



Business Identity Theft

- New and rapidly spreading type of ID theft
- Criminals hijack a legit business identity
- Criminals open accounts/steal using the legit business ID, often going unnoticed
- The victimized business is left holding the debts and credit damages from the crime

Use of Business Records

- Criminals looking to gain access to online business records
- Attempting to exploit state business registration websites
- Thieves altering data to open accounts

Impact of Business Identity Theft

- Tarnished business credit history
- Difficulty obtaining future credit
- Costly and time consuming to fix

State and National Efforts

- Outreach to the business community, particularly small and medium-sized entities
- Information-sharing between the States
- Establishment of National Association of Secretaries of State Identity Theft Task Force

What is Business Identity Theft?

Business identity theft is a relatively new type of crime that is on the rise and spreading quickly throughout the U.S. According to Dun & Bradstreet, a leading provider of business credit information in the U.S., business identity theft cases have been reported in at least 22 states.

Instead of targeting individuals for identity theft, criminals look for ways to steal a legitimate business identity by gaining access to its bank accounts and credit cards, as well as other sensitive company information. Thieves then secure lines of credit with banks and retailers at the expense of the victim entity. Once the scheme is uncovered, businesses may need to spend valuable time and resources to repair the damage to their credit and reputation, and banks and retailers may be left with significant financial losses.

How Do Criminals Steal Business Identities?

Examples of business identity theft include a variety of schemes involving fraudulent use of a company's information, including:

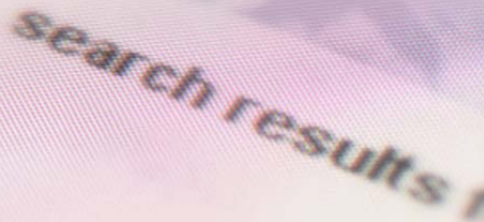
- Establishing temporary office space and/or merchant accounts in your company's name
- Ordering merchandise or services with stolen credit card information, or with bogus account details in the name of your company
- Scams and phishing attacks designed to get access to your company's banking or credit information, including rummaging through your trash
- Filing bogus reports with state business filing offices, or manipulating online business records, in order to change your registered address or appoint new officers/change your registered agent information (to then establish lines of credit with banks and retailers)

Clever criminals are using the economic downturn to their advantage by targeting inactive companies, or companies that can be re-instated for business.

How Can Businesses Prevent Business Identity Theft?

One of the most effective ways to protect your business from identity theft is by regularly checking your records with the Secretary of State's office (or the state agency responsible for housing such information). These offices provide online search features that make it easy to check and verify that business registration information is accurate. Businesses should notify the Secretary of State of any unauthorized changes. Other prevention steps include:

- Sign up for email notification of business record changes, if available
- Monitor credit reports and sign up for a credit monitoring service



Tips to Shield Yourself from Business Identity Theft

- Prevent: Check business records regularly
- Protect: Sign up for email alerts available & monitor credit reports on a regular basis
- Preserve: Report any irregularities or problems immediately

If You Suspect a Problem

- Notify banks and creditors right away
- Contact law enforcement and credit agencies
- Contact the Secretary of State's office
- Correct any altered business records

(Continued) How Can Businesses Prevent Business Identity Theft?

- Monitor business accounts, bills, credit card statements, etcetera, and reconcile your statements on a regular basis
- Sign up for email notifications from banks and other creditors, if available
- File all reports and renewals with state filing offices in a timely and thorough manner, and remain aware of who has access to this information within your company
- Continue checking business records, even if your business is dissolved or inactive
- Safeguard your company's sensitive information, including account numbers and passwords, being sure to shred any trash that contains this information
- Ensure that your computers are secure, and train employees to avoid phishing scams and emails that may contain malicious viruses

What to Do if Business Identity Theft Occurs?

If you suspect that your company has become a victim of business identity theft, it is important to take quick action to minimize the potential damage. Steps you should take in this situation include:

- Contact banks, credit card providers, and other relevant creditors to notify them of the fraud
- Report the issue to the credit reporting agencies (e.g. Dun & Bradstreet, Equifax, Experian, TransUnion)
- Place a fraud alert on business/merchant accounts
- Notify local and/or state law enforcement officials
- Request copies of documentation used to fraudulently open or access accounts
- If the theft involves unauthorized changes to business information on file with the state, correct the records and notify the Secretary of State's Office (or the state agency responsible for housing such information)

Additional State and National Resources

State Website Page Here: www.ProtectYourBusiness.us

The National Association of Secretaries of State: www.nass.org

National Federation of Independent Small Business: www.nfib.org

U.S. Secret Service Field Offices: www.secretservice.gov/field_offices.shtml