THE NATIONAL CYBERSECURITY SOCIETY

BUSINESS IDENTITY THEFT IN THE U.S.

FACT SHEET

WHAT IS BUSINESS IDENTITY THEFT?

In October 2017, the NCSS was selected by the Identity Theft Resource Center (ITRC), under the auspices of the Department of Justice, to lead a national coalition on business identity theft.

Through the grant provided by ITRC, the NCSS completed a study of the crime and recently published the findings in *"Business Identity Theft in the U.S."*, The report is available on our website. This fact sheet defines business identity theft and the main types of this insidious crime.

Business Identity Theft is defined as:

"identity theft committed with the intent to defraud or hurt a business by creating, using or attempting to use a business's identifying information without authority"

The types of business identity theft are:

1. ***Financial Fraud*** – obtaining new lines of credit, loans or credit cards in the business's name; and/or filing fraudulent UCCs,
2. ***Tax Fraud*** – filing fraudulent returns using tax subsidies and/or obtaining refunds either through the federal and/or state governments,
3. ***Website Defacement*** – manipulating a business's identity (website) on the web,
4. ***Trademark Ransom*** – registering the business name or logo as an official trademark and demanding a ransom for release of the trademarked business name or logo.

Information about your business is publicly available at the state registry office and with Dun & Bradstreet. These open records are available to facilitate trade and financial transactions. However, thieves utilize these open records to find businesses with good credit to steal. By accessing online state records, they change information about your business – such as registered agent, owners, address, and revenue. This new business information is then shared with the credit reporting agencies. Once an altered identity is created, the criminal uses this information to make online applications for credit cards and lines of credit. A business owner only knows this has happened when someone calls due to nonpayment.

Start by protecting your business identity through establishing a user name and password at the state registry and signing up for email alerts so you may be notified in the event a record has been changed.

Other measures you can take: 1) officially record your business name and logo as a trademark, 2) monitor your website for malicious code that could redirect your customers to nefarious websites that look like your own, and 3) monitor your credit regularly.