



FRAUD RECOVERY CHECKLIST

IMMEDIATE STEPS

After realizing you've fallen victim to a scam, it is important to remain calm so you can take the necessary steps to as soon as possible.

FOLLOWING STEPS

Take a breath. Now that the scam is reported, you can begin to repair the damage.

If you suspect you've become a victim of fraud, please follow our checklist to help fix your credit and limit the damage to your account(s).

- Call 781-444-2100 or your local Needham Bank branch to let us know that you've been a victim of fraud
- Contact other financial institutions with which you do business
- Contact all three credit bureaus to place a fraud alert or credit freeze on your credit report:

Equifax: 800-349-9960, [Equifax.com/personal/contact-us](https://www.equifax.com/personal/contact-us)

Experian: 888-397-3742, [Experian.com/help](https://www.experian.com/help)

TransUnion: 888-909-8872, [Transunion.com/customer-support](https://www.transunion.com/customer-support)

Fraud alerts and credit freezes are both free, however, they have different functions. When you have a fraud alert on your report, businesses must verify your identity before issuing new credit in your name. When you have a credit freeze on your report, access to your credit report is blocked and you cannot apply for new credit unless the freeze is lifted.

- Submit your case to the Federal Trade Commission (FTC)
FTC: 877-382-4357, [Reportfraud.ftc.gov](https://www.reportfraud.ftc.gov)
- Contact your local police or sheriff's office to report the fraudulent activity

-
- Close any accounts that were opened in your name
 - Remove any fraudulent charges from your account
 - Correct your credit report

FRAUD RECOVERY CHECKLIST

POTENTIAL STEPS

Depending on the type of fraud, there might be additional steps you will need to take.

- Get your electronic devices professionally wiped by a reputable company
 - Replace government-issued IDs
 - Clear your name of criminal charges
-

BEST PRACTICES

Follow these steps consistently to keep your accounts safe.

- Login to online or mobile banking to monitor your accounts and set up alerts to monitor your balances and detect large withdrawals, large deposits and when a check clears your account
- Review your credit reports regularly
- Use unique passwords that are hard to guess for each account you have
- Visit secure websites that have the “https” in the web address
- Confirm email requests via phone prior to making any transactions
- Avoid clicking on a link or opening an attachment within an email or text message unless it's from a known source
- Keep your computers up to date by having automatic updates activated and turning your computer off each night so updates occur
- Learn more by visiting these additional resources:

Federal Trade Commission: Reportfraud.ftc.gov

Federal Bureau of Investigation: FBI.gov/scams-and-safety

Consumer Financial Protection Bureau:
Consumerfinance.gov/fraud