Fieldpoint Private

Identity Theft Assistance Kit

This kit contains resources and a checklist to help you keep track of the companies and organizations you should contact if you believe you are a victim of identity theft. Be sure to document your conversations and any next steps.

CHECKLIST

☐ Contact Fieldpoint Private by calling us at **203-403-9300** or email us at: **inquiries@fieldpointprivate.com**

· Report any new Fieldpoint Private accounts that were opened without your authorization using your name and information.

· Report any suspected fraudulent activity on your existing Fieldpoint Private accounts.

  – Review activity on all your accounts, including checking, savings, credit card, loans, and lines of credit accounts.

  – Confirm that your contact information is correct and that no new cards have been ordered without your authorization.

· Close accounts that have been compromised and open new accounts with new passwords and PINs.

· Change your online banking username and password to something that you only use for your Fieldpoint Private accounts. Don't include personal information such as any part of your name, phone number, or email address in your username or password. For your password, use an uncommon phrase with a mix of upper and lowercase letters, numbers, and special characters.

  – If you bank online or use a mobile app at other financial institutions, change your username and password following the guidance above.

☐ Place a fraud alert or credit freeze on your credit report

Fraud Alert[1]

Contact one of the three credit bureaus to place a Fraud Alert. Placing a fraud alert at any of the national credit bureaus automatically updates your credit files with a fraud alert at all three bureaus.

Note: Fraud alerts are free. A fraud alert requires creditors to verify your identity before opening any new account(s) in your name or changing any existing accounts. Fraud alerts allow lenders to see your credit file, but it requires verification of your identity before any credit application is processed or any new account is opened in your name.

· Equifax: **1-800-525-6285** or www.equifax.com[2]

· Experian: **1-888-397-3742** or www.experian.com[2]

· TransUnion: **1-800-680-7289** or www.transunion.com[2]

Credit Freeze

Contact each of the credit bureaus to add a credit freeze. Freezing your credit is free and prevents anyone but you from accessing your credit. That means you will need to temporarily lift the freeze in order to apply for new credit.

· Equifax: **1-888-298-0045** or www.equifax.com/freeze[2]

· Experian: **1-888-397-3742** or www.experian.com/freeze[2]

· TransUnion: **1-800-916-8800** or www.transunion.com/freeze[2]

☐ Monitor your credit

· Request a free copy of your credit report from one of the bureaus or www.annualcreditreport.com.[2] If you notice information on your credit report that you believe is the result of fraud, file a dispute with the applicable credit reporting agency.

· Since identity theft can take time to resolve, continue to monitor your credit file.

· Consider researching additional credit monitoring products and services to fit your unique needs.

☐ Obtain a report of your banking history

Contact consumer reporting agencies to obtain a report of your banking history and review it for accuracy.

· Early Warning: www.earlywarning.com/consumer-information[2]

· ChexSystems: www.chexsystems.com[2]

☐ Contact other creditors

· Contact credit card companies, utility and phone providers, banks, lenders, and other financial institutions to let them know of potential fraud or identity theft.

· Close accounts that have been compromised and open new accounts with new passwords and PINs.

☐ File a report with local police

A police report provides proof of criminal activity which may help when contacting creditors to dispute charges or accounts opened in your name. Be sure to request a copy of the police report.

☐ Report the criminal activity to the Federal Trade Commission (FTC)

Contact consumer reporting agencies to obtain a report of your banking history and review it for accuracy.

· Call **1-877-ID-THEFT (1-877-438-4338**) to speak with a trained identity theft counselor.

· You can also file your complaint online at www.identitytheft.gov[2]

· For more information https://www.identitytheft.gov/#/

☐ Contact other state and federal agencies as appropriate

· **Department of Motor Vehicles**: If your driver's license was stolen or if you believe someone is trying to get a driver's license or identification card using your name and information, report it to your state agency.

· **Internal Revenue Service**: If you are a victim of tax-related identity theft or you believe someone has filed a fraudulent tax return in your name, follow this guide: www.irs.gov/newsroom/taxpayer-guide-to-identity-theft[2]

· **Postal Inspection Service**: If you believe your mail was stolen or redirected, report it at www.uspis.gov/report[2]

· **Social Security fraud hotline**: If you suspect someone is using your Social Security number for fraudulent purposes, call 1-800-269-0271 or visit www.ssa.gov/antifraudfacts[2]

· **U.S. Department of State**: If your passport is lost or stolen, report it at: travel.state.gov/content/travel/en/ passports/have-passport/lost-stolen.html[2]

☐ Continue to carefully review all your accounts

Continue to monitor all transactions through the mobile app[3] online banking or by reviewing your account statements. Report any unauthorized transactions immediately.

☐ Consider adding 2-Step Verification at Sign-On to your account

2-Step Verification provides an additional layer of security for mobile or online banking by sending you an access code to your mobile device when you sign onto your account.

1. Sign-up may be required. Availability may be affected by your mobile carrier's coverage area. Your mobile carrier's message and data rates may apply.
2. Fieldpoint Private has provided this link for your convenience but does not control or endorse the website and is not responsible for the content, links, privacy policy, or security policy of the website.
3. Availability may be affected by your mobile carrier's coverage area. Your mobile carrier's message and data rates may apply.