FRAUD RECOVERY CHECKLIST

The steps below can help guide you through the recovery process. Depending on the type of fraud involved, some steps may not apply to your situation.

First Steps

If you notice suspicious activity or realize you may have fallen victim to a scam, try to remain calm and act quickly.

Keep detailed records of all interactions, including:

- Names
- Dates / Times
- Phone numbers
- Summaries of conversations

Fraud Alerts vs. Credit Freezes

- **Fraud Alert:** Businesses must verify your identity before issuing credit in your name.
- **Credit Freeze:** Blocks access to your credit report so new credit cannot be opened unless the freeze is lifted.

Both are free and can help protect your credit.

Report the Fraud

Notify the appropriate organizations as soon as possible.

- ☐ **Contact BankNorth**
  Call **877-847-4540** or contact your local branch directly to report the fraudulent activity.
- ☐ **Notify other financial institutions**
  Contact the fraud departments at any banks or financial institutions where your accounts may have been compromised.
- ☐ **Place a fraud alert or credit freeze with the credit bureaus**
  Equifax: 888-378-4329 or Equifax.com/personal/contact-us
  Experian: 888-397-3742 or Experian.com/help
  TransUnion: 800-680-7289 or Transunion.com/customer-support
- ☐ **Report the incident to the Federal Trade Commission (FTC)**
  Call **877-382-4357** or Reportfraud.ftc.gov
- ☐ **File a report with your local police or sheriff's office**
  Provide as much detail as possible, including screenshots, emails, text messages, and other evidence. Be sure to request a copy of the report and case number.
- ☐ **Contact the Internal Revenue Service (IRS)** *(if your identity was stolen)*
  IRS.gov/identity-theft-central

Secure and Repair Your Accounts

Now that the scam has been reported, you can start fixing any impact the fraudulent activity may have caused.

- ☐ Change affected bank account numbers, credit cards, or debit cards.
- ☐ Review and correct your credit reports by disputing any fraudulent activity with the credit bureau(s) reporting the error.
- ☐ Close fraudulent accounts that were opened in your name.

BANKNORTH

Fraud Recovery Checklist | Next STEPS & Ongoing Protection

Helpful Resources

Federal Trade Commission:
Reportfraud.ftc.gov

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

Consumer Financial Protection Bureau:
Consumerfinance.gov/fraud

Identity Theft Resource Center:
IDtheftcenter.org

Tips for Managing Your Case

- **Send correspondence** by certified mail with return receipt requested.
- **Keep copies** of all documents and communications related to your case.
- **Track any expenses** related to resolving the fraud (postage, photocopies, etc.)

Additional Steps That May Be Necessary

Notify the appropriate organizations as soon as possible.

- ☐ Have your **electronic devices professionally cleaned or wiped** by a reputable company if malware or hacking is suspected
- ☐ **Reset all passwords** for online banking, financial apps, email accounts and any accounts linked to your financial information.
- ☐ **Reconnect accounts** to services such as digital wallets, bill pay, or payment apps.
- ☐ **Replace lost or compromised government-issued ID's.**
- ☐ **Contact creditors** where fraudulent accounts were opened. Inform them that you are a victim of identity theft and request the account(s) be "closed at consumer's request."

  Important: Request written confirmation that the account has been closed and will be removed from your credit report.

  You may be asked to submit a Fraud Affidavit (IRS Form 14039) available at: www.irs.gov

Best Practices for Ongoing Protection

Once your accounts are secured, these habits can help reduce the risk of future fraud.

- ☑ Monitor your accounts regularly through **online or mobile banking.**
- ☑ Set up **account alerts** for large withdrawals, deposits, and check activity, and always confirm the payee on cleared checks.
- ☑ Review your credit report regularly at: www.annualcreditreport.com
- ☑ Use **unique, strong passwords** for financial accounts.
- ☑ Only visit **secure websites** that begin with https://
- ☑ Be cautious of suspicious texts, emails, and links.
- ☑ Keep your **computer and devices up to date** with automatic software updates to help protect against security threats.

When In Doubt - Reach Out

At BankNorth, protecting your accounts and personal information is our top priority. If you ever notice suspicious activity, contact us right away — we're here to help.

BANKNORTH