BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 22-014 **February 2022, Issue #70**

BusinesSafe Threat Topic: Business Identity Theft

Business identity theft occurs when a criminal actor uses information related to a business such as its Employer or Tax Identification Number or corporate filing number to fraudulently obtain lines of credit, money, tax benefits, or to perpetuate individual identity theft. Business identity theft can impact the owner or company's ability to file taxes, and it can even result in the theft of client or employee personal identifiable information. This article includes an overview of common methods used by criminal actors to obtain sensitive information for fraudulent means along with warning signs and mitigation tactics businesses can use specific to business identity theft. While these lists are not all encompassing, they offer information for businesses to better recognize and protect themselves from identity theft.

How criminal actors may steal your business identity

- Cyber criminals may use tactics such as, business email compromise, phishing, smishing, or data accessed through a previous cyber data breach to obtain business electronic login or identifying information.
- Criminal actors may fraudulently pose as vendors, customers or government employees and request information about the business to update nonexistent business records.
- Criminal actors may pose as employees of vendors and make suspicious requests to change vendor bank deposit information or make requests for the business's updated bank account information.
- Employees may receive fraudulent emails or phone requests from criminal actors claiming to be from another department within the company. These criminal actors may request employee or business records or other reports that include personal identifiable information or business account information.

Signs that your business may be a victim

- You receive unexpected letters from the Internal Revenue Service (IRS) or state tax agency notifying you of a rejected filing, request to extend filing, or tax transcripts that were not requested. Conversely, the business has not received expected or routine IRS mailings.
- Bank accounts or lines of credit opened in the name of the company without authorization from the company.
- Banking or credit transactions not made by authorized account holders.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1 FSIN: 1.1.1, 1.2.1, 3.1 FFC: 1.1, 1.2, 1.3, 4.1, 4.4, 6

- Filing of bogus documents with the Secretary of State's office in order to change the business' registered address or the names of directors, officers or managers of the company.

Tactics for businesses to help mitigate against business identity theft

1. **Protect sensitive information.**
   - Protect your business's identifying information such as your Employer Identification Number, Tax Identification Number and Social Security Number. Don't give them out unless required, and shred old documents that include business identification information.
   - Protect your business's credit card, supplier and vendor account information. Keep an updated list of open accounts and key contact information.
   - Protect your business's computers and networks. Restrict use of your business computers to only business activities. Secure your company's wireless network and ensure software is continuously updated.
2. **Review records regularly.**
   - Regularly review your banking and credit card statements and report suspicious or fraudulent activity immediately.
   - Regularly review your state business registration information to make sure your information hasn't been changed or updated without authorization.
   - Consider reviewing your business and personal credit report at least annually. Report any suspicious activity or inquiries immediately.
3. **Train employees on safety measures**
   - Train employees on information security policies and how to detect and respond to fraudulent calls and emails.
   - Train your employees on cybersecurity and ways to prevent unauthorized access to sensitive information and accounts.

Resources

- Report business identity theft to the IRS if you think someone is using your business name or EIN to submit fraudulent tax returns. The IRS website also offers identity theft information for businesses.
- The Small Business Administration (SBA) offers resources for businesses to report business identity theft used to obtain a fraudulent COVID-19 Economic Injury Disaster or Paycheck Protection Program loans. The SBA also offers advice for business to avoid tax-related identity theft.
- Report identity theft to the Federal Trade Commission (FTC). The FTC also offers information on recovery from identity theft.
- The Florida Department of State Division of Corporations offers an identity theft resource guide for Florida businesses.
- The Florida Office of the Attorney General provides multiple resources for victims of identity theft.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us