
# How to Prevent Business Identity Theft

Here are the best ways to protect your business

companyalarm.com

Ralph Gagliardi, the leader of one of the nation's only law enforcement units dedicated to fighting business identity theft, calls the crime one of the biggest dangers facing American companies today. But, frustratingly, identity theft of any kind is incredibly difficult to prevent.

That's because identity thieves make their mischief by using information that is largely in the public sphere. The tools they use for their crimes are, generally speaking, easily available for the world to see, through government websites that publish business information, like the Nevada Secretary of State's business portal, SilverFlume.

That leaves concerned business owners with effectively only two options: Prevent the disclosure of any information about their enterprise or be incredibly mindful about everything they do in relation to their business, even the most mundane and seemingly unimportant tasks.

The first approach can be achieved, but at a significant cost to your business and, even then, it's not a realistic option for many, if not most, enterprises. The latter strategy may be more universally achievable, but it still, nonetheless, requires a great deal of work, both by the business owner and his or her staff.

Here are the best ways business owners can protect their enterprises from identity theft:

- Structure your enterprise as a business trust
- Closely monitor the correspondence you receive
- Watch the documents you throw away
- Protect your sensitive business information

## Structure your enterprise as a business trust

The only way you can completely prevent any critical information about your business being published on a government website like the Nevada Secretary of State's online business portal SilverFlume is to structure your business not as an LLC or an S-Corp or a C-Corp, but as a business trust.

That's because when you structure your business as a business trust, information about your business's officers and its address are not published on government websites like SilverFlume. That is the great advantage of business trusts. When you structure your company in this manner, limited information about your enterprise is revealed through the official incorporation process.

In effect, when you structure your company as a business trust, fundamental information about your enterprise is hidden behind a legal wall.  And if your business's information is not published on an official, government website, that makes it extremely difficult for identity thieves to hijack your business. (Extremely difficult, but not impossible. As we will discuss below, there are other places where identity thieves still can get critical information about your business besides the Internet.)

But business trusts are not for every business. They may not be for most businesses, in fact.

That's because business trusts don't offer nearly the kind of tax and other structural benefits offers by more traditional business structures, such a LLCs, S-Corps and C-Corps. Indeed, while business trusts are a comprehensive (but not complete) shield against business identity theft, they can end up costing businesses in other ways. Depending on the nature of your business and your personal finances, it's possible – perhaps even likely – that a business trust structure, despite its obvious security benefits, won't work for you now, or ever.

In that likely scenario, you're stuck leaving your business information exposed to the public, as the vast majority of businesses do across the United States. In that case, the only other strategy you can employ to protect your business from identity theft is to be extremely mindful about virtually every action you take in regards to your business.

The rest of this article is dedicated to explaining how, exactly, you need to be careful.

## Closely monitor the correspondence you receive

If your critical business information has to be published on a government website, you need to be vigilant and watch out for signs that your information has been stolen and used to impersonate your business. Signing up for a subscription to Company Alarm is an excellent first step, as Company Alarm offers 24-hour monitoring of your business's information on file with the local government.

In the event any of the information about your business is changed – say your business's mailing address or the names of its board of directors – you'll receive an immediate text message notifying you, if you've signed up for Company Alarm, of course. That text message can serve as your first – and earliest – warning that your company may be under attack by identity thieves.

But Company Alarm texts aren't the only clues you could receive. As we've explained many times on this website, identity thieves typically impersonate a business in order to obtain cash or goods from third parties by exploiting the business's assets or reputation. For example, an identity thief impersonating a business may try to secure an illicit business loan in the name of the business. The criminal, securing the loan, has no intention of repaying it and disappears with the money.

Or, perhaps, the identity thief will impersonate a business in order to purchase dozens of cell phones on credit. The criminal uses hijacked company's good credit rating to make the purchases, then re-sells the cell phones on the black market. Once again, the criminal has no intention of paying off the purchases, leaving the true business owner left holding the bag.

These kind of actions often generate correspondence from the third parties involved. In the instance where an identity thief takes out an unauthorized loan for your business, your business might receive a letter directly from lender, outlining the terms of the loan. Letters like this can easily get lost in the shuffle of a busy business, especially if the sender is unfamiliar. But in order to protect yourself from identity theft, you need to pay extra attention to the correspondence you receive from unfamiliar sources or about unfamiliar circumstances.

While it may be human nature to caulk up an letter from an unfamiliar source, talking about an unfamiliar loan, as a mistake and just move on with your life, that's the absolute last thing you want to do. Any letter or e-mail like this – or any correspondence welcoming you to a new, unfamiliar financing program, or thanking you for purchase you didn't make – should immediately set urgent alarm bells in your head, as well as heads of your staff members.

You see, when it comes to the close monitoring of your business correspondence, it's also critical that you educate your employees what to look for. In most enterprises, not just one person is responsible for going through the mail. Thus, everyone on your team needs to understand the importance of looking out for unexpected letters and e-mails. Besides a text alert from Company Alarm, correspondence of this nature is going to be your best warning of possible business identity theft.

## Watch the documents you throw away

Identity thieves, particularly those targeting businesses, generally and most commonly use the web to track down information about their target businesses. But that's not the only source of information they plumb.

Identity thieves of all stripes are notorious for dumpster diving. That means you have to be extremely careful about the documents you throw away. The garbage can of a careless business can include more critical and vulnerable information than anything found on an official government website.

The bottom line when it comes to throwing away documents is this: If you have any concern at all that a piece of paper includes information that an identity thief could use to compromise your business, shred it. It's really that simple. If you have any doubts about a document, make it completely unreadable.

Once again, because sensitive documents and information often pass through multiple hands at a business, and because everyone is throwing things away, you'll want to thoroughly educate all of your staff members on the importance of watching what goes into the garbage.

One easy thing you can do to make shredding more widespread at your business is to simply make cheap shredders easily accessible to everyone who works there. That can mean buying three $40 shredders from Amazon, instead of one, and spreading them throughout your office.

Generally speaking – and there is no hard-and-fast rule for this – you'll want to shred any document that includes your business's address; business IDs, including your federal Employer Identification Number and your filing number with your local state government; and the names of your board of directors, managing members and registered agents.

Any of these seemingly benign facts can be used in campaign to hijack your business. You want to make it extremely difficult for identity thieves to find them.

## Protect your sensitive business information

Keep in mind that the sensitive information we just discussed doesn't only appear in your trash. It can also show up on documents you leave lying around your office, or on files you keep on your hard drive, or in your e-mail. You'll want to protect those documents, too.

It may sound strange, but critical pieces of information about your business should be handed out sparingly – even to internal employees. Say you're the owner of a business and one of your staff members needs your business EIN to complete a form. Your initial reaction probably would be to e-mail the number and move on with your day. But that's not what you want to do.

A safer approach would be to walk over to your employee's desk and read the EIN to him or her. Don't create a digital or physical paper trail of this key piece of information, which an identity thief can use to file a fraudulent tax return in your business's name.

The same goes with the names of your board of directors or managing members or registered agents or office addresses or any foundation piece of information about your business. When at all possible, avoid putting that information down on a physical piece of paper or in a digital document.

If circumstances make that impossible, see to it yourself that the resulting paperwork is destroyed. Or, if the paper trail is digital, make it password protected.

That's right: To try to protect your business, consider password protecting the basic information about it, including your board of directors and your EIN.

That might sound like a lot of nonsense. It certainly creates a lot of extra work. But identity thieves can only operate if they somehow get access to your information.

If you're being extremely careful about what appears in your trash, you'll also want to be careful about where that same information lives within your business.

Remember identity thieves can come from all walks of life. They may even work for the company you pay to clean your office.

Preventing business identity theft is, at best, difficult. Thieves can hijack your business with just a handful of critical pieces of information about your enterprise – information that's often in the public sphere, if you know where to look. And you better believe thieves know exactly where to look.

The only way you can fight back is to limit the exposure of your business information. The most comprehensive approach, although nowhere 100 percent effective, is to shield your company's information behind the legal wall of a business trust. But that's not a viable option for every concern – or probably even most businesses.

That leaves your best tool as simple mindfulness. To prevent your business from becoming the next victim of identity theft, you need to be extremely careful about how much you expose your critical business information, and you and your staff need to keep an eye out for any unfamiliar or unexpected correspondence from banks or lending institutions.

The good news is that other than a subscription to Company Alarm, which costs less than a couple cups of coffee a month, this strategy doesn't carry a high price tag. It just requires vigilance. In our go-go business world of today, that's hard to maintain. But that's exactly what the identity thieves are counting on.

Don't let them win. Establish rigorous practices to prevent the exposure of your internal information and to carefully sift through the information streaming into your business. You'll be safer and better off if you do.

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