Business Identity Theft State of the Industry 2020 Report

companyalarm.com

COMPANY ALARM®

Where do we stand with business identity theft today?

At the beginning of a new year and a new decade, business identity theft looms as a major threat facing all American businesses. Several statistics indicate incidents of this crime are on the rise while the personal anecdotes of victims, like Company Alarm's founder Andy Pham, speak to tremendous impact it has on businesspeople.

Meanwhile, the authorities are doing little to address this burgeoning crime. No one in government at the state or federal level is collecting data on business identity theft and few in law enforcement understand it or will even pursue cases.

In the private security sector, some identity theft companies offer educational materials or programs to protect business's employees or immediate response services in the case of a data breach. But as we understand business identity theft, none of these services actually address its major consequences, like the hijacking of your company.

As far as we can tell, Company Alarm is the only service in the United States today that offers businesses real, practical protections against business identity theft. It certainly possesses the most robust storehouse of educational material on the topic.

Here's what we will be looking at in this report:

- The legal environment today, which allows business identity theft to flourish
- The leading indicators about the crime's prevalence
- Government's response to the crisis
- The availability of support for businesses

The legal environment today

Every state has a government agency specifically responsible for processing business registration documents. These documents include the articles of incorporation you file when you first establish your business as well as the annual filings you have to make in order to keep your business active and in good standing.

In most states, this task is handled by the Secretary of State – but not all. It might be handled by your state's Division of Corporations or the Corporation Commission.

Whatever the agency's name, in most cases state authorities assumed from the very beginning that these agencies' sole purpose was going to be a ministerial function – that is, ensuring that forms were filled out correctly and that filings were properly organized and stored.

As such, when the states established these agencies they granted them extremely limited powers. The power to confirm that a form was filled out correctly. The power to organize the filings and store them in big filing cabinets. That's it.

Notably, the vast majority of states did not give these agencies any discretionary power to confirm the accuracy or legitimacy of the filings presented to them. They simply have the power to see if the forms are properly filled in. If they are, the agencies have to accept them and make them official records, with no questions asked.

That's the loophole cybercriminals exploit to hijack businesses in the United States.

How the Internet made it worse

Before the Internet, filing business records with the state was a pain. You had to track down the proper forms and then submit the filings by mail or drive to your state capital and deliver the paperwork in person.

It was time consuming and onerous. The chances of someone intentionally filing a fraudulent document with the state were slim. That's why the agencies were given such limited powers to begin with. In an analog, paperwork, who could imagine a criminal investing the time and effort to file the paperwork necessary to hijack a business?

All that changed, of course, with the Internet. To make the lives of businesspeople easier, state agencies posted their forms online. They posted massive databases of all the registered businesses in their state. And, most critically, they made it so businesses could easily and quickly file their paperwork online.

Now, with just a few mouse clicks, you can file the paperwork necessary to establish a business or update its status – or change its address or managing members. What's more, thanks to those databases, you can look up the identifying information of literally any and every business in a given state.

In short, these state websites designed to make the lives of businesspeople easier have in truth made it incredibly simple for criminals to research companies and then take them over.

In practice, the states offer no real barrier against the filing of fraudulent business documents.

Leading indicators about business identity theft

Ralph Gagliardi, a Company Alarm advisor and a Colorado-based criminal investigator who leads one of the nation's only law enforcement units dedicated to business identity theft, says the crime is "one of the biggest problems facing American businesses today, but virtually no one knows about it."

Indeed, he's correct: There are very few reliable statistics available about business identity theft, since no one in government at the state or federal level tracks it. As it stands today, business identity theft is not a priority for the powers that be.

Which is all the more surprising when you examine the few good numbers that are available. Because all of them indicate that business identity theft is not only serious, but on the rise.

Overall, many estimate, including the FBI, that business identity theft accounts for hundreds of millions or even billions of dollars in losses each year. But that's just the tip of the iceberg.

In July 2017, the Internal Revenue Service reported a 2,757 percent increase in the filing of fraudulent tax returns for businesses from 2015 to 2017.

In 2015, the IRS discovered 350 fraudulent tax returns had been filed for businesses. A year later, that number jumped to 4,000. The following year: About 10,000.

Along with the spike incidents, the IRS saw a corresponding increase in potential losses: $122 million in 2015, $268 million in 2016 and $137 million in 2017.

A year later, Dun & Bradstreet, the commercial credit reporting agency based out of New Jersey, reported a major jump in business identity theft for the six-year period from 2007 to 2012. D&B saw the incidents of the crime decrease from 2013 to 2015, then jump again beginning in 2016.

In 2017, D&B saw incidents of business identity theft rise 46 percent year after year, the largest increase of any year since it began tracking the crime in 2005.

In the world of business identity theft, the IRS and D&B are two of the few big names on top of the issue. And both say the crime is on the rise.

The government's response

Business identity theft is not a priority for policymakers, politicians or even law enforcement officers.

In February 2017, the National Association of Secretaries of State reported on the results of its business identity theft survey. Secretaries of state, obviously, are uniquely positioned to solve the problem of business identity theft. But the NASS found that 83 percent of its respondents are not tracking business identity theft complaints.

In response, the NASS recommends that SoS offices track the crime, offer clear remedies for fraudulent filings and take the lead on state discussions on the issue.

That alone should tell you where the government is on this issue. But it gets worse.

Law enforcement is equally uninterested in this crime. That's why Company Alarm invited Agent Gagliardi to become an advisor – because there are very few law enforcement officers who actually know and care about this crime.

As he will tell you, his unit in Colorado frequently finds evidence of business identity theft in other jurisdictions. But when they call to inform the authorities there, often they're met with indifference.

Oftentimes, he says, authorities don't understand the significance of business identity theft, or don't know how to investigate the cases. And since this crime isn't tracked anywhere and since it's not a priority for anyone else in power, they have little incentive to learn more.

It's a vicious cycle of inertia, and, for the moment, there isn't much prospect for change.

In 2018, after The *Las Vegas Review-Journal* wrote about our founder's experience with identity theft, Nelson Araujo, a Democrat running for Nevada Secretary of State expressed interest in reforming the system in the Silver State. (Nelson even printed a campaign mailer with Andy, explaining what happened to him.)

But in November of that year he lost to the incumbent Republican, Barbara Cegavske, who has insisted business identity theft isn't much of a problem.

As far as we're aware, business identity theft isn't a major topic of discussion at any state capital these days. Likewise, there's little or no momentum in law enforcement circles on the issue.

In government, there's just people like Agent Gagliardi, toiling in relative anonymity, trying to get someone, anyone, to listen.

Support for businesses

Given that business identity theft isn't well known it should be no surprise that there are few service offerings in this area.

Sure, there are personal identity theft protection companies that dabble in protecting businesses. They might offer educational information on their websites or services to protect a business's employees from identity theft or help in the instance of a data breach.

But these offerings do not get to the heart of business identity theft. In fact, a data breach is not business identity theft at all. That is the theft of information from your business. It's not the impersonation of your business.

That's a big difference. And by conflating the two, it just makes it more difficult to bring attention to the scourge of business identity theft.

So, where does this leave us?

From where we sit, Company Alarm is the only dedicated service devoted to addressing -- and preventing -- true business identity theft in the United States today. Our service gives you the earliest possible warning that your venture could be under attack from cybercriminals -- and our warnings, if heeded, are early enough that business owners can nip any criminal mischief in the bud before it's become a costly problem. As we often say at Company Alarm, cybercriminals need time to pull off their schemes. With Company Alarm monitoring, you know immediately if you're under attack, giving you ample time to stop the bad guys in their tracks.

Company Alarm also is the only institution focused on developing educational materials solely on the topic. We have as an advisor one of the only bona fide leaders on business identity theft in American law enforcement.

When it comes to business identity theft protection, as far as we can tell there's Company Alarm and not much else.

So, our goal for the year is simply this: To raise the profile of this issue. To educate the public on the threat of business identity theft. To entice policymakers and politicians to take this issue seriously.

And, of course, to protect businesspeople like you.

Data breach protection or an identity theft program for your employees is not going to help you when cybercriminals log onto your local secretary of state website, remove you as the managing member of your company and hijack it for their own enrichment.

The only thing that's going to help you is immediate notification that the hijacking has occurred. And the only service that offers such an alert is Company Alarm.

Using our proprietary technology, Company Alarm monitors your business filings at the state level continuously, seven days a week. The moment anything is changed with your filing – the listed address of your office, the names of your board of directors or managing members – you receive a text message alerting you to the specific change.

Yes, some secretaries of state will send you a notification when information like this is changed. But as our founder learned, these e-mails are typically vague, saying only that a new filing has been made for your business. For a busy businessperson, that's meaningless. It gets lost in the shuffle of the million e-mails you receive daily.

But a text message delivered right to your phone saying specifically that your business address has been changed? That your company has a new managing member? That should set off alarm bells.

And that's ultimately our goal: To prevent other businesspeople from going through what our founder Andy has experienced.

He first realized that he was a victim of business identity theft in March 2017. He's been locked in a court battle ever since, trying to regain control of an$5 million piece of land in Las Vegas that was stolen out from under his nose by business identity thieves.

So far, he's spent more than $350,000 in legal fees trying to regain the land he and a group of investors had owned free and clear for more than a decade.

In 2020, in this decade, you don't want to go through that.

Investigate Company Alarm's services. Read our educational material. You'll find that we're the only ones right now who can help protect you from business identity theft.

COMPANY ALARM®

4805 N. Locust Grove Rd.
Meridian, ID 83646

800.488.2909

companyalarm.com