Identity Theft Recovery Kit: Taking Back Control

We understand that experiencing identity theft can be incredibly stressful and overwhelming. This kit is designed to provide you with immediate steps, crucial resources, and helpful tips to navigate this challenging situation and regain control of your financial identity.

IMPORTANT FIRST STEPS

- **Act Immediately:** Time is of the essence. The sooner you act, the better your chances of minimizing damage.
- **Review Your Account Activity:** Thoroughly review your accounts and check for any fraudulent transactions.
- **Keep Detailed Records:** Document every phone call, email, letter, and action you take. Include dates, times, names of people you speak with, and reference numbers. This will be invaluable.

IMMEDIATE ACTION CHECKLIST

Contact Your Nearest Branch:

Herndon: 703-481-4578
McLean: 703-218-5190
Clarendon: 703-218-5180
Fairfax | HQ: 703-481-4550
Leesburg: 571-375-1330
Washington, DC: 202-800-4150

***What to do:** Report any suspicious activity, unauthorized transactions, or accounts opened in your name. We will guide you through our internal procedures, close affected accounts, and issue new debit cards.*

Contact the Three Major Credit Bureaus to Place a Fraud Alert or Security Freeze:

- **Equifax:** 1-800-525-6285 | www.equifax.com
- **Experian:** 1-888-397-3742 | www.experian.com
- **TransUnion:** 1-800-916-8800 | www.transunion.com

***What to do:** Place a fraud alert on your credit report. This requires businesses to verify your identity before extending credit. You only need to contact one bureau; they are required to notify the other two. Consider a credit freeze for stronger protection.*

Contact ChexSystems to Place a Security Alert or Freeze:

- **ChexSystems:** 1-800-887-7652 | www.chexsystems.com

***What to do:** Place a security alert or security freeze on your ChexSystems file. ChexSystems is a system commonly used to help verify your information when you open a bank account. Security alerts notify ChexSystems clients when there is an inquiry in your name, while a security freeze prevents access to your ChexSystems report.*

File a Police Report:

- **Non-Emergency Police Number:** Fairfax County 703-691-2131
- **Online Police Reporting:** https://www.fairfaxcounty.gov/police/howdoi/financialcrimes

***What to do:** File a police report for identity theft. This provides an official record of the crime, which is often required by creditors and credit bureaus. Get a copy of the report and the report number. If you're not located in Fairfax County, contact your local police department to file a report.*

File a Report with the Federal Trade Commission (FTC):

- **FTC Identity Theft Website**: www.identitytheft.gov
- **FTC Phone**: 1-877-ID-THEFT (1-877-438-4338)

***What to do:** Create an Identity Theft Report with the FTC. This report is a crucial document that can serve as an official affidavit of identity theft, helping you dispute fraudulent accounts and transactions. You'll also receive a personalized recovery plan.*

HELPFUL TIPS FOR RECOVERY

- ✓ **Review Your Credit Reports Regularly:** For the next year, obtain free copies of your credit reports from AnnualCreditReport.com. Look for any accounts you don't recognize or inquiries you didn't authorize.
- ✓ **Close Fraudulent Accounts:** Contact any creditors, banks, or companies where fraudulent accounts were opened. Send them a copy of your FTC Identity Theft Report and police report (if applicable) and request that the fraudulent accounts be closedand removed from your credit report.
- ✓ **Update Passwords:** Change your online passwords, especially for email, banking, social media, and any other sensitive accounts. Use strong, unique passwords.
- ✓ **Monitor Bank and Credit Card Statements:** Scrutinize all your financial statements for any unusual activity.
- ✓ **Consider a Credit Freeze:** This is a stronger protection than a fraud alert. A credit freeze restricts access to your credit report, making it difficult for identity thieves to open new accounts in your name. You will need to contact each credit bureau individually to place a freeze. You can temporarily lift or "thaw" the freeze when you need to apply for credit.
- ✓ **Beware of Phishing Scams:** Be extra vigilant about suspicious emails, texts, or phone calls requesting personal information. Your bank will never ask for your full Social Security number, PINs, or full account numbers via unsolicited email or text.
- ✓ **Secure Your Mail:** If your mail has been stolen, consider a locking mailbox or picking up your mail at the post office.
- ✓ **Protect Your Social Security Number:** Only provide your SSN when absolutely necessary and when you are sure of the legitimacy of the request.
- ✓ **Sensitive Documents:** Before discarding, shred any documents containing personal information like bank statements, credit card offers, and utility bills.

ADDITIONAL RESOURCES & CONTACT INFORMATION

Social Security Administration (SSA) Fraud Hotlines:
If your Social Security number is being misused:
1-800-269-0271
www.ssa.gov

U.S. Postal Inspection Service:
If you suspect mail theft:
1-877-876-2455
www.uspis.gov

Federal Bureau of Investigation (FBI) - Internet Crime Complaint Center (IC3):
For internet-related crimes:
www.ic3.gov

Consumer Financial Protection Bureau (CFPB):
Information on financial products and services, including identity theft:
www.consumerfinance.gov

Federal Trade Commission (FTC):
Report identity theft and get a recovery plan:
1-877-438-4338
www.identitytheft.gov

REMEMBER: We’re here to help! If you have any questions or need assistance with next steps, reach out to your Business Banker, Relationship Manager, or visit your nearest Branch.