Protecting Your Business from Identity Theft and Cybercrime

HOW TO RECOGNIZE AND FIGHT BACK AGAINST IDENTITY THEFT, CYBERCRIME, AND SCAMS

About Georgia Watch

OUR ORGANIZATION

- Founded in 2002
- Statewide advocacy organization
- Non-profit and non- partisan

OUR WORK

- Equity and justice for all Georgia consumers.
- Protecting and informing consumers so all Georgians prosper and communities thrive.
- Serve as a trusted source for elected officials, the public, and the media.
- Offer a toll-free consumer hotline.

We focus mainly on issues that impact economic security and quality of life.

Financial Protection

Healthcare Access

Consumer Energy

Access to Civil Justice

Goals:

- Encourage open dialogue around cyber-crime and identity theft concerns for small business owners
- Help participants identify red flags and teach them how to take proactive steps to minimize their company's risk
- Encourage participants to utilize available reporting resources if they know or suspect their company is a victim of identity theft and/or a cyber-crime
- Equip participants with information to train business owners about ways to protect themselves

This module was produced by Georgia Watch under award #2016-XV-GX-K004, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this module are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

During COVID-19, identity theft and cybercrime are even more of a threat to small businesses. The information discussed in this presentation was applicable before COVID-19 and even more applicable now.

What is Business Identity Theft?

- Like consumer identity theft that occurs when someone steals a consumer's personal information to commit fraud, **business identity theft occurs when someone steals a business's information to commit fraud:**
  - Stealing a business's identity can mean theft or misuse of business identifiers and credentials, manipulation or falsification of business filings and records, and other related activities intended to derive gain to the detriment of the business, and/or to defraud creditors, suppliers, financial institutions, the business's owners, consumers, or the government.

Source: BusinessIDTheft.org

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

General Strategies for Managing Identity Theft Risk

1. **Understand that identity is an asset.**
2. **Take an inventory of your identity assets.**
   - If you can't observe or see it, you can't control it.
3. **Evaluate the value of your identity assets and liabilities.**
   - You can't understand the value and liabilities unless you **understand the prevalence of identity theft.**
4. **Determine your identity threats and vulnerabilities.**
   - To determine your threats and vulnerabilities, you must understand what identity criminals want from you and their process for obtaining it.
5. **Develop a plan for incidents that may occur.**

Source: The University of Texas at Austin Center for Identity

Identity is an Asset: Treat it Like Gold

Your business likely not only has its own personal identity information (tax identification number, address, etc.) but also collects, stores, uses, or even shares the personal identity information of customers or clients (social security numbers, date of birth, etc.). These pieces of personal identity information are assets, meaning they have value.

Source: The University of Texas at Austin Center for Identity

Your Inventory:

What does your business or organization have that may be valuable to an identity thief?

GEORGIA WATCH™
PROTECTING CONSUMERS SINCE 2002

Your Value: What Do You Have that an Identity Thief Might Want?

WHAT DO IDENTITY THIEVES WANT?

- Employer identification number (EIN)
- Social security number
- Account numbers
- Credit card numbers
- PINs, usernames, and passwords
- Financial records

WHERE AND HOW DO THEY GET IT?

- ***Directly from you***
- "Dumpster diving" or your mailbox
- Large scale commercial data breaches
- Your computer files
- **Phishing emails and malware**
- Your filing cabinets or closets

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Your Value: Why are these Assets so Valuable to an Identity Thief?

REASONS IDENTITY THIEVES TARGET BUSINESSES

- Larger bank account balances
- Easy credit and account opening
- Flexible payment terms
- Higher credit limits
- Larger purchases can be made without raising red flags
- Minimal security
- Easily available information
- Difficult to investigate and prosecute

Source: BusinessIDTheft.org

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Your Vulnerability: What Threats Do Identity Thieves Pose to You?

IDENTITY THIEVES WILL OFTEN USE YOUR INFORMATION TO ENGAGE IN:

- Fraudulent business registrations and filings
- Physical address mirroring
- Tax fraud using your business EIN
- Bank account fraud
- Manipulation of credit reports and records
- Misuse of business owner's or officer's identity for fraud

These activities can wreak havoc on a business and lead to personal and professional ruin.

Source: BusinessIDTheft.org

Let’s take a look at 6 common ways identity thieves target businesses and organizations.

GEORGIA WATCH™
PROTECTING CONSUMERS SINCE 2002

Fraudulent Business Registrations and Filings

There are a variety of ways criminals target businesses through state filing and registration systems. Identity thieves may attempt to:

- File a change of business address or a change to the business's officers, directors, or registered agent
  - This may enable a criminal to gain perceived control of the business and act on its behalf and/or receive important, sensitive materials related to the business.
- Reinstate a dissolved, closed, or dead business
  - This is particularly concerning because a dissolved business entity can typically be reinstated up to two years after it has been dissolved.
- Register a business as a foreign or out of state business
  - This enables a criminal to leverage the businesses reputation and credentials, and often goes unrecognized until the business owner is contacted by creditors or law enforcement.
- File or use or similar business name
  - This act often goes unrecognized until the business owner starts receiving invoices for items that were never ordered.

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Source: BusinessIDTheft.org

Physical Address Mirroring

Identity thieves may closely mimic the physical address of the target business for the purpose of obtaining lines of credit, loans, cash advances, and goods and services in the business's name.

- To carry out this scam, the identity thief:
  1. Finds a good location and victim business;
  2. Gains information about the victim business's finances, creditors, owners and officers;
  3. Rents space in the same building as the victim business;
  4. Applies for credit or loans in the victim business's name; and finally
  5. Accrues bills and debts in the victim business's name and vanishes
- This tactic is often successful the nearly exact address match is generally all that's need for verification in financial transactions.

Source: [BusinessIDTheft.org]

Use of Business EINs for Tax Fraud

An identity thief may use a stolen EIN to engage in tax fraud. It is increasingly easy to do and, therefore, a popular crime against businesses.

- The identity thief simply files tax returns reporting false income and withholding in order to obtain a fraudulent tax return.
  - This is even more of a danger now, given how many e-filing platforms do not require an actual, physical W-2 form, meaning all the criminal needs to file business taxes in the business's EIN, name, and address.
- It can take the IRS a while to detect that an e-filed tax return was fraudulent because the IRS may not have access to the W-2 information at the time that the return is processed because different schedules exist for filing tax returns and releasing W-2 forms.
  - A tax return can be e-filed any time in January, while W-2 information only becomes available to the IRS after January 31st, which is the deadline for employers to distribute W-2 forms to employees. **Criminals take advantage of this gap and e-file fraudulent returns early.**
  - The IRS then may be unable to immediately verify the reported income and withholding during the tax return processing until after the fraudulent return has been received. **This can put the victim business on the hook for thousands of dollars once the fraudulent reporting is detected!**

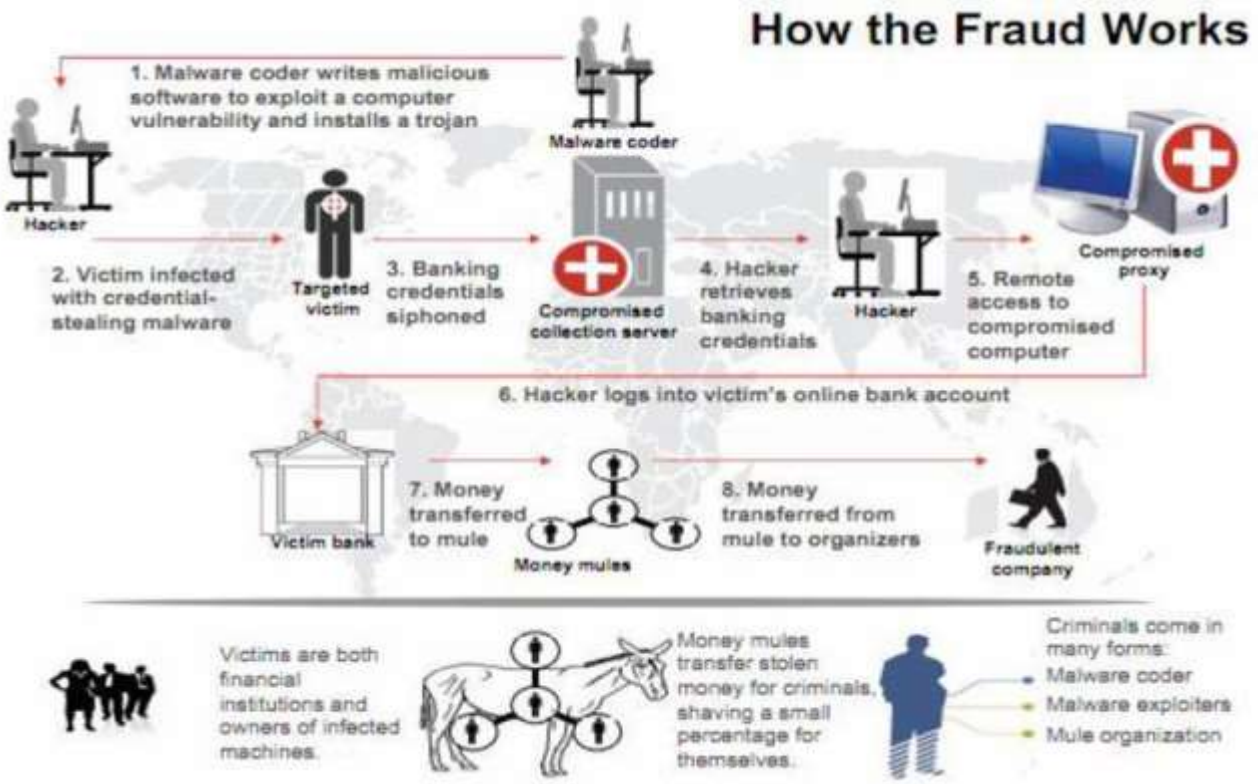
Source: BusinessIDTheft.org

Bank Account Fraud

Identity thieves sometimes target businesses to steal bank account information that enables them to take over the accounts to conduct fraudulent activities, including: unauthorized wire transfers, credit and debit card transactions, and check fraud.

- Unauthorized wire transfers
- Credit and debit card transactions
- Check fraud

Banks often do not provide fraud protection to companies, so do not assume that your bank protects your business account!



Source: BusinessIDTheft.org

Manipulation of Credit Reports and Financial Records

Identity thieves seek access to the self-reported and publicly available financial information and credit reports of businesses.

- With this information, thieves can manipulate credit and financial files to deceive creditors or lenders.
- Thieves may obtain sensitive credit information by creating fake credit applications that appear legitimate to the business owner.
  - This can be done simply by modifying a legitimate credit application form and changing the return mailing address to the thief's mailing address. Once the business owner fills out the form and mails it, the thief will then have all the sensitive information he needs to commit fraud.
- Thieves manipulate financial reports (sometimes even creating entirely false reports) to make a business appear to be better off than it is to creditors and lenders. This enables the thief to defraud institutions in granting loans or lines of credit in the business's name.

Source: [BusinessIDTheft.org]

Misuse of Business Owner/Officer Identity

Identity thieves sometimes target business owners, officers, executives, and directors, hoping to use their personal information or status to commit fraud. Thieves may:

- Impersonate the owner or officer to carry out important transactions in the business's name, including changing the business's information to usurp authority from the owner, making fraudulent cash withdrawals and purchases, and even opening bank or credit accounts in the business's name.
- This can ultimately harm the business owner's or officer's personal credit and existing account services, leading to increases in interest rates, loss of credit lines, inability to open new accounts or obtain business or personal financing.

Source: BusinessIDTheft.org

Let’s discuss some ways you can protect your business or organization.

GEORGIA WATCH™
PROTECTING CONSUMERS SINCE 2002

How does your business or organization manage and protect sensitive information and identity assets currently?

GEORGIA WATCH™
PROTECTING CONSUMERS SINCE 2002

Protect Your Business: Take an Inventory of Your Identity Assets

General Advice: Make sure you are always well-informed of business decisions regarding the collection, sharing, storage, and use of the business personal identity information as well as that of customers or clients. You should have full control of this information.

If you can't observe or see it, you can't control it.

Source: The University of Texas at Austin Center for Identity

Protect Your Business Identity Assets

- **Think of your business EIN as your own social security number.**
  - Limit how often and to whom you disclose your EIN. Only disclose your EIN when it's required.
- **Keep documents containing important business identity information in a secure, preferably locked, location that cannot be accessed by unauthorized individuals.**
  - This includes physical and electronic copies of important documents.
  - Create passwords, if possible, for accessing sensitive electronic folders and documents.
- **Shred old or unnecessary documents that contain important business identity information.**

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Source: BusinessIDTheft.org

Educate Your Employees

- **Issue rules for email, internet browsing, and social networks**
  - Encourage a culture of "safe browsing" and caution staff to be wary of suspicious links and attachments from unknown sources when using company devices.
- **Train your employees to recognize and respond to a cyber attack**
  - Give staff a clear channel, such as an emergency number, to alert administrator to any suspicious emails or unusual activity.
- **Make cyber security everyone's responsibility**
  - No one is immune so include everyone, including management and IT, in cybersecurity-related education program.

GEORGIA WATCH
PROTECTING CONSUMERS SINCE 2002

Source: Sungardas.com

Protecting Customer Private Information

- **Protection starts with leadership from information security, IT and cybersecurity teams**
  - All data, files and communications must be encrypted across all devices. That way, even if those items were stolen, they would be unusable.
- **Software can be used to detect suspicious activity across all platforms**
  - Identifying suspicious activity is a critical first step to alert consumers that something is wrong.
- **Key stakeholders throughout the organization must be prepared with an action plan if a data breach occurs**

Source: Bankingjournal.aba.com

Protect Your Financial Accounts from Fraud

- **Review your business banking agreements to understand the banks' policies regarding fraud.**
- **Set up security controls and authentication process to minimize risk of fraudulent wire transfers and electronic transactions**
  - Add 2-step authentication to all accounts.*
- **Monitor your credit cards, bank accounts, and credit reports daily.**
  - Report any suspicious activity immediately. Have alerts sent to your phone when your credit or debit card is used.
- **Create strong, unique passwords for your various online accounts.**
  - Make sure your passwords have a mix of letters, numbers, punctuation, both upper and lowercase letters, and at least eight characters long. Choose obscure security questions..
- **Be wary when opening emails that could be phishing scams.**
  - Check the header, any embedded links, and the domain name. Read the body of the email carefully. Don't open attachments unless you are familiar with the sender.

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Source: BusinessIDTheft.org

Protect Your Financial Accounts from Fraud (cont'd)

- Keep an inventory of all your accounts and key contact information
- Make sure your review and reconcile all account statements as soon as they arrive
- Request that financial institutions with which you have trade and credit accounts notify you if they are contacted
- Review your business credit reports
  - Pull your reports from Dun & Bradstreet, Experian, Equifax, and TransUnion
- Keep all business and personal finances and accounts separate

Source: BusinessIDTheft.org

GEORGIA WATCH
PROTECTING CONSUMERS SINCE 2002

Protect Your Business Registration

- **Set up email alerts from the Secretary of State.**
  - It is free to enroll and the alerts notify you when your business registration information has been changed or updated.
- **Check your business registration information online regularly, whether your business is active or close.**
- **File your annual reports and renewals on time.**
  - Report any suspicious activity immediately.

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Source: BusinessIDTheft.org

Protect Your Computer, Networks, and Online Presence

- Restrict the use of business computers to business only activities
- Install and use a regularly-updated anti-virus or similar internet security software
- Check for and regularly install security updates
- Install and use a firewall on your computer and networks
- Secure your wireless network by encrypting access
- Export and/or delete all information associated with expiring domains
- Use Google Alerts to monitor internet presence
- Use a database and domain privacy service
- **Use a VPN or password manager to add an extra layer of protection.**

Source: BusinessIDTheft.org

Protect Your Business While Working from Home

- **Be alert for phishing emails and malware**
  - These emails look very legitimate but seek to steal your business's information.
- **Use encryption software**
  - Encrypt any communications that contain sensitive information.
- **Use a VPN to connect to your business's network**
  - This helps secure the transmission of your information.
- **Install anti-virus software to protect your home network**
- **Secure your wi-fi network**
  - Change or create a password.

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Source: TechStak.com

Protect Your Business from Fraudulent Orders

- Be on the lookout for large or unusual orders from unknown customers or companies
  - Review order and customer information before providing products or services
  - Consider checking the customer's credit and references before filling an order
- Use fraud prevention services for online orders
  - These services include zip code, address, or card code verification
- Respond quickly to any customer notifications about fraudulent orders

Source: BusinessIDTheft.org

Protect Your Personal Identity: Your Credit Score and Report

- **Check your credit report at least twice per year for all three major bureaus**
  - **Equifax: 1-800-525-6285**
  - **Experian: 1-888-397-3742**
  - **TransUnion: 1-800-680-7289**
  - **AnnualCreditReport.com**
- **By federal law, you are entitled to one free credit report from each major bureau every year**
  - COVID-19 update: you can check your credit report for free every week until April 2021 due to the crisis
- **Georgians are entitled to an additional two reports each year from each major bureau - meaning you get a total of *9 free reports every year***

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

Protect Your Personal Identity: Freeze Your Credit

- Freezing your personal credit prevents people from using it.
  - This is important for business officers and owners, who are often targets for thieves
- Anyone can freeze and unfreeze their credit **for free** and at their leisure
- *If you think you may be a victim of identity theft, freeze your credit immediately*

Source: Consumer Federation of America

GEORGIA WATCH™ PROTECTING CONSUMERS SINCE 2002

What to Do If Your Personal Identity Was Stolen

- **Contact your bank or card company immediately.** If it involves fraudulent use of your credit card or check card, contact the bank or credit card company immediately to inform them and file a report.
- **Create an initial fraud alert and request your credit reports.**
  - Contact one of the three credit report agencies and ask for a fraud alert to be put on your account, as well as a copy of your credit report. Fraud alerts are free and last for 90 days. Carefully review your credit report upon receiving it – check that all information is correct. Dispute any errors with the three national credit bureaus and any businesses involved in your ID theft.
- **File a police report immediately.**
- **Create an Identity Theft Report.**
  - First, create an Identity Theft Affidavit with the Federal Trade Commission: 1-877-438-4338 or www.ftc.gov/complaint. Then, file a police report. Bring a copy of your FTC Identity Theft Affidavit, a government-issued photo ID, proof of address, and additional proof of theft.

Source: The University of Texas at Austin

GEORGIA WATCH
PROTECTING CONSUMERS SINCE 2002

What to Do If Your Personal Identity Was Stolen (cont'd)

- **Replace any missing documents.**
  - Contact your state DMV, the U.S. Department of State, the Social Security Administration, and your bank and credit card companies to replace missing driver's licenses, passports, SSNs or cards, and debit/credit cards or checks (respectively).
- Consider a credit freeze and an extended fraud alert (lasts for 7 years instead of 90 days).
- Clear compromised tax records by contacting the IRS.
- *Keep all documents related to the theft and your report.*

- For more help, **contact the Identity Theft Resource Center (ITRC).**
  - Contact the ITRC at 888-400-5530.
  - Visit www.idtheftcenter.org for resources and information about identity theft.

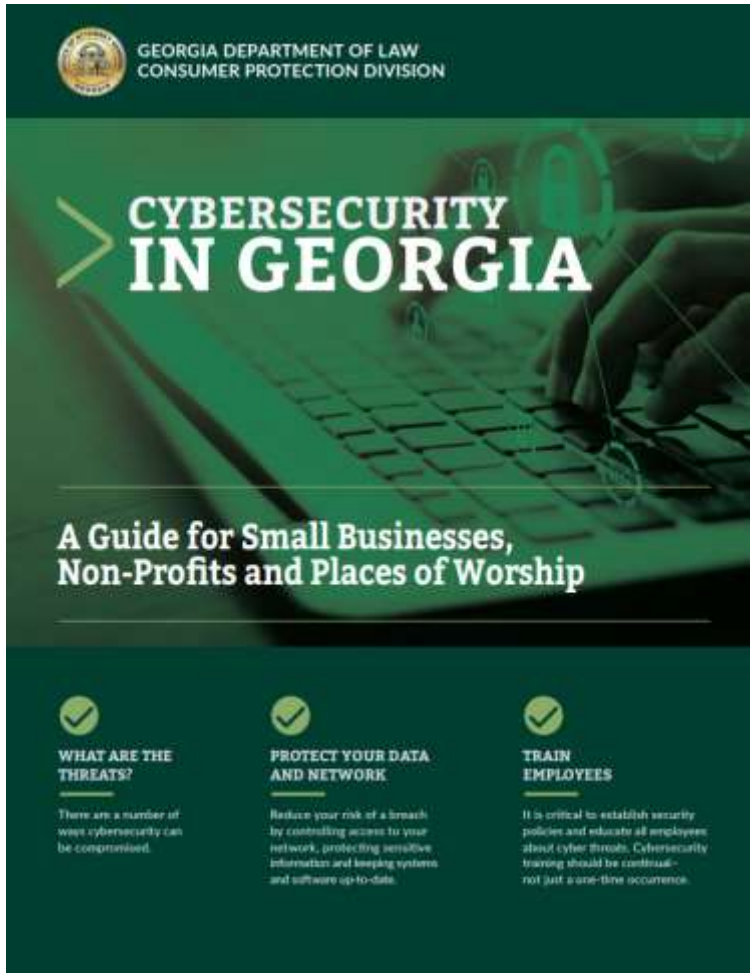
ITRC | IDENTITY THEFT RESOURCE CENTER
888.400.5530

Source: The University of Texas at Austin

GEORGIA WATCH
PROTECTING CONSUMERS SINCE 2002

What to Do If Your Personal Identity Was Stolen (cont'd)

- If you were targeted by a scam or received any suspicious communications, **report it** immediately
  - If identity theft may be involved,
    - File a police report
    - Contact the FTC
      - 1-877-FTC-HELP
      - www.ftccomplaintassistant.gov
- As appropriate, you may also consider contacting:
  - Consumer Financial Protection Bureau
  - Georgia Attorney General Consumer Protection Division
  - Banks/credit unions
  - Creditors
  - Involved retailers or companies
  - Better Business Bureau



New Cybersecurity Guide!

The **Georgia Attorney General Consumer Protection Division** released a cybersecurity guide for small businesses, non-profits, and religious organizations in October 2019.

Download the guide: http://consumer.ga.gov/uploads/pdf/Cybersecurity_in_Georgia.pdf.

Helpful Resources and Guides

- Visit University of Texas Center for Identity for resources for small businesses
- **Visit BusinessIDTheft.org and sign up for alerts**
- Sign up for alerts at Fraud.org
- Visit the Federal Trade Commission site for tips about scams and subscribe to the blog to stay up-to-date
- Read the Federal Trade Commission resources on cybersecurity
- **Read the U.S. Small Business Administration cybersecurity information guide**
- **Visit CSN's Resources for Remote Work and Small Businesses**