NATIONAL SECURITY AGENCY
CYBERSECURITY INFORMATION

# IDENTITY THEFT THREAT AND MITIGATIONS[1]

## Introduction to Identity Theft

Identity theft is a crime that involves using another person's personal information to take malicious actions, such as conducting fraud or stealing funds. The information provided in this document is designed to help individuals protect themselves against identity theft and mitigate the risk.

The frequency of identity theft has increased dramatically. Criminals can use a multitude of methods to obtain Personally Identifiable Information (PII), which can be leveraged to carry out malicious actions. Personal protection from these actors must be dealt with on all fronts, as a layered approach. As set forth throughout this paper, there are numerous steps that one can and should take to defend against identity (ID) theft in general and the prevalence of targeting by sophisticated and not-so-sophisticated hackers. However, none of the steps, either alone or in the aggregate, can absolutely preclude becoming a victim of identity theft or prevent PII from being stolen. The information provided throughout this document is designed to help protect against this possibility and to mitigate the risks that could happen. If, despite best efforts to defend against ID theft, a determined attacker is successful in conducting ID theft, basic guidance is provided to assist in addressing the situation.

## The Threat

The threat is real as evidenced in some of the key findings from the U.S. Department of Justice, "Victims of Identity Theft (Revised 2017)" report (Source: https://www.bjs.gov/content/pub/pdf/vit14.pdf):

- 17.6 million American or 7% of 16 years or older were victims
- 86% experienced misuse of an existing credit card or bank account.
- 7% experienced multiple types of identity theft
- 14% of identity theft victims experienced an out of pocket loss. 49% of those suffered losses less than $100 and 14% lost $1,000 or more.

The threat actor's goals may include (but aren't limited to) character degradation, altering financial status, and/or creating legal problems. The classes or types of threat actors could include hacktivist (hackers for a social/political cause), disgruntled employees, cyber criminals, and nation-state actors. Today's online connectivity fosters a proliferation of locations where PII may be retained and (readily) available. Personalized email based phishing attacks are becoming more sophisticated. All of the aforementioned factors result in a heightened cyber risk environment and requires greater vigilance on the part of individuals to protect private information. PII can facilitate successful ID theft to include obtaining Social Security Number (SSN), age, salary, and phones numbers. This information is critical for successful identity theft. Any, and all, public, personal data can be useful to perform ID theft and aid in crafting believable spear-phishing emails that can appear to be sent from trusted sources. Through phishing, an attacker can gain remote control of a device (desktop, laptop, cellphone, tablet, etc.) or can gain access to stored data to authenticated websites; all of which can further facilitate ID theft.

## Typical Techniques

Whaling, a common ID theft technique, is the targeting of high ranking corporate executives (the *big fish*) via malicious emails, links, or attachments. The goal is to compromise networks, devices, and/or to collect personal/organizational information. Unbeknownst to the victim, the threat actor performs targeted research on exposed personal information in

[1] The information contained in this document was developed in the course of NSA's cybersecurity mission including its responsibilities to identify and disseminate information on threats to national security systems and Department of Defense information technologies, develop and issue security implementation specifications for cybersecurity-enabled products, and to assist Executive departments and agencies with operational security programs. The information may be shared broadly to reach all appropriate stakeholders.

order to craft deceptive emails. The emails often contain attachments/links and information designed to deceive. These appear to originate from a known person, have a professional look and feel, and are difficult to identify as malicious. The ID thieves' target will often open the bogus emails and then "click-on" the socially engineered malicious attachments/links. While the skill level required for successful ID theft is minimal, data/PII manipulation or assumption of target ID, requires increased sophistication. ID theft includes, but is not limited to, fabricating criminal liability, ruining an individual's reputation or credit, and blackmailing the target, which could result in legal action, job loss, or arrest. ID theft may achieve these goals through the following means:

- **Take Advantage of System Access:** Place material on a hard drive that is indicative of serious illegal activity (e.g. maliciously edited photographs, espionage, insider trading, incriminating emails)
- **Alter or Access Financial Information:** Collect sensitive financial information, access, modify, or create accounts (e.g. credit accounts, investment sites), steal funds
- **Recover Credentials** (e.g. user names, passwords, challenge question answers)
- **Establish Persistent Presence on Network or Device:** Gather long-term information on network and device related data. This may be aggregated with data from other information technology systems used.

### Where Can Personal Information be Found?

Personal information can be found online; individuals actively publish data about themselves to include information from signature blocks, social networking sites, organizational sites (e.g. professional, alumni, and clubs), resumes, biographies, or interviews. Personal information can be thought of as identity DNA. It can be used to uniquely "mark" a person for tracking and be leveraged to gain footholds in the personal lives of friends, family members, and co-workers.

<table>
<tr><th colspan="3">Personal Information Related to PII<br>Aggregation of identifiers/credentials could constitute PII</th></tr>
<tr><th>Core Identifiers</th><th>Access Credentials</th><th>Physical</th></tr>
<tr><td>Full Name/Previous Names</td><td>Passwords/PINs</td><td>Gender</td></tr>
<tr><td>Address</td><td>Account Numbers</td><td>Hair Color</td></tr>
<tr><td>Date of Birth</td><td>Email Addresses</td><td>Height</td></tr>
<tr><td>Driver's License Number</td><td>Mother's Maiden Name</td><td>Weight</td></tr>
<tr><td>Insurance Card Number</td><td>Biometric Information*</td><td>Eye Color</td></tr>
<tr><td>Telephone Number</td><td>Medical Information</td><td>Race</td></tr>
<tr><td colspan="3">Personal, Educational, Criminal, Family Information (that can readily be found in public records)</td></tr>
</table>

Most people understand the need to protect their SSN and Personal Identification Numbers (PIN); however, there are other identifiers that could help a thief access PII. The table above lists a few of those less thought about identifiers. Having this additional information enables threat actors to build a better personal profile that may be used to more effectively assume another person's identity.

### Personal Information Trust Relationships

ID theft may exploit networks or accounts of trusted associates from which to send malicious email, as these networks and systems are often not up-to-date with security procedures. Emails sent at specific times of the year may serve to increase the believability of the phishing attempt, such as a tax service provider email sent in the spring or a medical benefits email sent in the fall. Examples of trusted service providers include:

- **Personal:** Spouse/child's employer or school, friends, associates, lawyers, social groups, educational groups (university associations–as student, instructor, or alumni), and Facebook®[2]
- **Professional:** Workplace contacts, conferences, organizations, job posting sites, LinkedIn®[3], and certification groups.
- **Medical:** general practitioner, dentist, specialists, labs, hospitals, therapists
- **Financial:** credit union, banks, investments, mortgage company, pension plans, income tax services, accountants, credit card companies, online purchasing sites
- **Media/Entertainment:** reporters/organizations (interviews, quotes), subscriptions, technical publications, special interest sites, streaming video sites, gaming sites, and Twitch®[4]/YouTube®[5]
- **Social Relationships:** online friends, apps
- **Insurance:** medical, life, homeowners, auto
- **Service Providers:** utilities (Internet Service Providers (ISP), gas, electric, water), home security
- **Other:** Department of Motor Vehicles (DMV), court (jury duty, subpoena), law enforcement, Civilian Welfare Fund (CWF), transportation

### Mitigations – Systems (Hardware, Software, Services)

Several steps that help safeguard hardware, software, and services against ID theft include securing systems, limiting exposure (electronic and physical), applying application controls, and service partitioning (e.g. using different devices/OSes/browsers for activities of differing sensitivities). Specific areas that require attention include home networks, mobile devices, email services, authentication, storage, game consoles, and applications.

### Mobile Devices

Maintain physical control of the device. Turn off wireless, Bluetooth®[6], and GPS when not in use. Exercise extreme caution when considering connection to public WiFi networks, using cellular networks if available. Create a robust device PIN. Enable automatic screen locking (after inactivity) and device disk encryption, if available.

### Home Network

Keep home network devices (e.g. WiFi routers) patched and updated to help deal with the latest attacks and to protect against website drive-by infection. Use anti-virus and anti-malware software to help eliminate threats. Keep browsers and

[2] Facebook is a registered trademark of Facebook, Inc.

[3] LinkedIn is a registered trademark of LinkedIn Corporation

[4] Twitch is a registered trademark of Twitch Interactive, Inc.

[5] YouTube is a registered trademark of Google, Inc.

[6] Bluetooth is a registered trademark of the Bluetooth Special Interest Group

browser plug-ins up-to-date, enable automatic updates if possible, and disable Java™[7] in the browser. Limit privileges (e.g. “guest” or “user” privileges) for accounts used by guests, children, and other daily accesses. Periodically change passwords and keep a higher level of complexity. Make sure wireless access points and domain name servers are secure using the most up-to-date methods.

### Separate Device Activities

Consider having different devices dedicated to different purposes, i.e. one computer for financial/PII use, another for games/children, and another for use while travelling, etc. When travelling, do not take an unnecessary device (laptop or smartphone) on the trip. In general, avoid accessing sensitive services (such as financial and medical) while travelling. Be careful of services that are accessible from mobile devices, and know which services store credentials since these services may not store these securely.

### Email and Cloud

Do not open emails or email attachments from untrusted sources. Opening email attachments from unknown senders can load malware and access sensitive information via deceptive procedures such as whaling. Filter emails; run anti-malware and virus scans.

### Authentication/Passwords

Some online services are beginning to allow the use of physical tokens as a form of authentication. Many others allow for the use of a second authentication channel, such as a text message with a passcode. Biometrics can be paired as a secondary authentication when paired with a password. When these measures are available, use them.

For online services that use password-based authentication. Make passwords complex, and do not use the same password for multiple accounts. If passwords are written down, they should not be associated with the account, and the written list should be stored in a safe place (e.g., in a locked box at home). Most services also provide password reset questions based upon various life information. Often these questions have answers that can be discovered and used to facilitate ID theft.

### Storage (media, SD card, USB, portable, backups, file sharing, disposal)

Disable autorun capability. Never accept removable media from untrusted sources, such as giveaways. Free storage media from conferences or from unknown source may contain malware. Remove or disable hardware from machines that do not need removable media. Secure and maintain physical control over media, computers and mobile devices. Virus scan all removable media. When accessing this media, use non-privileged accounts; if possible, access such media from a virtual machine or sandbox. Make use of document viewers instead of full applications. Prior to discarding removable media, or a computer or smartphone with fixed media, delete all data or physically destroy the media. Consider using secured USB storage, particularly bootable USB drives that offer secure operating systems with identity and password protections.

### Mitigations – Behavioral

Successfully protecting against ID Theft requires planning and effort. Be aware of how your normal mode of operation (behavior) could be used to compromise your identity, and implement safeguards to reduce the threat.

### Be Aware of the Context of the Machine You Use

Exercise extreme caution when accessing public WiFi hotspots. Usually, using a mobile device’s cellular data connection is safer than WiFi. Do not exchange any personal information or transact any sensitive business on untrusted networks.

[7] Java is a trademark of Oracle Corporation

Do not exchange home and work content. Use different usernames for home and work email addresses. To prevent reuse of compromised passwords, use different passwords for each of your email accounts. Use password recovery or challenge questions that no one else (including children) would know or could find from Internet searches or public records. Use two-factor authentication when available for accessing webmail, social networking, financial, and other accounts. Avoid posting photos with embedded GPS coordinates, since this provides information about the location of the persons in the photo at the time embedded in the photo metadata.

### Offline Interactions

Lock financial documents and records, including Social Security cards, in a safe place at home, and lock up wallets or purses in a safe place at work. Before sharing information at the workplace, businesses, children's schools, or a doctor's office, inquire as to why PII is required. Further, ask how will the PII be safeguarded, and discuss the consequences of not sharing. Always shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar PII related documents when no longer needed. Before disposing of a computer or mobile device, always dispose of all the personal information it stores.

### Online Interactions

Be alert to impersonators. Make sure to know who is receiving personal or financial information. Unless initiating the contact or the person communicated with is known, PII should not be given out on the phone, through the mail or over the Internet. If a company that claims to have an account sends an email asking for PII, do not click on links in the email. Instead, type the company name directly into the web browser to access their site, and/or contact them through their customer service center to confirm whether or not the company truly sent the request.

### Travel

Never do online banking in public places. Maintain a low profile. If possible, use cash for purchasing personal items like souvenirs. Advise family members not to discuss your travel details and not to post these on social networking sites.

### Credit Freeze

Take steps to limit others from opening new credit cards and accounts by enabling a credit freeze. Safeguards are available that disallow ahead of time any new purchases

### Monitoring for Identity Theft

Everyone is a potential victim of ID theft; therefore, all must be keenly aware of indications that they have been victimized or are actively being targeted. Monitoring these potential indicators is essential in identifying, mitigating and protecting against the threat. There are two classes of monitoring that are key: personal and commercial.

### Personal Monitoring

Personal monitoring involves individual steps that a person can take to detect ID theft activity. The steps involve routinely searching for evidence of compromise. Examples include reviewing credit card and bank statements, call logs, browser history, email (including the "Sent Items" folder), change in social networking privacy settings, and detecting an increase in unsolicited contacts. Be mindful of credit card skimmers in public places like gas stations, and restaurants. A deluge of unsolicited emails, calls, or letters about making a purchase is an indicator that ID theft may be in progress.

### Credit Report

The most important personal monitoring is reviewing credit reports which contain a history of residences, credit accounts - minimum and maximum balance, open/close status and payment history. Any erroneous information in a credit report can

be an indicator of ID Theft. Credit bureaus generate credit reports and are required by the Fair Credit Reporting ACT (FCRA) to provide a free copy of a person's credit report every 12 months.

### Commercial Monitoring

Credit Monitoring is a commercially available service (normally $10 - $20/month) providing a subscriber with information that indicates changes in their personal profile. Areas of monitoring can be divided into two categories – Financial (credit and banking) and Personal. Financial monitoring identifies changes that are specific to a person's credit, not necessarily their assets. For example, a new bank loan would be detected by a credit monitoring report but a large deposit or withdrawal would not. Personal monitoring identifies non-fiduciary references to a subscriber's identity. This includes civil, criminal or other personal information available in public records. Commercial Monitoring services have proven effective in using Financial and Personal monitoring to identify and mitigate ID Theft activity.

### Response Steps

Recommended steps by the Federal Trade Commission (FTC), the US Government entity responsible for receiving and processing complaints concerning ID theft, are:

1. Place an Initial Fraud Alert
2. Order your credit reports
3. Create an Identity Theft Report with the FTC (1-877-438-THEFT). The initial report is called a Theft Affidavit. The Affidavit in conjunction with a police report makes the formal Identity Theft Report. Identity Theft, Federal Trade Commission;

### Other steps that can be taken include:

1. Contact the fraud department of the three major credit bureaus
2. Contact the company that holds any account that you suspect may have been compromised. Ask for the fraud/security department; consider documenting all interactions with the company and closing all compromised accounts.
3. Contact your local police department and obtain copies of all police reports made in relation to the company.
4. Keep a detailed log of all contacts, notifications and interactions as you report the ID theft. Being as organized and detailed as possible will help you limit exposure to and recover from this crime.

## ADDITIONAL REFERENCES

- DSS' Identity Theft Guidance https://www.dss.mil/pyi/theft.html
- FBI's Insider Threat Guidance

https://www.fbi.gov/ investigate/white-collar-crime/identity-theft

- How To Keep Your Personal Information Secure: http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure
- Banking: Safeguarding Your Accounts: https://www.investopedia.com/university/banking/banking8.asp
- U.S. Cert's Identity Theft Guidance https://www.us-cert.gov/ncas/tips/ST05-019

## CONTACT INFORMATION

Client Requirements and Inquiries or General Cybersecurity Inquiries
CYBERSECURITY REQUIREMENTS CENTER (CRC)
410-854-4200
Cybersecurity_Requests@nsa.gov

## DISCLAIMER OF WARRANTIES AND ENDORSEMENT