,⁴¹ while the Alaska Department of Law published a press release about its efforts to tackle Alaska's first case of business identity theft.⁴²

The Pennsylvania Department of Revenue mentions business identity theft only in passing in a post about "unauthorized insurance."⁴³ That only one state tax agencies would post any information about business identity theft when its federal counterpart, the IRS, is one of the top institutions in America warning about it suggests a deep disconnect between federal and state priorities and concerns.

It is Company Alarm's view that business owners, particularly small business owners, are far more likely to interact with state-level government agencies than federal ones. As such, it is imperative that state officials lead the charge in the fight against business identity theft. But our research shows that, with a few exceptions, they are failing at this critical public service.

Federal agencies

With the exception of the Secret Service, every federal agency reviewed included information about business identity theft on their websites. As mentioned earlier, the IRS has consistently provided some of the nation's most comprehensive data and information about business identity theft, although the agency is narrowly focused on the filing of fraudulent tax returns, rather than larger concerns of business hijackings in order to secure illicit loans.

Meanwhile, the Treasury Inspector General for Tax Administration referenced the business identity on its website far more than any other institution in our review, thanks largely to its consistent inclusion in the inspector general's reports. The other two federal agencies posting information about business identity theft were the FBI and FTC, both of whom victims are recommended to contact for help. Ironically, neither of their websites had much in the way of information for victims. The FBI primarily published press releases about business identity theft cases⁴⁴ or mentioned business identity in passing in testimony before Congress or in reports.⁴⁵

The federal government's attention is, of course, a welcome discovery, but it's unclear to us how many business owners are actually visiting federal websites on a semi-regular basis. Likewise, while the IRS should be commended for producing solid statistics, there needs to be more and better tracking of business identity theft on a nationwide level, a task that could fall to the FBI and/or FTC, but has, thus far, not been handled by anyone at the national level.

Private entities

It is no surprise that the two private associations and the three credit rating agencies surveyed all published information about business identity theft on their websites. These are niche-focused institutions in which business identity theft plays a major, and increasing, role. Generally speaking, their information is informative and helpful.

But, once again, we question whether members of the public who need to learn about business identity theft are actually visiting these particular sites.

It's also disturbing that there was such a sizable gap between Equifax and Experian and Dun & Bradstreet. As reported above, Experian and Dun & Bradstreet had among the most informative websites in our review. However, Equifax, one of the nation's three major commercial credit rating agencies, had only one informational article.⁴⁶

Of course, we believe the websites that business owners are most likely to visit are those of the large, private business concerns, like banks and major retail outlets. These private institutions are perhaps the best positioned to spread the word about business identity theft – better than even the state-government institutions.

Yet, these private concerns, for the most part, seem uninterested in warning their customers about the dangers of business identity theft. You could reasonably argue that it is not their duty to offer such warnings. However, many of the 101 large, private businesses reviewed included warnings on their websites about personal identity theft, suggesting that they do believe it is their job to warn their customers about some threats. Just not business identity theft.

Recommendations

It is Company Alarm's belief that the vast majority of America's critical institutions are not taking the threat of business identity theft seriously, nor are they providing business owners with enough of the right kind of information. To that end, we recommend the following:

Recommendation 1: Every secretary of state or state-level business registration office collect annual statistics on the number of business identity theft incidents in their jurisdiction and forward that data to the Federal Trade Commission for an aggregated, nationwide report.

Recommendation 2: Every secretary of state or state-level business registration office, state tax agency and state law enforcement agency include information on their website about business identity theft, including guidance for victims.

Recommendation 3: Private business concerns that handle more than \$10 million worth of financial transactions each year develop a plan for protecting businesses from identity theft and publish information about these programs in a prominent place on their website.

Recommendation 4: Business organizations of all sizes and locales demand that their government representatives make business identity theft a top policy priority and develop guidance and resources for victims.

Recommendation 5: Government agencies at both the state and federal level work cooperatively to share information about business identity theft and develop policies and procedures for effectively and efficiently investigating and prosecuting criminal cases. In particular, state attorneys general and secretaries of state should be working closely together to search out and prosecute these crimes.

Recommendation 6: Laws at the local, state, and federal level be reformatted or, if needed, rewritten, to make it clear that stealing the identity of a business is as much a crime as impersonating an individual. These statutes should be clearly labelled and worded to communicate this important nuance.

Recommendation 7: State attorneys general and/or secretaries of state track on an annual basis all pieces of state legislation pertaining to business identity theft and make that information available to business organizations in their jurisdiction. The U.S. Department of Justice should also track such proposals at the Congressional level and report it annually to national business organizations, like the U.S. Chamber of Commerce.

Appendix 1

Here is the list of the 287 American institutions surveyed for this report.

Secretary of state offices and other state agencies that register businesses

- Alabama Secretary of State
- Division of Corporations, Business and Professional Licensing within the Alaska Department of Commerce, Community, and Economic Development
- Arizona Corporation Commission
- Arkansas Secretary of State
- California Secretary of State
- Colorado Secretary of State
- Connecticut Secretary of State
- Delaware Division of Corporations
- Florida Division of Corporations
- Georgia Secretary of State
- Hawaii Department of Commerce and Consumer Affairs
- Idaho Secretary of State
- Illinois Secretary of State
- Indiana Secretary of State
- Iowa Secretary of State
- Kansas Secretary of State
- Kentucky Secretary of State
- Louisiana Secretary of State
- Maine Secretary of State
- Maryland Department of Assessments & Taxation
- Secretary of the Commonwealth of Massachusetts

- Michigan Secretary of State
- Minnesota Secretary of State
- Mississippi Secretary of State
- Missouri Secretary of State
- Montana Secretary of State
- Nebraska Secretary of State
- Nevada Secretary of State
- New Hampshire Secretary of State
- New Jersey Division of Revenue and Enterprise Services
- New Mexico Secretary of State
- Division of Corporations, State Records & UCC within the New York Department of State
- North Carolina Secretary of State
- North Dakota Secretary of State
- Ohio Secretary of State
- Oklahoma Secretary of State
- Oregon Secretary of State
- Pennsylvania Department of State
- Rhode Island Secretary of State
- South Carolina Secretary of State
- South Dakota Secretary of State
- Tennessee Secretary of State
- Texas Secretary of State
- Division of Corporations and Commercial Code within the Utah Department of Commerce
- Vermont Secretary of State
- Virginia State Corporation Commission
- Washington Secretary of State
- Washington, D.C. Department of Consumer and Regulatory Affairs
- West Virginia Secretary of State
- Wisconsin Department of Financial Institutions
- Wyoming Secretary of State

State law enforcement agencies

- Alabama Law Enforcement Agency
- Alabama Attorney General
- Alaska Department of Public Safety
- Alaska Department of Law (Alaska Attorney General)
- Arizona Attorney General
- Arkansas Attorney General
- California Attorney General
- Colorado Bureau of Investigation
- Colorado Attorney General

- Connecticut Attorney General
- Delaware State Police
- Delaware Attorney General
- Florida Department of Law Enforcement
- Florida Attorney General
- Georgia Attorney General
- Hawaii Attorney General
- Idaho State Police
- Idaho Attorney General
- Illinois State Police
- Illinois Attorney General
- Indiana Attorney General
- Iowa Attorney General
- Kansas Attorney General
- Kentucky Attorney General
- Louisiana State Police
- Louisiana Attorney General
- Maine State Police
- Maine Department of Public Safety
- Maine Attorney General
- Maryland State Police
- Maryland Attorney General
- Massachusetts State Police
- Massachusetts Attorney General
- Michigan Attorney General
- Minnesota Attorney General
- Mississippi Attorney General
- Missouri Department of Public Safety
- Missouri Attorney General
- Montana Attorney General
- Nebraska Attorney General
- Nevada Department of Public Safety
- Nevada Attorney General
- New Hampshire Attorney General
- New Jersey State Police
- New Jersey Attorney General
- New Mexico Attorney General
- New York Attorney General
- North Carolina Department of Public Safety
- North Carolina Attorney General
- North Dakota Attorney General
- Ohio Attorney General

- Oklahoma Attorney General
- Oregon State Police
- Oregon Attorney General
- Pennsylvania State Police
- Pennsylvania Attorney General
- Rhode Island State Police
- Rhode Island Attorney General
- South Carolina Law Enforcement Division
- South Carolina Attorney General
- South Dakota Attorney General
- Tennessee Attorney General
- Texas Department of Public Safety
- Texas Attorney General
- Utah Attorney General
- Vermont Attorney General
- Virginia Attorney General
- Washington Attorney General
- Washington, D.C. Metropolitan Police Department
- Washington, D.C. Office of the Attorney General
- West Virginia State Police
- West Virginia Attorney General
- Wisconsin Department of Justice
- Wyoming Attorney General

State tax agencies

- Alabama Department of Revenue
- Alaska Department of Revenue
- Arizona Department of Revenue
- Arkansas Department of Finance and Administration
- California Franchise Tax Board
- Colorado Department of Revenue
- Connecticut Department of Revenue Services
- Delaware Division of Revenue
- Florida Department of Revenue
- Georgia Department of Revenue
- Hawaii Department of Taxation
- Idaho State Tax Commission
- Illinois Department of Revenue
- Indiana Department of Revenue
- Iowa Department of Revenue
- Kansas Department of Revenue

- Kentucky Department of Revenue
- Louisiana Department of Revenue
- Maine Revenue Services
- Maryland Office of the Comptroller
- Massachusetts Department of Revenue
- Michigan Department of Treasury
- Minnesota Department of Revenue
- Mississippi Department of Revenue
- Missouri Department of Revenue
- Montana Department of Revenue
- Nebraska Department of Revenue
- Nevada Department of Taxation
- New Hampshire Department of Revenue
- New Jersey Department of Treasury
- New Mexico Taxation and Revenue Department
- New York Department of Taxation and Finance
- North Carolina Department of Revenue
- North Dakota Office of the State Tax Commissioner
- Ohio Department of Taxation
- Oklahoma Tax Commission
- Oregon Department of Revenue
- Pennsylvania Department of Revenue
- Rhode Island Division of Taxation
- South Carolina Department of Revenue
- South Dakota Department of Revenue
- Tennessee Department of Revenue
- Texas Comptroller
- Utah State Tax Commission
- Vermont Department of Taxes
- Virginia Department of Taxation
- Washington Department of Revenue
- Washington, D.C. Office of Tax and Revenue
- West Virginia State Tax Department
- Wisconsin Department of Revenue
- Wyoming Department of Revenue

Federal agencies

- Federal Bureau of Investigation (FBI)
- U.S. Secret Service
- Federal Trade Commission (FTC)
- Internal Revenue Service (IRS)
- Treasury Inspector General for Tax Administration

Private associations representing government employees responsible for business registration and organization

- International Association of Commercial Administrators (IACA)
- National Association of Secretaries of State (NASS)

Credit Rating Agencies

- Dun & Bradstreet
- Experian
- Equifax

Large, private business concerns that process a lot of financial transactions

- JPMorgan Chase
- Bank of America
- Citigroup
- Wells Fargo & Co.
- Goldman Sachs
- Morgan Stanley
- U.S. Bancorp
- PNC Financial Services
- TD Bank
- Capital One
- Trust Financial
- The Bank of New York Mellon
- TIAA
- Charles Schwab Corporation
- HSBC Bank USA
- State Street Corporation
- American Express
- Ally Financial
- MUFG Union Bank
- Fifth Third Bank
- State Farm
- USAA
- Citizens Financial Group
- BMO Harris Bank
- Barclays
- KeyCorp
- UBS
- Santander Bank
- Deutsche Bank

- Regions Financial Corporation
- Credit Suisse
- RBC Bank
- Northern Trust
- BNP Paribas
- M&T Bank
- Discover Financial
- Huntington Bancshares
- Synchrony Financial
- BBVA USA
- Comerica
- E-Trade
- Zions Bancorporation
- Silicon Valley Bank
- New York Community Bank
- CIT Group
- Popular, Inc.
- People's United Financial
- Synovus
- Mutual of Omaha
- CIBC Bank USA
- East West Bank
- First Horizon National Corporation
- BOK Financial Corporation
- Mizuho Financial Group
- John Deere Capital Corporation
- Raymond James Financial
- First Citizens BancShares
- FNB Corporation
- Associated Banc-Corp
- BankUnited
- Valley National Bank
- Wintrust Financial
- Frost Bank
- IberiaBank
- Sterling Bancorp
- Hancock Whitney
- Texas Capital Bank
- Webster Bank
- Umpqua Holdings Corporation
- Investors Bank
- PacWest Bancorp

- Pinnacle Financial Partners
- Commerce Bancshares
- TCF Financial Corporation
- Stifel
- Western Alliance Bank
- UMB Financial Corporation
- Utrecht-America (Rabobank)
- Sumitomo Mitsui Financial Group
- Prosperity Bancshares
- Chemical Financial Corporation
- First National of Nebraska
- Bank OZK
- Fulton Financial Corporation
- First Hawaiian Bank
- Old National Bank
- United Bank (West Virginia)
- Flagstar Bank
- MidFirst Bank
- Macy's
- Arvest Bank
- FirstBank Holding Co
- Cadence Bank
- Bank of Hawaii
- Cathay Bank
- CenterState Bank
- Atlantic Union Bank
- Washington Federal
- Simmons Bank
- First Midwest Bank
- South State Bank

Appendix 2

Here are the survey questions we posed to the institutions.

Secretary of state offices and other state agencies that register businesses

- Do business owners or principals have the option of establishing a password or PIN associated with their business filings?
 - If yes, how does it work?

- Do business owners receive a notification when something has been changed in their filing?
 - If yes, can you provide an example of the notification messages they receive?
 - If yes, how are such notifications delivered? (i.e. via text message or e-mail)
- Does your office operate under the Model Business Corporation Act?
- Does your office have the legal authority to verify the accuracy or legitimacy of the filings it receives?
 - If yes, can you site the specific statute that gives your office that authority?
 - If yes, can you explain how your review system works?
 - If yes, can you explain how many staff members are devoted to this function and where you receive the funding for them?
- Does your office track anything related to business identity theft – including, but not limited to, verified cases or complaints?
 - If yes, can you provide summaries of all the years of data you have collected?
- Are you aware of any other government agency in the state that tracks data related to business identity theft?
 - If yes, can you identify them and what they track?
- What laws, if any, in your state make business identity theft a crime?
- What resources does your office make available to victims of business identity theft?
- Are you aware of any other government agencies in your state that make resources available to victims of business identity theft?
 - If yes, can you identify them and what those resources are?
- Is business identity theft discussed by policymakers in your state?
- Does your office discuss business identity theft with policymakers?

State law enforcement agencies

- Does your office track anything related to business identity theft – including, but not limited to, verified cases or complaints?
 - If yes, can you provide summaries all of the years of data you have collected?
- Are you aware of any other government agency in the state that tracks data related to business identity theft?
 - If yes, can you identify them and what they track?
- What laws, if any, in your state make business identity theft a crime?
- What resources does your office make available to victims of business identity theft?
- Are you aware of any other government agencies in your state that make resources available to victims of business identity theft?
 - If yes, can you identify them and what those resources are?
- How many staff members in your department are qualified to handle business identity theft cases?

State tax agencies

- Does your office track anything related to business identity theft – including, but not limited to, verified cases or complaints?
 - If yes, can you provide summaries all of the years of data you have collected?
- Are you aware of any other government agency in the state that tracks data related to business identity theft?
 - If yes, can you identify them and what they track?

- What laws, if any, in your state make business identity theft a crime?
- What resources does your office make available to victims of business identity theft?
- Are you aware of any other government agencies in your state that make resources available to victims of business identity theft?
 - If yes, can you identify them and what those resources are?

Federal agencies

Federal law enforcement agencies (FBI and U.S. Secret Service)

- Does your office track anything related to business identity theft – including, but not limited to, verified cases or complaints?
 - If yes, can you provide summaries all of the years of data you have collected?
- Are you aware of any other government agency that tracks data related to business identity theft?
 - If yes, can you identify them and what they track?
- What laws, if any, make business identity theft a crime?
- What resources does your office make available to victims of business identity theft?
- Are you aware of any other government agencies that make resources available to victims of business identity theft?
 - If yes, can you identify them and what those resources are?
- How many staff members in your agency are qualified to handle business identity theft cases?

Federal Trade Commission

- Does your office track anything related to business identity theft – including, but not limited to, verified cases or complaints?
 - If yes, can you provide summaries all of the years of data you have collected?
- Are you aware of any other government agency that tracks data related to business identity theft?
 - If yes, can you identify them and what they track?
- What laws, if any, make business identity theft a crime?
- What resources does your office make available to victims of business identity theft?
- Are you aware of any other government agencies that make resources available to victims of business identity theft?
 - If yes, can you identify them and what those resources are?
- How many staff members in your agency are qualified to handle business identity theft complaints?

Internal Revenue Service

- Does your office track anything related to business identity theft – including, but not limited to, verified cases or complaints?
 - If yes, can you provide summaries all of the years of data you have collected?
- Are you aware of any other government agency that tracks data related to business identity theft?
 - If yes, can you identify them and what they track?

- What laws, if any, make business identity theft a crime?
- What resources does your office make available to victims of business identity theft?
- Are you aware of any other government agencies that make resources available to victims of business identity theft?
 - If yes, can you identify them and what those resources are?

Treasury Inspector General for Tax Administration

- Does your office track anything related to business identity theft – including, but not limited to, verified cases or complaints?
 - If yes, can you provide summaries all of the years of data you have collected?
- Are you aware of any other government agency that tracks data related to business identity theft?
 - If yes, can you identify them and what they track?
- What laws, if any, make business identity theft a crime?
- What resources does your office make available to victims of business identity theft?
- Are you aware of any other government agencies that make resources available to victims of business identity theft?
 - If yes, can you identify them and what those resources are?

Private associations representing government employees responsible for business registration and organization

- Does your association track anything related to business identity theft – including, but not limited to, verified cases or complaints?
 - If yes, can you provide summaries all of the years of data you have collected?
- Are you aware of any entity that tracks data related to business identity theft?
 - If yes, can you identify them and what they track?
- What laws, if any, make business identity theft a crime?
- What resources does your association make available to victims of business identity theft?
- Are you aware of any other entity that make resources available to victims of business identity theft?
 - If yes, can you identify them and what those resources are?
- What effort has your association made to spread the word about business identity theft?
 - Is this an issue for which you are currently lobbying?

Credit Rating Agencies

- Does your association track anything related to business identity theft – including, but not limited to, verified cases or complaints?
 - If yes, can you provide summaries all of the years of data you have collected?
- Are you aware of any entity that tracks data related to business identity theft?
 - If yes, can you identify them and what they track?
- What laws, if any, make business identity theft a crime?
- What resources does your association make available to victims of business identity theft?
- Are you aware of any other entity that make resources available to victims of business identity theft?
 - If yes, can you identify them and what those resources are?

- What is the process for businesses to submit changes to their credit reporting file in your system?
- Can businesses buy from you a service that monitors their credit rating?
- Can businesses freeze their credit within your system?

Large, private business concerns that process a lot of financial transactions

- Does your association track anything related to business identity theft – including, but not limited to, verified cases or complaints?
 - If yes, can you provide summaries all of the years of data you have collected?
- Are you aware of any entity that tracks data related to business identity theft?
 - If yes, can you identify them and what they track?
- What laws, if any, make business identity theft a crime?
- What resources does your association make available to victims of business identity theft?
- Are you aware of any other entity that make resources available to victims of business identity theft?
 - If yes, can you identify them and what those resources are?

Appendix 3

Survey response from the Ohio Secretary of State's Office, as answered by the director business services and deputy assistant secretary of state.

Q: Do business owners or principals have the option of establishing a password or PIN associated with their business filings?

A: No

Q: If yes, how does it work?

A: N/A

Q: Do business owners receive a notification when something has been changed in their filing?

A: Yes – if they have submitted any online filing for the entity then they are signed up for our e-notification system. If they filed their entity on paper and haven't done online filings to update the record, then they only get notifications if they elected to sign up for this service on our website.

Q: If yes, can you provide an example of the notification messages they receive?

A: Struggling to find an example right now, but I will get one generated to forward to you.

Q: If yes, how are such notifications delivered? (i.e. via text message or e-mail)

A: Email

Q: Does your office operate under the Model Business Corporation Act?

A: No

Q: Does your office have the legal authority to verify the accuracy or legitimacy of the filings it receives?

A: No

Q: If yes, can you site the specific statute that gives your office that authority?

A: N/A

Q: If yes, can you explain how your review system works?

A: N/A

Q: If yes, can you explain how many staff members are devoted to this function and where you receive the funding for them?

A: N/A

Q: Does your office track anything related to business identity theft – including, but not limited to, verified cases or complaints?

A: No

Q: If yes, can you provide summaries of all the years of data you have collected?

A: N/A

Q: Are you aware of any other government agency in the state that tracks data related to business identity theft?

A: No

Q: If yes, can you identify them and what they track?

A: N/A

Q: What laws, if any, in your state make business identity theft a crime?

A: Unsure

Q: What resources does your office make available to victims of business identity theft?

A: <https://www.ohiosos.gov/businesses/business-identity-theft/>

Q: Are you aware of any other government agencies in your state that make resources available to victims of business identity theft?

A: Unsure

Q: If yes, can you identify them and what those resources are?

A: Unsure

Q: Is business identity theft discussed by policymakers in your state?

A: Not a lot – but our office is starting these conversations

Q: Does your office discuss business identity theft with policymakers?

A: Yes – we are brainstorming ideas to help protect business entities and some of them involve legislative fixes, and others would require system changes.

Appendix 4

Here are the institutions that did not post information about business identity theft on their own websites, but were featured in articles about business identity theft on other websites. Included are details about the articles on the other sites.

- TIAA (large, private business concern): The LinkedIn profile of a Denver-based investigator for the Teachers Insurance and Annuity Association of America-College Retirement Equities Fund, a financial services provider, indicates that the investigator previously investigated business identity theft for the Colorado Bureau of Investigation.⁴⁷
- North Carolina Secretary of State (state-level business registration office): A 2012 story in *Governing* magazine⁴⁸ quotes North Carolina Secretary of State Elaine Marshall as saying that “most business owners are somewhere between not knowledgeable and totally clueless” about business identity theft. The story also reports that North Carolina officials had discovered that criminals were particularly interested in hijacking dissolved businesses and again quotes Marshall as recommending that business owners reviewing their business filings with the state at least once a month to ensure they haven't been altered.
- Barclays (large, private business concern): In a 2018 Barclays-sponsored news report⁴⁹ about cybersecurity with the news service Reuters, Barclays reports that it is working to protect businesses from identity theft. “...Barclays, in partnership with Hitachi, has developed a biometric reader for its clients to help UK businesses combat identity fraud. By using finger vein reading technology, employees can easily access their online bank accounts and authorise [sic] payments, without the need for pins, passwords or authentication codes – all of which can be easily used by fraudsters.”
- Comerica (large, private business concern): In a 2006 article⁵⁰ in *Crain's Detroit Business* about business identity theft, employees of a Detroit-area Comerica bank talk about the need to spread the word about the crime. The relevant portions of the article state:

“To protect against ID theft businesses must make their customers and employees aware, said Scott Vowels, manager of the security architecture and engineering department at Comerica Bank’s Auburn Hills Operation Center.

“‘Comerica has a security awareness program where we work with all of the departments to make sure people are aware of the problems surrounding ID theft,’ he said.

“To protect information outside of the office, home computers should have proper security and suspicious emails should not be opened, said Ken Schaeffler, head of the corporate information security services department at Comerica Bank’s Auburn Hills Operations Center.”

- U.S. Secret Service (large, private business concern): At least three banks refer to the Secret Service in brief articles on their websites about business identity theft. One World Bank, based in Dallas, writes in a post about data security⁵¹ that “Conference of State Bank Supervisors and the Financial Services – Information Sharing and Analysis Center have joined with the United States Secret Service and Texas Department of Banking” to develop practices to mitigate “Corporate Account Takeover,” a form of business identity theft. Limestone Bank in Louisville, Kentucky⁵² and City State Bank in Iowa⁵³ have both posted information about business identity theft jointly released by the Secret Service, the FBI and the Internet Crime Complaint Center.⁵⁴ The Texas Department of Banking mentions in an exam⁵⁵ that “A task force of bankers in Texas worked with the U.S. Secret Service to develop recommended practices to mitigate the risks of electronic crimes such as corporate account takeover.”

The Secret Service is also referenced in two news stories about business identity theft. In a 2018 *South Florida Sun-Sentinel* story⁵⁶ about an attorney who was the victim of business identity theft, quotes an Orlando police detective investigating the case who is looking for help from the Secret Service to subpoena documents. In a 2010 article in the *Colorado Independent* about business identity theft in the Colorado,⁵⁷ the director of the Colorado Bureau of Investigation is quoted as saying the pursuing business identity theft cases “in conjunction with the Los Angeles County Sheriff’s Office and the U.S. Secret Service.”

- Wyoming Secretary of State (state-level business registration office): Four news stories –published by KTWO radio (Wyoming),⁵⁸ Wyoming Public Media,⁵⁹ the *Casper Star-Tribune*,⁶⁰ and KGAB radio (Wyoming)⁶¹ – all quote warnings, by Wyoming Secretary of State, about business identity theft.
- JPMorgan Chase (large, private business concern): Hackers stole the identities of seven million businesses by accessing JPMorgan’s digital records. This 2014 breach was reported on [fightingidentitycrimes.com](#)⁶² and [armstrongarchives.com](#).⁶³
- Division of Corporations, Business and Professional Licensing within the Alaska Department of Commerce, Community, and Economic Development (state-level business registration office): The Alaska agency responsible for registering businesses is mentioned in a 2019 KTVA (Anchorage, Alaska) news report about the Alaska Attorney General filing the state’s first lawsuit involving business identity theft.⁶⁴
- Vermont Secretary of State (state-level business registration office): The news website VTDigger published a 2011 press release from the Vermont Secretary of State warning about the dangers of business identity theft.⁶⁵ The National Notary Association published a 2012 post about the Vermont Secretary of State launching online resources to help “businesses protect themselves against identity theft.”⁶⁶

About Company Alarm

Company Alarm combats business identity theft by offering businesses 24-hour monitoring of their information on file with the local government. If any of that information is ever changed, which could be a sign of business identity theft, business owners receive an immediate text alerting them to exactly what changed. Company Alarm was founded by serial entrepreneur Andy Pham after a holding company he used to house a \$5 million piece of land was hijacked by identity thieves. For more information, visit www.companyalarm.com.



Endnotes

Findings

¹These were the 29 secretary of state offices or other state-level agencies responsible for registering businesses: Alabama Secretary of State, Arizona Corporation Commission, Arkansas Secretary of State, California Secretary of State, Colorado Secretary of State, Connecticut Secretary of State, Florida Division of Corporations, Georgia Secretary of State, Hawaii Department of Commerce and Consumer Affairs, Idaho Secretary of State, Indiana Secretary of State, Iowa Secretary of State, Kentucky Secretary of State, Louisiana Secretary of State, Maine Secretary of State, Minnesota Secretary of State, Mississippi Secretary of State, Montana Secretary of State, Nebraska Secretary of State, Nevada Secretary of State, Ohio Secretary of State, Oregon Secretary of State, Rhode Island Secretary of State, South Carolina Secretary of State, Tennessee Secretary of State, Texas Secretary of State, Utah Secretary of State, Washington Secretary of State, and West Virginia Secretary of State.

²These were the four state law enforcement agencies: Colorado Bureau of Investigation, Alaska Department of Law, Colorado Attorney General and Georgia Attorney General.

³The state tax agency was the Pennsylvania Department of Revenue.

⁴The federal agencies were Federal Bureau of Investigation, Federal Trade Commission, Internal Revenue Service, and Treasury Inspector General for Tax Administration.

⁵These were the 14 large, private business concerns that process a lot of financial transactions: American Express, Bank of America, BNP Paribas, Citizens Financial Group, First Horizon National Corporation, FNB Corporation, Huntington Bancshares, Investors Bank, KeyCorp, M&T Bank, Morgan Stanley, The Bank of New York Mellon, Western Alliance Bank, and Wintrust Financial.

⁶See “General Questions” on <https://ecorp.azcc.gov/AzFAQ/Index#>.

⁷See “Hammond Receives Medallion Award from National Association of Secretaries of State,” <<https://sos.sc.gov/news/2017-07/hammond-receives-medallion-award-national-association-secretaries-state>>: “...Hammond was recognized for his outstanding service and longtime leadership support, including multiple committee leadership roles. Since 2004, Secretary Hammond chaired, co-chaired or served on the Standing Committee for Business Services; Company Formation Task Force Subcommittee; Business Identity Theft Task Force Subcommittee; and the Standing Committee on International Relations.”

⁸See B2B eCommerce report, February 2020, <https://www.americanexpress.com/content/dam/amex/us/merchant/pdf/B2B_eCommerce_Report-February-2020.pdf>

⁹See "9 Ways to Help Prevent Business Fraud This Holiday Season,"

<<https://www.westernalliancebancorporation.com/torrey-pines-home/about-torrey-pines/insights/insights-details/9-ways-to-help-prevent-business-fraud-this-holiday-season>>

¹⁰See "Business Identity Theft Resource Guide: A Guide to Protecting Your Business and Recovering from Business Identity Theft, January 24, 2012" <<https://www.stopfraudcolorado.gov/sites/default/files/BITguide.pdf>>

¹¹See "A Guide to Protecting Your Business and Recovering from Business Identity Theft"

<<https://www.sos.state.co.us/pubs/business/ProtectYourBusiness/protectYourBusiness.html>>

¹²See "Colorado Secretary of State: Business Identity Theft"

<<https://www.sos.state.co.us/pubs/business/ProtectYourBusiness/BusinessIdentityTheftPamphlet.pdf>>

¹³See 2014 CBI Annual Report

<https://www.colorado.gov/pacific/sites/default/files/CBI%20Annual%20Report_2014.pdf>, 2015 CBI Annual Report

<https://www.colorado.gov/pacific/sites/default/files/CBI%20Annual%20Report%202015_1.pdf>, 2016 CBI Annual

Report <https://www.colorado.gov/pacific/sites/default/files/CBI%20Annual%20Report_2016.pdf>, 2017 CBI Annual

Report <https://www.colorado.gov/pacific/sites/default/files/CBI%20Annual%20Report_2017.pdf>, 2018 CBI Annual

Report <https://www.colorado.gov/pacific/sites/default/files/CBI%20Annual%20Report_2018.pdf>, 2019 CBI Annual

Report <<https://www.colorado.gov/pacific/sites/default/files/2019%20CBI%20Annual%20Report.pdf>>

¹⁴See "Types of Identity Theft and Fraud" <<https://www.colorado.gov/pacific/cbi/types-identity-theft-and-fraud>>,

"Identity Theft/Fraud and Cyber Crimes Unit Role"

<<https://www.colorado.gov/pacific/cbi/identity-theft-fraud-and-cyber-crimes-unit-role>>, and "Identity Theft, Fraud and

Cyber Crimes FAQs" <<https://www.colorado.gov/pacific/cbi/identity-theft-fraud-and-cyber-crimes-faqs>>

¹⁵See <<https://www.irs.gov/pub/irs-utl/PractitionerGuideBMFIDT051415.pdf>> and

<<https://www.irs.gov/tax-professionals/tax-practitioner-guide-to-business-identity-theft>>

¹⁶See "Identity Theft Information for Businesses"

<<https://www.irs.gov/individuals/identity-theft-information-for-businesses>>, "Five Signs of Small Business Identity Theft, New Protection Methods"

<<https://www.irs.gov/newsroom/five-signs-of-small-business-identity-theft-new-protection-methods>>, "Identity theft remains on IRS' "Dirty Dozen" list despite progress"

<<https://www.irs.gov/newsroom/identity-theft-remains-on-irs-dirty-dozen-list-despite-progress>>, "IRS urges small businesses: Protect IT systems from identity theft"

<<https://www.irs.gov/newsroom/irs-urges-small-businesses-protect-it-systems-from-identity-theft>>

¹⁷See "Stolen and Falsely Obtained Employer Identification Numbers are Used to Report False Income and Withholding," September 23, 2013, <<https://www.treasury.gov/tigta/auditreports/2013reports/201340120fr.pdf>>

¹⁸See "IRS Could Improve Detection of Business Identity Theft, TIGTA Finds," November 10, 2015 <https://www.treasury.gov/tigta/press/press_tigta-2015-36.htm>, "Actions Are Needed to Reduce the Risk of Fraudulent Use of Employer Identification Numbers and to Improve the Effectiveness of the Application Process," February 12, 2018 <https://www.treasury.gov/tigta/press/press_tigta-2018-05.htm>

¹⁹See "Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection," September 9, 2015 <<https://www.treasury.gov/tigta/auditreports/2015reports/201540082fr.pdf>>, Treasury Inspector General for Tax Administration, Semiannual Report to Congress, October 1, 2015 to March 31, 2015 <https://www.treasury.gov/tigta/semiannual/semiannual_mar2016.pdf>, Treasury Inspector General for Tax Administration, Semiannual Report to Congress, April 1, 2016 to September 30, 2016 <<https://www.treasury.gov/tigta/semiannual/semiannualsept2016.pdf>>, "Actions Are Needed to Reduce the Risk of Fraudulent Use of Employer Identification Numbers and to Improve the Effectiveness of the Application Process," February 7, 2018 <<https://www.treasury.gov/tigta/auditreports/2018reports/201840013fr.pdf>>, Treasury Inspector General for Tax Administration, Semiannual Report to Congress, October 1, 2018 to March 31, 2019 <https://www.treasury.gov/tigta/semiannual/semiannual_mar2019.pdf>, "Criminal Investigation Should Increase Its Role in Enforcement Efforts Against Identity Theft," August 28, 2019 <<https://www.treasury.gov/tigta/auditreports/2019reports/201930047fr.pdf>>, "Strengthened Validation Controls Are Needed to Protect Against Unauthorized Filing and Input of Fraudulent Information Returns," September 26, 2019 <<https://www.treasury.gov/tigta/auditreports/2019reports/201940071fr.pdf>>

²⁰See Treasury Inspector General for Tax Administration, Fiscal year 2018 Annual Audit Plan <https://www.treasury.gov/tigta/auditplans/auditplans_fy2018.pdf>, Treasury Inspector General for Tax Administration, Fiscal year 2019 Annual Audit Plan <https://www.treasury.gov/tigta/auditplans/auditplans_fy2019.pdf>, and Treasury Inspector General for Tax Administration, Fiscal year 2020 Annual Audit Plan <https://www.treasury.gov/tigta/auditplans/auditplans_fy2020.pdf>

²¹See "Hearing Before the Committee on the Budget United States Senate: 'Identity Theft,'" August 26, 2015 <https://www.treasury.gov/tigta/congress/congress_08262015.pdf>, "Hearing Before the Committee on Appropriations Subcommittee on Financial Services and General Government United States Senate: 'Review of the President's Fiscal Year 2017 Funding Request for the Internal Revenue Service,'" March 8, 2016 <https://www.treasury.gov/tigta/congress/congress_03082016.pdf>, "Hearing Before the Committee on Ways and Means Subcommittee on Oversight U.S. House of Representatives: 'The 2016 Tax Filing Season,'" April 19, 2016 <https://www.treasury.gov/tigta/congress/congress_04192016.pdf>, "Hearing Before the Committee on Appropriations Subcommittee on Financial Services and General Government United States Senate: 'Review of the President's Fiscal Year 2018 Funding Request for the Internal Revenue Service,'" July 26, 2017 <https://www.treasury.gov/tigta/congress/congress_07262017.pdf>, "Joint Hearing Before the Committee on Oversight and Government Reform, Subcommittee on Health Care, Benefits and Administrative Rules and Subcommittee on Government Operations U.S. House of Representatives: 'Continued Oversight of the Internal Revenue Service,'" April 17, 2018 <https://www.treasury.gov/tigta/congress/congress_04172018.pdf>

²²See "Developing State Solutions to Business Identity Theft: Assistance, Prevention, and Detection Effort by Secretary of State Offices," January 2012,

<<https://www.nass.org/sites/default/files/surveys/2017-08/white-paper-business-id-theft-012612.pdf>>

²³See <<https://www.iaca.org/wp-content/uploads/20101027BusinessIDTheft.pdf>>, <<https://www.iaca.org/wp-content/uploads/20120105CorporateldentityTheft.pdf>>, <<https://www.iaca.org/wp-content/uploads/20130903Business-Identity-Theft.pdf>>

²⁴For IACA, see

<<https://www.iaca.org/wp-content/uploads/IACA-2019-Conference-Planning-Agenda-and-Locations-5.2.19.pdf>>, <<https://www.iaca.org/wp-content/uploads/37th-Annual-Conference-Agenda2.pdf>>, <https://www.iaca.org/wp-content/uploads/2012_Virginia_IACA_Conference_Agenda.pdf>, <<https://www.iaca.org/wp-content/uploads/2014-Conference-Minutes.docx>>, <https://www.iaca.org/wp-content/uploads/2012_Conference_Invitation_Letter-.pdf>, <https://www.iaca.org/wp-content/uploads/2012_Conference_Preview2-1.pdf>, <<https://www.iaca.org/wp-content/uploads/2019-Conference-Registration-Invitation-Letter.pdf>>. For NASS, see <<https://www.nass.org/node/1802>>, <<https://www.nass.org/node/246>>, <<https://www.nass.org/node/245>>, <<https://www.nass.org/node/253>>

²⁵For IACA, see <https://www.iaca.org/wp-content/uploads/COLORADO_1.pdf>, <<https://www.iaca.org/wp-content/uploads/Hawaii-MyBusiness-Alerts.pdf>>, <<https://www.iaca.org/wp-content/uploads/USA-VERMONT-2014-small.pdf>>.

²⁶For IACA, see <<https://www.iaca.org/business-organization/2013-2014-bos-list-serve-summaries/>>. For NASS, see <<https://www.nass.org/committees/business-services-committee>>, <<https://www.nass.org/sites/default/files/events/2016%20Summer/co-business-id-theft-summer16.pdf>>

²⁷For IACA, see <<https://www.iaca.org/wp-content/uploads/Jurisdictional-Presentation-Hawaii1.pdf>>, <<https://www.iaca.org/wp-content/uploads/ECRF-CRF-IACA-Business-Registries-Report-Presentation.pdf>>. For NASS, see <<https://www.nass.org/sites/default/files/Winter%202020%20Presentations/presentation-sos-winter20.pdf>>, <<https://www.nass.org/sites/default/files/2019%20Summer/presentations/presentation-reynolds-summer19.pdf>>, <<https://www.nass.org/sites/default/files/events/2016%20Summer/co-business-id-theft-summer16.pdf>>.

²⁸For NASS, see <<https://www.nass.org/node/248>>, <<https://www.nass.org/node/244>>.

²⁹For IACA, see <<https://www.iaca.org/wp-content/uploads/2014-International-Business-Registers-Report.pdf>>, <<https://www.iaca.org/wp-content/uploads/The-Journey-2007-2016-Report-Shrunk.pdf>>. For NASS, see <<https://www.nass.org/sites/default/files/2020-01/white-paper-smartmatic-nass-winter20.pdf>>

³⁰See "Best Practices in Registration Data Management: Government agencies can reduce fraud and turn registrant data into a powerful asset," 2011

<https://www.dnb.com/content/dam/english/dnb-solutions/risk-management/whitepaper_registration_management.pdf>, "Enabling Commerce. Mitigating Business Fraud. Strategies for Businesses to stop fraud without slowing commerce," August 2013

<https://www.dnb.com/content/dam/english/dnb-solutions/risk-management/enabling_commerce_mitigating_business_fraud.pdf>,

"Busting Bust-Out Fraud: Five steps for combatting bust-out business fraud," 2015

<<https://www.dnb.com/content/dam/english/business-trends/dnb-bust-out-business-fraud-whitepaper.pdf>>

³¹See "Tax & Revenue: Increase tax revenue while ensuring compliance and preventing fraud"

<<https://www.dnb.com/solutions/government/federal/tax-revenue.html>>, "Tax Administration: Uncover the relationships among business identity theft schemes"

<https://www.dnb.com/content/dam/english/business-trends/tax_administration.pdf>, "Why small businesses should manage their business credit"

<<https://www.dnb.com/content/dam/US/dnb/legacy/small-business-manage-business-credit.pdf>> and "Tackling Corporate Identity Theft with a Public-Private Partnership"

<https://www.dnb.com/content/dam/english/dnb-solutions/risk-management/tackling_corporate_identity_theft.pdf>

³²See "The 5Cs of Fraud Prevention"

<<https://www.dnb.com/perspectives/finance-credit-risk/fraud-prevention-tips.html>> and "How to Protect Against Business Identity Theft" <<https://www.dnb.com/resources/business-identity-theft.html>>

³³See "Business Identity Theft: How to Protect your business from identity theft and other forms of fraud"

<<https://www.experian.com/small-business/business-identity-theft>>, "Protection your business from identity theft," December 7, 2010

<<http://www.experian.com/blogs/data-breach/2010/12/07/protecting-your-business-from-identity-theft/>>, "New forms of small business identity theft," December 16, 2010

<<https://www.experian.com/blogs/insights/2010/12/new-forms-of-small-business-identity-theft/>>, "Corporate account takeover is a serious fraud risk; but good resources are available," June 21, 2011

<<http://www.experian.com/blogs/insights/2011/06/corporate-account-takeover-is-a-serious-fraud-risk-but-good-resources-are-available/>>, "Small Businesses: Targets of Deception," May 2013

<<http://www.sbcr.experian.com/Marketing/May13-BC-Anderson.pdf>>, "Is small business fraud overlooked?" October 19, 2015 <<https://www.experian.com/blogs/insights/2015/10/dont-overlook-small-business-fraud/>>, "Business identity theft poses a growing threat: Scammers look past consumers to target companies' credit profiles, assets," February 24, 2020 <<https://www.creditcards.com/credit-card-news/business-identity-theft/>>

³⁴The 11 large, private institutions were American Express, BNP Paribas, Citizens Financial Group, First Horizon National Corporation, Huntington Bancshares, Investors Bank, M&T Bank, Morgan Stanley, The Bank of New York Mellon, Western Alliance Bank, and Wintrust Financial.

³⁵See "Reducing the Risk of Corporate Account Takeover"

<https://www.fnbbellville.com/Business/Corporate-Account-Takeover>, "Business Identity Theft and Corporate Account Takeover Risk Assessment"

<https://www.fnbhereford.com/_kcms-doc/390/21854/Business-Identity-Theft-and-Corporate-Account-Takeover-Risk-Assessment.pdf>, and "Corporate Account Takeover (CATO)"

<<https://www.fnbh.com/business/corporate-account-takeover--cato->>

³⁶See "What is Business Identity Theft?" <<https://www.key.com/about/security/business-identity-theft.jsp>>, "Business Information Security and You <<https://www.key.com/about/security/business-banking-information-identity-theft.jsp>>, "Cybersecurity & Fraud: Strong security safeguards for your protection."

<<https://www.key.com/businesses-institutions/solutions/cybersecurity.jsp>>, and "Identity Theft: Working hard to protect your identity from cyberthreats." <<https://www.key.com/about/security/identity-theft.jsp>>

³⁷See "Business Identity Fraud: What it is and eight ways to prevent it"

<<https://smallbusinessonlinecommunity.bankofamerica.com/community/running-your-business/technology/blog/2013/03/06/business-identity-fraud-what-it-is-and-eight-ways-to-prevent-it>>, "Business Identity Theft in the U.S. - 2018 Report"

<<https://smallbusinessonlinecommunity.bankofamerica.com/community/running-your-business/technology/blog/2018/11/30/business-identity-theft-in-the-us-2018-report>>, "Tips to Protect Business Identity"

<<https://smallbusinessonlinecommunity.bankofamerica.com/community/running-your-business/technology/blog/2018/11/29/tips-to-protect-business-identity>>, "Business Identity Theft in the U.S: Victim Resources"

<<https://smallbusinessonlinecommunity.bankofamerica.com/community/running-your-business/technology/blog/2018/11/29/business-identity-theft-in-the-us-victim-resources>>, "Business Identity Theft Scams"

<<https://smallbusinessonlinecommunity.bankofamerica.com/community/running-your-business/technology/blog/2018/11/29/business-identity-theft-scams>>, and "Resource Guide: Business Identity Theft"

<<https://smallbusinessonlinecommunity.bankofamerica.com/community/managing-your-finances/cash-management/blog/2013/06/13/resource-guide-business-identity-theft>>

³⁸See "Secretary of State Business Identity Theft Resources"

<<https://www.sos.ca.gov/business-programs/customer-alerts/alert-business-identity-theft/>>, "Corporate Identity Theft Information" <https://sos.ga.gov/index.php/corporations/corporate_identity_theft_information>, "Corporate ID Theft Information" <https://sos.ga.gov/index.php/corporations/corporate_id_theft_information>, "Preventing Business Identity Theft <<https://sos.nebraska.gov/sites/sos.nebraska.gov/files/doc/business-identity-theft-prevention.pdf>>, "Business Identity Theft: Business ID Theft Protect Yourself"

<<https://sos.nebraska.gov/sites/sos.nebraska.gov/files/doc/business-identity-theft-prevention.pdf>>, "Business Identity Theft: Business ID Theft Protect Yourself"

<<https://www.ohiosos.gov/businesses/business-identity-theft/> > and "Business Identity Theft,"

<<https://www.ohiosos.gov/businesses/business-identity-theft/> > and "Business Identity Theft,"

<<https://www.sos.state.tx.us/corp/businessidentitytheft.shtml>>

³⁹See <<https://k2radio.com/secretary-of-state-warns-of-business-identity-theft/>>,

<<https://www.wyomingpublicmedia.org/post/maxfield-warns-business-identity-theft#stream/0>>,

<https://trib.com/news/state-and-regional/govt-and-politics/wyoming-legislative-committee-tackles-corporate-fraud-is-sues/article_59b2bf3c-68b2-5d84-9316-a2f513265b9c.html>,

<<https://kgab.com/wyoming-building-commission-considers-revisions-to-policy-audio/>>

⁴⁰See <https://www.governing.com/news/state/secretaries-of-state-try-to-combat-a-new-form-of-identity-theft.html>

Discussion & Recommendations

⁴¹See [https://law.georgia.gov/press-releases/2018-06-04/consumer-alert-attorney-general-chris-carr-warns-consumers-time share](https://law.georgia.gov/press-releases/2018-06-04/consumer-alert-attorney-general-chris-carr-warns-consumers-time-share)

⁴²See <http://www.law.state.ak.us/press/releases/2019/011819-Webb.html>

⁴³See https://revenue-pa.custhelp.com/app/answers/detail/a_id/2991/~what-is-unauthorized-insurance%3F

⁴⁴See <<https://www.justice.gov/usao-edva/pr/las-vegas-man-pleads-guilty-corporate-identity-theft-scheme>>, <<https://www.justice.gov/usao-edva/pr/corporate-hijacker-sentenced-14-million-id-theft-scheme>>, <<https://archives.fbi.gov/archives/miami/press-releases/2012/boca-raton-resident-charged-with-mail-fraud-in-corporate-identity-theft-scheme>>

⁴⁵See <<https://archives.fbi.gov/archives/news/testimony/identity-theft-and-cyber-crime>>, <https://www.fbi.gov/stats-services/publications/fcs_report2005>, <https://www.fbi.gov/stats-services/publications/fcs_report2006>, <https://www.fbi.gov/stats-services/publications/fcs_report2007>, <https://www.fbi.gov/stats-services/publications/fcs_report2008>, <<https://archives.fbi.gov/archives/news/testimony/the-need-for-increased-fraud-enforcement-in-the-wake-of-the-economic-downturn>>, <<https://archives.fbi.gov/archives/news/testimony/fbis-efforts-in-combating-mortgage-fraud>>

⁴⁶See <https://insight.equifax.com/cerca-recap-identity-fraud-tax-reform-implementation/>

Appendix 4, Institutions Featured on Other Websites

⁴⁷See Kevin Hyland profile, <<https://www.linkedin.com/in/kevin-hyland-20122611/>>

⁴⁸See "States Work To Combat Business Identity Theft: Business records in many states can be edited by just about anybody, making them an easy target for scammers," by Ryan Holeywell, March 26, 2012, <<https://www.governing.com/news/state/secretaries-of-state-try-to-combat-a-new-form-of-identity-theft.html>>

⁴⁹See "Cyber crime is most serious threat to businesses," by Barclays Corporate Banking, October 3, 2018, <<https://www.reuters.com/sponsored/article/When-it-comes-to-cyber-security-dont-wait-until-you-become-a-victim>>

⁵⁰See "25: Protect against identity theft," by Katie Maurer, September 1, 2006, <<https://www.craigslist.com/article/20060901/HOWTO/60810008/25-protect-against-identity-theft>>

⁵¹See <https://www.oneworldbank.com/cybersecurity/>

⁵²See <https://www.limestonebank.com/corporate-takeover>

⁵³See <https://www.citystatebank.com/tools/security>

⁵⁴See "Fraud Advisory for Businesses: Corporate Account Takeover,"
<<https://www.limestonebank.com/assets/files/Ealzgded/2017/03/16/CorporateAccountTakeOver.pdf>>

⁵⁵See "#17 Account Takeover Risks,"
<<https://www.dob.texas.gov/public/uploads/files/Bank-Trust-Companies/Exam-Procedures/it17-ato.pdf>>

⁵⁶See "'Like being in the Twilight Zone': Lawyer on hunt for thief who stole his identity," by Anne Geggis, May 11, 2018,
<<https://www.sun-sentinel.com/news/crime/fl-pn-lawyer-identity-stolen-20180508-story.html>>

⁵⁷See "New scam takes advantage of Secretary of State's business filing system," by Joseph Boven, July 16, 2010,
<<https://www.coloradoindependent.com/2010/07/16/new-scam-takes-advantage-of-secretary-of-states-business-filing-system/>>

⁵⁸See <https://k2radio.com/secretary-of-state-warns-of-business-identity-theft/>

⁵⁹See <https://www.wyomingpublicmedia.org/post/maxfield-warns-business-identity-theft#stream/0>

⁶⁰See
https://trib.com/news/state-and-regional/govt-and-politics/wyoming-legislative-committee-tackles-corporate-fraud-issues/article_59b2bf3c-68b2-5d84-9316-a2f513265b9c.html

⁶¹See <https://kgab.com/wyoming-building-commission-considers-revisions-to-policy-audio/>

⁶²See <https://www.fightingidentitycrimes.com/jpmorgan-chase-hacked-76-million-households-exposed/>

⁶³See <https://www.armstrongarchives.com/business-id-theft-protection/>

⁶⁴See <https://www.ktva.com/story/39817496/state-reports-first-case-of-business-identity-theft>

⁶⁵See <https://vtdigger.org/2011/10/18/secretary-of-state-condos-continues-fight-against-business-identity-theft/>

⁶⁶See <https://www.nationalnotary.org/notary-bulletin/blog/2012/06/business-identity-theft-anti-fraud-resources>