THE NATIONAL CYBERSECURITY SOCIETY

BUSINESS IDENTITY THEFT IN THE U.S. FACT SHEET

TIPS TO PROTECT BUSINESS IDENTITY

Business identity theft is more complex than individual identity theft. The challenge businesses face is that the majority of the elements that comprise a business identity are publicly available.

Business Information. Data used to manage a business's identity contains public, non-sensitive data. Elements of business identity data are: fictitious name, or "doing business name", DBA, owner's name, legal entity type, address, county, state, registered agent, date of formation, subsidies, and website address (url). Protecting this data involves knowing where it is stored and learning ***how to control access*** to it. Criminals easily access these data repositories and change the identifying information to support their heist.

State Registry Office. First, it is important to manage the data held with the state registry office(s). Know which states you are registered in to do business. Ensure that access to the data about your business is locked down with a user name and a strong password. Change your password every 3 months. Ensure your password is at least 16 characters or longer or use a password manager. Additionally, some states offer the ability to sign up for automated alerts – a great way to be notified if a change has been made, and if the state offers two factor authentication, sign up for this protection as well.

Business Credit File. The Credit Reporting Agencies (CRAs) recommend that businesses be proactive in monitoring and updating their business credit file and notify them of any potential errors. Each of the three CRAs – Dun & Bradstreet (D&B), Equifax and Experian collect different data about your business. Additionally, the credit rating scales are also different. See our report for a full listing of the data collected. The key to manage your credit is to monitor your D&B business file. This file is accessible and free. As a business owner, you can go in and correct any erroneous data, as well as track whether someone might have gone in and changed it. Any changes to the D&B file are shared with the other CRAs.

If you believe your company's data in the business file has been changed by an unauthorized user, contact Dun and Bradstreet at 1-866-895-7262, highriskandfraudinsight@dnb.com. The other CRAs require you to register to have your credit file monitored, whereas D&B allows you to do that for free.

During our review, D&B informed us they will provide businesses recovery support for an identity theft – offering research support, flagging the account as "stop distribution" until the file is corrected, and assisting in resolving any inaccurate data.

CRA Contact Information for Identity Theft are:

Dun & Bradstreet: 1-866-895-7262
Experian: 1-888-397-3742
Equifax: 1-800-685-5000, option 4.

Website. Managing your identity on the web, is an important aspect of your business, especially if your business depends on e-commerce through your website. Recommendations for a safe and secure website are:

- Conduct regular backups for your site; at least every day;
- Ensure your website is routinely scanned for malware and/or viruses;
- Ensure your site is protected by a web application firewall;
- Ensure your site transactions are secure and your website is listed as https:

Trademark. Officially register your firm's name and logo as a trademark. Many state offices provide this service at a nominal cost.

EIN/SSN. Protect your business's EIN (Employer Identification Number from disclosure, and the owner's SSN.

Training. Train your employees not to release information about your business to callers; or post business information on social media or the web. Have periodic phishing training for your employees.

Partners. Verify the financial/solvency position of your potential and existing business partners before you share critical business data. D&B provides this service for a nominal fee. Require your partners to sign a partnership agreement that requires them to protect your critical business data.