Business Identity Theft Schemes

companyalarm.com

Table of Contents

What Are The Most Common Business Identity Theft Schemes and How to Protect Your Company From them

Identity thieves don't just target people – they prey on businesses, too. Their schemes vary widely, from the unimaginably complex to the absurdly simple. But in every case, their effects can be devastating to the business involved and its personnel.

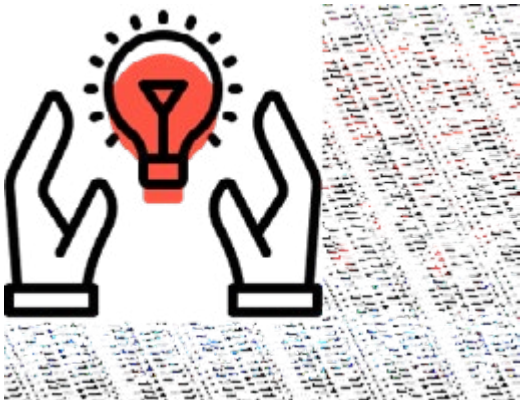
Business identity theft is when criminals hijack a business's name to plunder its assets, credit and/or reputation. The crime comes in a variety of forms, from scammers merely impersonating a business to fraudsters filing fraudulent paperwork to take over a company. However it's done, the goal is always the same: To exploit the business for the criminal's financial gain. That can mean purchasing luxury cars or dozens of cell phones on company credit and selling them for a quick profit. It can mean seizing company assets, like a piece of property stashed in a holding company, and transferring it to another business entity, where it's sold to an unsuspecting third party. Or it can be masquerading as your business to exploit your good reputation and defrauding your current or potential customers.

At worst, business identity theft can bankrupt a company. But even if you somehow survive the blow financially, it can leave you battling creditors or tied up in court or repairing your reputation – for years. The impact, therefore, isn't just to your bottom line. It's to your physical and mental health, and the health of your staff members as well. Years after one of his businesses was hijacked, Company Alarm founder Andy Pham is still fighting to regain his business assets, and he's still paying attorney's fees, too. Entrepreneurs start businesses so they can get a piece of the American dream. But business identity theft can turn that dream into a nightmare.

Identity theft is a growing problem facing American businesses big and small. In fact, it's arguably one of the biggest problems facing businesses today – but virtually no one knows about it. The Internal Revenue Service reported a 2,757 percent increase in fraudulent business returns 2015 to 2017. Dun & Bradstreet reported a 46 percent increase in business identity theft cases in 2017.

Here are the most common ways thieves steal a business's identity and tips for how to respond if you become a victim.

- Hijacking a Business through Fraudulent Filings with the Secretary of State
- Impersonating a Business with a Fake Website
- Imitating an Existing Business by Obtaining a Similar Mailing Address
- Masquerading as a Business by Using a Federal Employer Identification Number



Hijacking a Business through Fraudulent Filings with the Secretary of State.

Most secretaries of state lack the legal authority to verify the accuracy of the business filings they receive. That means in most states if you know a little bit about a company – say, its name and its ID number – and are willing to pay a nominal fee, you're free to file anything you'd like about that company. As long as the filing is filled out correctly, your filing at the local Secretary of State will mark it as an official document.

This loophole in America's business registration system has existed for decades. But for the vast majority of our country's history, it didn't pose much of a problem. That's because filing business records used to take a lot of effort. You'd have to track down the proper forms and submit the filings by mail or drive to your state capital and deliver the paperwork in person.

All that changed with the emergence of the Internet. Now, with just a few mouse clicks, you can not only file business records online, you also can look up information on every business in a given state. Typically, secretaries of state websites include online disclaimers that require filers to affirm they have authorization to make changes to the business or else face a criminal charge of perjury. But these warnings are easily, and often, ignored. In short, secretaries of state, who champion ways to streamline business filings for legitimate purposes with user friendly access via the web, have in turn made it incredibly easy for criminals to hijack businesses as well.

Here's how it works: Identity thieves research a targeted business online, using the Secretary of State's website and possibly a search engine or two. Then, the thieves change the business records with the Secretary of State. This new record typically will change the business's official address and/or the business's managing member. Within minutes, the Secretary of State accepts the new filing and, poof, the thieves now have an official, government document stating that he or she owns your business, which is now located at an address the thieves control.

When identity thieves employ this scheme, they're counting on the legitimate owners of the business not to notice that their information has been changed with the government. That's why Company Alarm's 24-hour monitoring is so crucial: It lets you know immediately when your business has been hijacked. I've seen business owners go weeks or even months before they discover their company has been stolen. By then, identity thieves have had plenty of time to do lasting damage to your business. Company Alarm prevents that from happening.

Active versus Inactive Businesses

Because identity thieves want to work in the shadows, they often target not only active companies, but inactive ones – companies that the Secretary of State may have labelled delinquent or dissolved. Thieves like inactive businesses because they assume the rightful owners are not paying attention.

But inactive companies often have a secondary benefit as well. Many inactive companies have been inactive for years, which in the language of registered agents makes them "aged." Some legitimate entrepreneurs like to purchase businesses that have been in existence for a while so they can immediately qualify for credit.

That makes inactive businesses perfect candidates for thieves to sell to unsuspecting businesspeople. Thieves will troll the Secretary of State's website, looking for inactive businesses. They'll file the necessary paperwork and pay the fees to reactivate the companies, naming themselves the owner. Then they'll sell the companies to the entrepreneurs for a tidy profit. It's a simple scam that often goes undetected.

What Thieves Can Do With a Hijacked Business

Once criminals have taken control of your company, they have a lot of options for what they can do.

1. They can exploit the company's assets and credit for immediate cash.

Under this scenario, scammers typically purchase or lease hard goods like luxury vehicles, cell phones, computers or commercial copiers, through credit they've obtained using your company's identity. Then they turn around and sell the goods to unsuspecting buyers and disappear with the money. Or they might obtain a business loan and run off with the cash.

Sometimes, thieves also can sell off the company's physical assets. That's what happened to Company Alarm's founder, Andy Pham. Andy and a group of investors held a $5 million piece of land in a holding company. Someone logged into the Secretary of State's website and removed Andy as the managing member of the holding company. Then, the land was moved into a second holding company, where loans were taken out on it and later it was advertised for sale.

2. They can open new bank accounts in your company's name.

In this case, the scammer is looking to establish a bank account in the name of a legitimate business. Such accounts frequently are used to launder funds from illegal activities, including other fraud such as credit card or personal identity theft schemes.

3. They can use your business's identity to defraud other people.

Criminals love the cover of a legitimate business with a good reputation to defraud consumers. There's no end to the kinds of scams they can run on other people by using your business.

One common scam is thieves will hijack some kind of real estate company and then use that cover to offer to purchase timeshares from individuals. The scam is that criminals will ask the timeshare owners to pay them a couple thousand dollars to get the sale moving. The criminals pocket the cash and the timeshare owner is left without little recourse.

In this case, the legitimate owners of the real estate company aren't out any money. But their reputation is destroyed – especially if consumers have filed complaints about them. That is one of the biggest dangers of this kind of scheme, the reputation loss to your company.

What To Do If You Discover Your Business Has Been Hijacked

Immediately file a report with your local police as well as the Federal Trade Commission and the FBI at www.IC3.gov. Unfortunately, many law enforcement and/or government agencies aren't familiar with business identity theft. They either don't recognize it and/or know how to pursue a criminal investigation.

But that shouldn't stop you from filing such reports, which is a critical step and needed to have on hand in case creditors show up at your doorstep looking to collect from purchases made by your identity thieves.

You'll also want to contact your local Secretary of State, to not only get yourself reinstated as the official owner of the company, but also to flag your company as having been a victim of identity theft. Again, the level of awareness of this issue varies from jurisdiction to jurisdiction, but you want to notify as many officials as you can about your problem and find someone who can help.

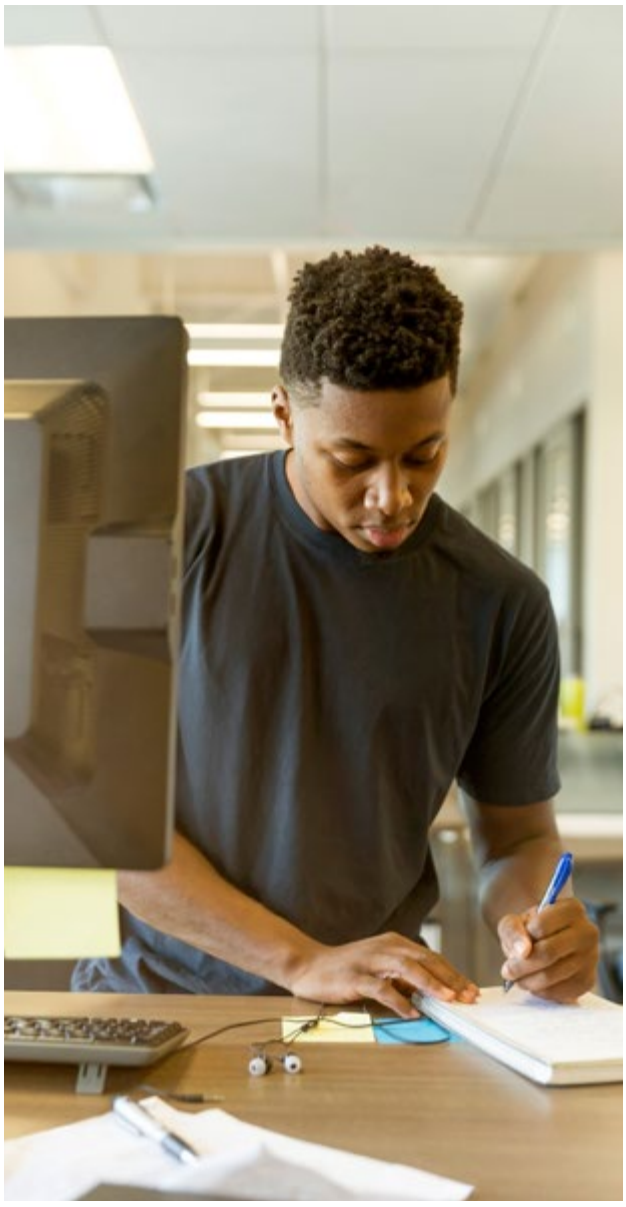
Impersonating a Business with a Fake Website.

Another kind of business identity theft is when scammers create a fake website for your business. These fake sites can take on many different forms. Sometimes, criminals will try to make their fake site look like your real one. Other times they create a whole new website – especially if the targeted company doesn't have one at all.

In these cases, criminals may not have actually seized control over your company. They're merely impersonating it, on the web. But that still can have some pretty disastrous consequences for your business.

What Thieves Can Do With a Fake Website

Fraudsters who impersonate legitimate businesses on the web typically have one of two goals:



1. They want to defraud other people.

They use your company's good name to attract customers and then rip them off, either by taking their money and not giving them services, or by collecting their personal information, which they use to commit more crimes or sell for cash.

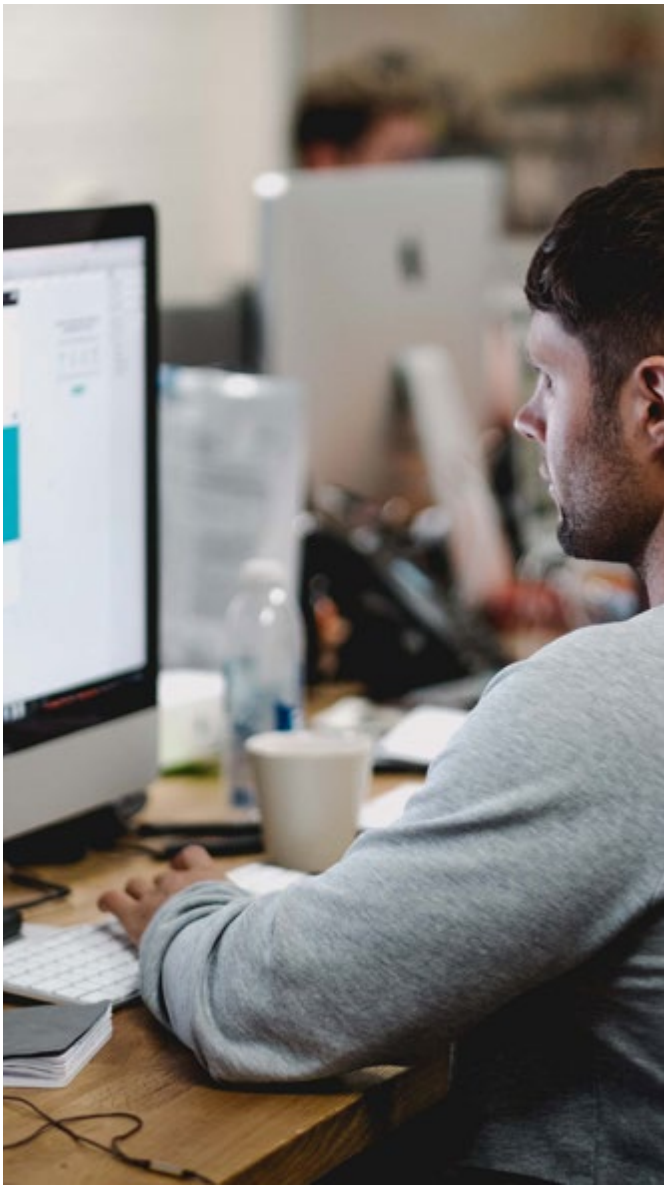
2. They want to take out credit or loans in your business's name.

Believe it or not, some lenders due diligence is very shallow when it comes to vetting candidates for business loans or lines of credit. Some will just ask to see the company's website. Identity thieves give the lender the fake URL and, wham, they're granted credit.

But when the bill comes due, they won't be on the hook. Your business will be.

What To Do If You Find A Fake Website About Your Business

Your goal here is to contact the web hosting service overseeing the fake website and getting them to take it down. You might be able to make that happen by contacting your local police – but, remember, not all law enforcement officers understand this issue or have the resources to assist.



There's a chance you might have to contact the web hosting service on your own, or hire a lawyer to do it.

Imitating an Existing Business by Obtaining a Similar Mailing Address.

Another way identity thieves will impersonate a business is by obtaining a physical or mailing address that is very similar to a legitimate company's. Sometimes, they'll even set up an office in the same office complex as the target business.

Then, using the address, the thieves will start to operate as though they are that business. This scheme is known as "mirroring" an address.

What Thieves Can Do With a Similar Business Address

Scammers who employ this scheme are looking to exploit the sloppy review processes of lenders. They hope to obtain business loans or purchase physical goods on credit.

Then they walk off with the cash or sell the products for money and disappear, leaving your business holding the bag.

What To Do If You Learn Your Business Address has been 'Mirrored'

This is a tougher situation to address, because your only real course of action is to enlist the help of the local police, and, as we've discussed, not every law enforcement officer understands the gravity of business identity theft. But it's worth a shot and, again, it gets you a case number if you need it down the road.

Another step you can take is to make sure your physical and mailing address is up-to-date and matches what you have with your your local Secretary of State. But that obviously won't stop the fraudsters from impersonating with you a similar address.

Masquerading as a Business by Using a Federal Employer Identification Number.

The last major business identity theft scheme involves federal Employer Identification Numbers. Some identity thieves like to steal the existing EINs of legitimate businesses. Others prefer to apply for a new EIN using an existing business's information.

Which every path they choose, criminals in the end obtain a critical piece of business information, which they then use to line their pockets.

What Thieves Can Do With an EIN

The primary scam identity thieves use with EINs is filing fraudulent tax returns. From 2015 to 2017, the Internal Revenue Service reported a 2,757 percent increase in the number of fraudulent tax returns involving business identity theft. The dollar amounts involved topped $120 million each year.

In those instances, identity thieves file fake returns in order to secure an illicit refund from the government.

Thieves also can use EINs to secure loans or credit – but, typically, the EINs are used in conjunction with another scheme listed above, like hijacking a company.

What To Do If You Discover Thieves are Using an EIN tied to Your Business

In this case, your solution is simple: Contact the IRS. They know about business identity theft and will listen carefully to your complaint.

In closing, it's important to realize that identity thieves often don't stick to just one scheme when they target a business. They can hijack a business through the Secretary of State and set up a fake website and obtain a new EIN, all in an effort to secure a loan or a line of credit.

As business owners, it's important that you watch out for all of these forms of business identity theft. Your business, whether big or small, is vulnerable to all of these schemes, just by virtue of being in business.

But Company Alarm can help. With our 24-hour monitoring, you can be confident that your information on file with your local Secretary of State is being watched. And with our educational materials, like this one, you can learn more about business identity theft and how to protect yourself.

COMPANY ALARM®

We help business people protect their company and preserve their American dream by monitoring their business data and alerting them of any changes in real time, so they can focus on growing their business instead of worrying about losing their assets or reputation, or worse.

4805 N. Locust Grove Rd.
Meridian, ID 83646

800.488.2909

companyalarm.com