TEALWOOD
ASSET MANAGEMENT

Summary: Security and Private Data Tool

Prevention Must-Dos

☐ **Protect all your internet enabled devices with current security software (page 3).**

☐ **Ensure your passwords/personal identification numbers (PINs) are complex, change them often, and use a password vault to protect them (page 3).**

Detection Must-Dos

☐ **Check your credit reports annually (page 4).**

☐ **Check your financial statements, preferably monthly (page 5).**

Restoration Must-Dos

☐ **Act quickly (page 6).**

☐ **Contact all three credit bureaus to place a fraud alert on your file (page 6).**

☐ **Create an Identity Theft Report (page 6).**

☐ **Contact your financial institutions to report the fraud (page 7).**

TEALWOOD
ASSET MANAGEMENT

Security and Private Data Tool

Prevention To-Dos

Protect all your internet enabled devices.

These include: computers, cell phones, tablets, and gaming devices.

☑ **Make sure your computer has the most up-to-date security software.** Set the scan to run automatically at least once a week, if not daily. If you get a message and the software itself cannot correct it, contact a professional.

☐ **Consider upgrading to the most current web browser(s) and operating systems**. These will provide a better defense against newer threats.

☐ **Use a mix of defensive tools:**

- Anti-Virus software;
- Spyware software; along with
- Firewalls to prevent hacking

☐ **Ensure your defensive tools are up-to-date to protect against new threats to your security.**

☐ **Delete your junk email.**

☐ **Do not use links in emails or on websites unless you are sure of the source** (this is how many cyber criminals embed spyware or malware on your computer). Instead, type the URL address into the web browser yourself.

☐ **Scan USB data sticks (flash drives) or other data storage devices before you open any files**.

☐ **Do not act on pop-up messages that warn you of viruses and then offer you a program to clean it up.** Go to your task manager and end the program. If you cannot get rid of the message, contact a professional.

☐ **Treat your laptop like you would a large amount of cash.**

☐ **Download banking or other financial institution software applications (apps) directly from the institution's website.**

Passwords/Personal Identification Numbers (PINs) and Security Questions.

Remember these are equivalent to the keys to your house or car.

☐ **Never use default passwords—change them immediately.**

☐ **Make passwords complex.**

- They should *never* include: Your date of birth; last four digits of your social security number; or family names
- They should *always* contain a combination of characters (upper case, lower case, numbers and symbols) and be at least 8 characters long.

☐ **Use different passwords for different accounts**.

☐ **Change passwords regularly**.

☐ **Do not store them in your browser's memory.**
☐ **Do not write them down.**
☐ **Consider selecting a password vault software program if you have too many to remember.** This allows you to store the information and access it later. Choose a reliable program and be sure it has a very strong password (see above) that is memorized (never write this one down—it is the keys to your life).
☐ **Choose security questions that are considered "out of wallet," questions where the answers cannot be found easily on-line. For instance, "Where did you spent your honeymoon?" or "What was the name of your first pet?"**

Protect your wireless networks.

☐ **Restrict access to your wireless network.**
☐ **Make the password difficult to guess (see above).**
☐ **Avoid using open Wi-Fi networks to do anything personal** (including checking your email) or to give any personal information (e.g., using your credit card for purchases or to check your bank account).
☐ **Your best defense is to purchase a data plan or your own secure mobile hot spot.**

Other Considerations.

☐ **Consider purchasing an Identity Theft Protection Service that will alert you to unauthorized access to your credit.**
☐ **Consider placing a "credit hold" status on your credit report.**
☐ **Protect your social security number. Do not give it out unless you know the source is reliable.** REMEMBER: Most firms you have a relationship with already have this information and will not request it again.
☐ **Guard your mailbox:**
- Mail your payments at the post office;
- Pay attention to your billing cycles—call creditors if you have not received your bills on time;
- Shred your junk mail—especially pre-screened credit card or mortgage offerings;
- Reduce your junk mail by:
  - Review the "privacy policy" of those you do business with and consider opting out;
  - Contact Direct Marketing Association to opt out of mass marketing by calling 1-888-567-8688 or writing to Direct Marketing Association, PO Box 9008, Farmington, NY 11735-9008.

☐ **Have your checks delivered to your bank and pick them up there.**
☐ **Take your receipts and do not dispose of them in public places.**
☐ **Use only secure internet sites when purchasing**. Look for a yellow  padlock symbol next to the address bar or the "s" in "http**s**" in the address itself.
☐ **Know positively who you are dealing with** over the phone, internet or by mail when dealing with personal private data. It is best to initiate the contact yourself.
☐ **Minimize the personal data you carry.** Put in your wallet or purse only what is necessary.
☐ **Have a list of your credit card numbers and who to contact if they are stolen**. Store this list in a secure place.
☐ **Do not forget to protect your other important documents,** e.g., medical records, tax returns, insurance cards, anything that has personal data.
☐ **Remember the adage: If it sounds too good to be true it usually is!**

TEALWOOD
ASSET MANAGEMENT

Security and Private Data Tool

Detection To-Dos

Check your credit reports annually.

There are three credit report agencies—check all three.

☐ **Request a copy of your *free* annual credit report** by contacting the federally authorized source maintained by Central Source, LLC in one of these three ways:

- www.annualcreditreport.com;
- 877.322.8228; or
- Complete an Annual Credit Report Request Form (contact us if you need a copy) and mail to:
    - Annual Credit Report
      Request Service
      P.O. Box 105281
      Atlanta, GA 30348-5281

☐ **Things to look for on these reports:**

- Personal Information Section:
    - Complete and accurate name
    - Complete and accurate address and phone numbers (if you have not lived very long at your current address, your previous address should be listed)
    - Correct Social Security Number
    - Correct date of birth
    - Correct employment information
    - Correct marital status
- Public Records Section:
    - Confirm any listings are correct and complete, e.g. lawsuits or bankruptcies listed that you were not involved in.
    - Confirm that any tax liens, judgments, etc. that have been satisfied are listed as paid.
- Credit Accounts Section:
    - Confirm you recognize all the accounts and loans listed.
    - Confirm the accounts listed are your responsibility (e.g. accounts listed as joint when only one spouse is responsible, premarital debts attributed to you, etc.).
    - Confirm that all your open accounts are reported as open. Having a closed account with a balance will affect your credit score.
    - If you closed an account, confirm it indicates "closed by consumer." Otherwise, it may affect your credit.
    - Incorrect account histories, e.g. late notations, when you paid on time.

- Review the Inquiries Section to ensure you recognize the lender(s) or creditor(s). It is important to note that "pre-approved" credit cards and insurance inquiries should be labeled as such so these will not affect your credit score.

☐ **Correct any mistakes immediately by:**

- Contacting the source of the error, e.g. the lender or creditor that provided the information to the credit bureau;
- Contacting the credit bureau(s) that shows the mistake and asking them to investigate the error. Below is the contact information. Once the mistake is corrected, the credit bureau correcting the error will contact the other two credit bureaus with the correct information:
    - Equifax: 1.800.525.6285; www.equifax.com
    - Experian: 1.888.397.3742; www.experian.com
    - TransUnion: 1.800.680.7289; www.transunion.com

Check your financial statements.

☐ **Review the following statements often, preferably monthly:**

- Credit card statements for any incorrect charges;
- Bank statements for unauthorized withdrawals or charges; and
- Any other financial statements where withdrawals or charges can be executed

☐ **If you see something erroneous, contact the firm *immediately*.**

Check your medical statements.

☐ **Review your medical bills carefully, ensuring all charges are yours.** Medical identity thieves will steal your information to submit false claims for reimbursement, especially to Medicare. Contact your medical provider to correct any discrepancies *immediately*.

Other consumer reporting agencies.

There are many specialty consumer reports. You have the right to receive free annual reports. You may only need to see them if you have received some adverse decision because of what it listed on them.

☐ **For a good overall "check-up" of what is reported about you outside of your credit report the following may be your best option:**

- LexisNexis, https://personalreports.lexisnexis.com

☐ **Following is a list of some other common reporting agencies:**

- Insurance claims: A-Plus Report from ISO; http://www.verisk.com/underwriting/how-to-order-your-free-a-plus-loss-history-report.html or 1.800.627.3487
- Medical and Prescription Drug History. (Note: you would only have a file if you applied for individual life, health, long-term care and/or disability insurance in the last seven years): The Medical Information Bureau (MIB): 1.866.692.6901 or www.mib.com
- Residential and Tenant Reports: 1.888.333.2413 or http://www.corelogic.com/landing-pages/SafeRent-Consumer.aspx
- Check writing history: 1.800.428.9623 or www.consumerdebit.com

TEALWOOD
ASSET MANAGEMENT

Security and Private Data Tool

Restoration To-Dos

Immediate Steps.

Acting quickly may limit the harm. DOCUMENT ALL CONVERSATIONS AND CORRESPONDENCE WITH ALL ENTITIES.

☐ **Contact the fraud department of one of the three credit bureaus.** Inform them of your identity theft and request a "fraud alert" on your file. This alert is free and the bureau you call is required to notify the other two (always confirm this with them). This alert makes it harder for the identity thief to open any more accounts in your name. The alert stays in place for 90 days and may be renewed. Their numbers are:

- Equifax: 1.800.525.6285; www.equifax.com
- Experian: 1.888.397.3742; www.experian.com
- TransUnion: 1.800.680.7289; www.transunion.com

☐ **Ask all three credit bureaus for a copy of your credit report,** asking them to only show the last four digits of your social security number. This will be free even if you have already received your free annual report. Things to look and act on:

- Inquiries for loan and credit you did not make. Ask for these to be removed.
- Look for accounts not opened by you. Contact the issuing creditor's fraud department and follow up with them in writing sent by certified mail with a return receipt.
- For existing accounts that have been tampered with, again, contact that entity's fraud department and follow up with them in writing sent by certified mail with a return receipt.

☐ **Create an Identity Theft Report.**

- This report gives you important rights that will help you recover from the theft:
  - Get fraudulent information removed from your report;
  - Stop companies from collecting debts as a result of this theft or selling this debt to another company;
  - Place an extended fraud alert on your credit report.
- To create the Identity Theft Report:
  - Complete and submit an Identity Theft Affidavit form to the FTC. Go to www.ftccompaintassisstant.gov and follow the prompts or call them at 1.877.438.4338.
  - Bring the Identity Theft Affidavit to your local police and file a report along with any other proof you have. They will also require a government-issued photo ID and proof of your address, e.g. utility bill or pay stub.
  - Note: In some states the police will not take a report about identity theft. In this case, ask the police to file a "miscellaneous Incidents" report.
  - Keep a copy of the Identity Theft Affidavit and Report for your records.

☐ **With credit cards that have been tampered with or opened fraudulently** (as seen from your credit report or billing statement) contact the issuing company's fraud departments.
- Restrict access to your wireless network;
- Give them a copy of the Identity Theft Report;
- For tampered accounts, open new accounts with new cards, PINs and passwords; and
- Verify your address is correct, as this is a one of the first things thieves change so you can't monitor their activity.

☐ **Contact your bank to verify all the transactions in your account are yours.** If you see something erroneous:
- Close your account and open a new one. Insist on password-only access to minimize any more violations; and
- Change your PIN for your ATM card.

☐ **Contact your account manager on your investment accounts**. Verify no unauthorized transactions have taken place. If so, have them open a new account. Any unauthorized transactions should be reported to the Securities and Exchange Commission (SEC) at www.sec.gov/complain.shtml or calling 1.202.942.7040.

Other considerations.

☐ **If your Social Security was used in committing the fraud,** notify the Federal Trade Commission (FTC) at 1.877.438.4338 and the IRS Identity Theft Hotline at 1.800.908.4490.

☐ **If you are over 65 and receiving Social Security,** contact the Social Security Administration at 1800.772.1213.

☐ **Consider having a professional inspect your computer for viruses, malware, spyware, etc.**

☐ **Consider changing your email provider, especially if this is where the theft initiated.**

☐ **After the Fraud Alert expires, which is 90 days after it is placed on your account unless your renew it, consider putting a Credit Freeze or Extended Fraud Alert on your credit file.** These usually cost a nominal fee (about $10), and need to be done at each individual credit bureau. This is an important consideration as identity thieves may hold on to information for years before they use it.

☐ **Passports**: Contact the US, State Department, Passport Services Department at 1.877.487.2778.

☐ **Driver's License:** Contact your local DMV (MN 651.296.6911).

☐ **For more detailed information** and sample letters to use, visit the FTC website and specifically the Identity Theft Pages at www.ftc.gov/idtheft.