Small Business Identity Theft is Big Business for Fraudsters

How to Keep Your Business, Employees, and Customers Safe from Cybercrime
As a small business owner, you’ve taken important steps to secure your dream. You’ve come up with an idea for a promising business opportunity. You’ve researched your industry and market, completed your business plan, secured your financing, and created a company name and brand. Now your goal is to expand into a profitable and sustainable business, hire employees, and become a true entrepreneur in your space.

You’ve worked hard, and you don’t want a fraudster to destroy all that you’ve built. How much could be at stake? A median loss of $200,000 per fraudulent scheme impacts small business enterprises (SMBs) globally (that is, those with fewer than 100 employees) — nearly twice that of large enterprises, according to the Association of Certified Fraud Examiners.¹

Business identity theft occurs when a criminal impersonates a business and uses the information for personal or financial gain, to open new accounts, or commit crimes using stolen identities.

Identity theft and fraud can leave your business and reputation in shambles, disrupt your income stream, and seriously complicate your life.

It’s not just about protecting your key business assets and intellectual property, it’s also about securing your documents, networks, accounts, and sensitive customer and employee information.

This whitepaper examines the growing risk to SMBs from identity theft, the growing range of sophisticated threats facing companies, and how organizations can mitigate the threat of devastating losses with comprehensive business identity theft protection.

¹ ACFE, Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse.
Small businesses need to protect not only their identity, as they have intermingled consumer and business information, but also their customers’ data. Letting this information fall into the wrong hands can be catastrophic in terms of critical data loss, disruption to operations, financial losses stemming from restoring systems and files, and, of course, damage to the company’s reputation.

Guarding against cyberattacks and fraud is no easy feat, given that cyber threats can come from external as well as internal sources. SMBs typically lack appropriate technical resources, processes, or infrastructure to mitigate cyber risks, vulnerabilities, and attacks, and are rarely able to allocate a sufficient budget to counteract the threats.

Why do cybercriminals target small businesses?

1. They are very lucrative targets | Even if SMBs don’t have the resources or data that’s comparable to large enterprises, they do hold valuable data and potential connections to larger organizations. Fraudsters target SMB data to gain access to other organizations, such as through unprotected connections within a supply chain. Recall that the Target data breach of 2013 was instigated through a small HVAC company.

2. They have valuable customer data | When a fraudster pounces on a small business, they can get access to Personally Identifiable Information (PII), which can lead to identity theft and devastating financial damage.

3. They are more vulnerable | SMBs face the same threats as large enterprises, but few have the infrastructure sufficient to protect their assets. They also often lack the necessary time, money, and expertise to detect and repel threats.
The FBI has been tracking email financial scams since 2013. Since then, organized crime groups have targeted small companies, including organizations in every U.S. state, and more than 100 countries around the world — from regular businesses to nonprofits, churches, and school systems. BEC/EAC scams comprise a growing and evolving illicit global scheme that targets businesses of all sizes.² The scale and methods used in BEC/EAC wire-transfer fraud are eye-opening:

- **Domestic and international incidents**: 78,617
- **Domestic and international dollar loss**: $12,536,948,299
- **Business executive scam**: Fraudsters will use your email address to contact an employee responsible for your company’s finances, requesting a large wire transfer into a fake account.
- **Supplier swindle scam**: Thieves target your company’s foreign suppliers or overseas vendors, hoping to authorize wire transfers to a fake account.
- **Bogus invoice scam**: Bad actors approach your customers or third-party vendors, hoping to collect money through false invoice requests.
- **Personal data scam**: Fraudsters focus on stealing employee’s PII, most commonly targeting your human resources’ email accounts to obtain W-2 information.

2. Ransomware

A malicious lockdown of your data can threaten both your business’ security apparatus and most valuable company assets. Hackers gain access to your networks, compromise sensitive business data, and then hold those files or data for ransom. Until you pay the ransom, usually through virtually untraceable cryptocurrencies, your infected devices are rendered essentially useless. Also bear in mind that not all criminals follow through on promises to restore your data; they are crooks, after all. The volume of ransomware attacks has increased significantly over the past two years. Between October 2017 and 2018, for example, there were 286 million worldwide ransomware attacks, up 117 percent from 132 million attempted attacks one year before.  

3. Cybercrime

Protecting your organization against cybercrime is more critical than ever in the event of rising threats. In February 2018, the U.S. Director of National Intelligence ranked cyberattacks as the top security threat in the country. As technology advances, cybercrime tactics used to steal your most sensitive “crown jewels” — employee records, intellectual property, or customer data — likely will advance as well.

One in five SMBs who paid the ransom never got their data back

SOURCE | 2016 AO Kaspersky Lab. All Rights Reserved.

---

The top four cyber threats facing SMBs include data breaches, malware, network vulnerabilities, and mobile devices. The growing frequency and complexity of cybercrime make it necessary for SMBs to increase their vigilance exponentially:

**Data Breaches** | Often reported in the news, data breaches are incidents in which a person's individual name plus a Social Security number, driver's license number, medical record, or financial record (credit/debit card) are potentially put at risk because of electronic or paper-record exposure.

**Malware** | As noted earlier, malware is most often introduced to a company's secure network via phishing emails sent to employees. According to Verizon, 92.4 percent of malware is delivered via email\(^4\) and 88 percent of malicious emails use malware-laden attachments to capture their prey. Perhaps an even more concerning statistic is that each user at a business with less than 250 employees gets, on average, nine malicious emails per month.\(^5\)

**Network Vulnerabilities** | Unauthorized access to your network via a security flaw can be especially damaging. Hackers take advantage of security weaknesses within your software because they serve as back doors into your network. Every time a user opens a program on the operating system without restrictions or limited access, the user potentially invites attackers to cross over and rewrite the codes that keep information protected. According to the Cloud Service Alliance, 75 percent of all cyberattacks target known vulnerabilities. Furthermore, 90 percent of small business don’t use any data protection at all for company and customer information. And almost two-thirds of all cyberattacks are now directed at small businesses.\(^6\)


It should be clear by now that no business is fully safe from a cyberattack. However, there is cause for optimism. By assessing your company’s cybersecurity risk, improving overall security behavior, and ensuring that you are using the right solutions for your business, it’s possible to protect your company from most data breaches.

Mobile Devices | While mobile devices are meant to improve efficiency, criminals can also exploit unsecured laptops and smartphones to gain entry into your business. Many businesses allow employees to connect their personal devices to the corporate network — known as Bring Your Own Device (BYOD). However, personal devices can pose a threat to your company’s cybersecurity since over 75 percent of employees do not secure their computers.

Criminals also target corporate cloud services because of the large pools of data they can hold. Even though many of today’s cloud services offer sufficient security measures to prevent hackers from accessing sensitive business data, initial misconfiguration or misuse by the user of these services can lead to vulnerabilities in the services’ defensive features.

Finally, any device that is connected to the internet can be hacked. For example, DVRs, printers, and Smart TVs (known as the Internet of Things (IoT) devices) can help hackers gain access to your business’ network through unsecured Wi-Fi networks. If successfully hacked, criminals can compromise these devices and turn them into “bots” that can be used to unwittingly target other victims as part of future attacks.

Payroll outsourcing company Paychex cites that over 70% of cyberattacks specifically target SMBs.
In the years we have been working with small business owners on preventing identity theft, we have developed three profiles of a small business owner:

1. The Disbelievers & DIYs  
First are owners who believe fraud or business identity theft never will happen to them. Or if it did, they would be able to deal with the theft on their own without the assistance of a provider (known as Do-It-Yourselfers (DIYs)). In general, we find that these owners may lack a full understanding of the steps and time it takes to detect, remediate, and resolve an identity crime.

2. The Believers  
The second are small business owners who are too busy to deal with the hassles of guarding against identity theft and recognize the benefit of a service that will aid them in the event of a data breach, fraud, or business identity theft. These owners understand that the business identity theft protection provider can save them time, so they can focus on running their businesses.

3. The Educated Planners  
Finally, there are those company leaders who are already confident about the steps they need to take if a cyber event occurs. However, they may still need guidance on best practices and prevention tips to protect against a data breach or identity theft incident. This will ultimately help them alleviate or remediate both known and unknown risks and vulnerabilities.
EZShield delivers mission-critical services that empower you to run your business effectively, while making it easy to deliver essential identity and business protection. We are the trusted provider for your business, and for your employees.

As part of EZShield’s Small Business Suite, we include the following identity theft protection and mobile cybersecurity services:

**Business Credit Monitoring, Score, & Report** | This includes features like Business Credit Score, Business Credit Report, and Business Credit Monitoring so that you can confidently manage your business credit. As a result, you’re able to focus more of your time and attention on building capital, expanding your customer base, and creating customers for life.

**Business Dark Web Monitoring** | The Dark Web, a part of the internet that isn't visible to mainstream search engines, contains thousands of illegal websites that criminals use to buy and sell stolen business information. Business Dark Web Monitoring will let you know if your Personally Identifiable Information (PII) or sensitive business data is on the Dark Web. For example, your Employer Identification Number (EIN), domain, D-U-N-S Number, and corporate credit card number, will be continuously monitored. Additionally, EZShield will provide a one-time scan that will begin looking for the information you provide during enrollment throughout thousands of Dark Web chatrooms.
Mobile Defense Suite | As part of EZShield’s Small Business Suite, you’ll gain access to innovative mobile cybersecurity capabilities:

- **Mobile Attack Control**, which includes access to EZShield’s award-winning mobile app, performs comprehensive mobile device scanning and alerts your employees if their device has been compromised. It looks for a wide array of threats including rogue apps, spyware, unsecured Wi-Fi connections, and even recognizes fake or “spoof” networks.

- **Mobile Attack View** delivers a single-source view for your internal team, showing any mobile threats from devices that are connected to your system. This ability to recognize vulnerabilities in real-time gives technology leaders the advantage of stepping in to take action before a data breach occurs.

Fully-Managed Business Restoration | It’s critical to protect your business’ valuable assets from misuse or fraud. This exclusive service includes proactive capabilities and a white-glove response program, featuring access to dedicated resolution experts, to keep your business identity safe.

Data Breach Program | If you are a small business that has experienced a data breach, EZShield offers a tailored package at a special rate.
You've worked hard to build your business and you don't want a single fraudster — or worse, a network of organized criminals — to destroy all the value and goodwill you've created. Here are six steps you can take to help protect your business against continuously evolving, and increasingly sophisticated cyber threats.

1. **Develop and implement a company-wide security awareness program |** Make it everyone’s priority to protect company information for the benefit of your employees, your customers, and the long-term health of your business.

2. **Prohibit employees from using their work email as their personal email |** Company time and property should only be used for company work. If your employees are using their email for personal use, you are unable to control and safeguard emails that may contain sensitive client information.

3. **Store business documents, account numbers, and other sensitive documents in a secure place |** Use an offsite source or third-party service to back up your files or data, making them less susceptible to ransomware.
4. Avoid co-mingling your personal and business accounts |
Allowing employees to use personal passwords for business accounts (and vice versa) adds more risk that sensitive business account information could be compromised when someone’s login credentials are hacked.

- Use complex passwords that are a mix of letters, numbers, symbols, and non-dictionary words, along with a password manager to store and track them.
- Ensure you are using anti-malware software and regularly updating the latest security patches.

5. Never use public Wi-Fi | Especially when accessing customer or employee information. Unsecured public networks or hotspots — now broadly available in airports, hotels, cafés, and so forth — can allow hackers to position themselves between the users of unsecured devices and the connection spot. Hackers thus have access to every bit of information the user is sending out on the internet, such as sensitive emails, credit card information, and even security credentials.

6. Get Business Identity Protection | Small business owners may not realize how negative an impact identity theft can have on their businesses and employees. Lost productivity from distracted workers, potential breaches of valuable data from personal devices tied to company networks, and the mental drain resulting from the theft of PII all have quantifiable costs. EZShield’s extensive suite of business protection services caters to small business owners and includes secure online storage, live support, timely small-business education, and advanced monitoring of sensitive data.

Visit BusinessIDTheft.org
Learn more about prevention and the assistance available, while protecting your company from business identity theft
When the Unthinkable Happens: EZShield’s End2End Defense® Restoration Service

No one can entirely prevent identity theft — one can only detect anomalous events and alert the business that something potentially suspicious may be happening with their company information. At that point, steps can be taken to further stop an additional whirlwind of malicious activities.

Our End2End Defense® identity restoration service is built on the premise that, in fixing the aftermath of identity theft, our customers deserve to work with real people, not navigate a recorded phone tree. We are always here to help you put your business back on track in the event of an identity crime.

End2End Defense® follows an extensive and proven process to resolve fraud, which involves discovery, mitigation, and protection. Our goal is to ensure that fraud incidents are resolved and that all possible mitigation actions have been taken to protect against future threats. Other benefits of the service include:

- An in-house, U.S.-based customer support team available from 8 AM – 8 PM ET (M-F)
- Multilingual representatives who speak English, Spanish, and French
- A dedicated Resolution Specialist assigned to each case
- Industry memberships and key certifications maintained annually
- An average tenure for our team of seven years
- Limited power of attorney for fully managed restoration services
Cybercrime is the biggest threat facing consumers and businesses today, and the time to act is now. But when it comes to protecting your business from identity theft, it does not pay to take shortcuts. EZShield’s Small Business Protection allows you to focus on what matters most: your company’s long-term survival and success. Call or click today!
Mobile Defense Suite

Our Mobile App Recognized by BankNews for Excellence in: Authentication | Fraud Protection | Cybersecurity

Learn More