Middlesex Savings Bank®
right there with you

FRAUD AND IDENTITY THEFT

Resource and Information Guide

Middlesex Savings Bank®

TAKING ACTION
Fraud and identity theft recovery checklist

01

STEP 1: NOTIFY THE RELEVANT BANKS

- ☐ Get in touch with your banks immediately to alert them.
- ☐ Dispute the activity you believe to be fraudulent.

02

STEP 2: NOTIFY THE CREDIT BUREAUS

- ☐ Obtain credit reports from the three credit bureaus to look for fraud. Notify all credit bureaus to investigate and resolve.
- ☐ Consider adding a credit freeze or alert.

03

STEP 3: FILE A COMPLAINT WITH THE FEDERAL TRADE COMMISSION

- ☐ Go to their website, identitytheft.gov, to file a report and get a recovery plan.

04

STEP 4: SUBMIT YOUR CASE TO THE INTERNET CRIMES COMPLAINT CENTER (IC3) IF CYBER/CRYPTO-RELATED.

- ☐ File an Internet Crimes Complaint Center (IC3) Report at www.IC3.gov.

05

STEP 5: REACH OUT TO LOCAL LAW ENFORCEMENT.

- ☐ Provide all information you can (dates, times, and account numbers).
- ☐ File a police report.
- ☐ Save a copy of the police report for financial institutions or agencies that may require it.

FRAUD AND IDENTITY THEFT
Resource and Information Guide

Middlesex Savings Bank®

Are you experiencing fraud or identity theft? We're here to guide you through the next steps.

We understand that identity theft can be a deeply unsettling and overwhelming experience. If you suspect that your personal information has been compromised, we're here to support you. It's crucial to act quickly to minimize any potential harm, and this guide is designed to walk you through the steps needed to protect yourself and your finances.

Where to begin:

Step 1 Immediately notify any financial institution, card issuer or company where fraudulent transactions have occurred.

WHAT TO DO:

- ☐ Determine which charges are fraudulent and then call your bank or credit card company's fraud department to report unauthorized charges and request confirmation in writing. If it's a credit or debit card account, ask for a new card with new numbers.
- ☐ Report lost or stolen identification, checks, debit/credit cards, fraudulent transactions, and unauthorized account activity.
- ☐ Request to close compromised accounts and open new ones with different account numbers*
- ☐ Change passwords, PIN numbers, or any other credentials as applicable.
- ☐ Set up enhanced security features such as transaction alerts.
- ☐ Update any digital wallets or bill pay providers.
- ☐ Identity theft or fraud may be covered by your homeowners insurance policy. If it's not, then you might want to ask your insurance agent about any possible endorsements.

Middlesex Savings Bank®

TIPS:

- Utilize the tracking sheet in this packet to maintain a written record of whom you contacted and when. Also, keep any confirmation letters from banks or businesses since you may need them to dispute credit report discrepancies.
- Make sure you understand if your bank, credit card company, or payee holds you responsible for any unauthorized charges.
- Don't forget to notify utilities, insurance and other auto-pay companies attached to the compromised account(s).
- Be prepared to complete a dispute form at your bank or credit card company's request, as well as send them copies of federal or law enforcement reports.
- Get your electronic devices professionally scrubbed by a reputable company.

WHEN CLOSING ANY BANK ACCOUNTS OR DEBIT/CREDIT CARDS:

1. Provide a list of any outstanding checks or pre-authorized payments as applicable.
2. Any automatic deposits or withdrawals will need to be switched to the new account number. Notify each company of your new account information.
3. Date Compromised Account Should Be Closed By: _____
   Affected accounts are typically closed within 90 days of the reported fraud.

Step 2 Report ID theft to credit reporting agencies.

- Equifax: 888-766-0008, Equifax.com/personal/contact-us
- Experian: 888-397-3742, Experian.com/help
- TransUnion: 888-909-8872, Transunion.com/customer-support

WHAT TO SAY:

- Tell them your identity has been stolen.
- Add a short-term fraud alert if you're planning on applying for a new mortgage, car loan, student loan or other type of credit in the near future.
- Add a stronger, longer-term credit freeze if you won't be applying for new credit soon.
- Ask for a FREE copy of your credit report and review it carefully.
- Most credit bureaus will give you a free copy when you place or renew a fraud alert.
- If you add an alert, you may be opted out of receiving pre-approved credit card and insurance offers.
- When you receive a report, make note of the unique number assigned to you since you may need it later when communicating with the credit bureau.

TIPS:

- You can request a copy of your credit report at no cost to you once each year by visiting the government-approved website AnnualCreditReport.com. You're entitled to a free credit report from each of the three major credit reporting agencies every year, too. Since you have three reports available to you each year, mark your calendar to request one report every four months.

FRAUD ALERT VS CREDIT FREEZE.

Fraud Alert: With a fraud alert, businesses must verify your identity before issuing new credit in your name.

Consumers only need to contact one of the three major credit reporting agencies by phone or through their website. The law requires that the credit reporting agency notify the other two when a consumer requests a fraud alert. A fraud alert is available at no charge.

How long does it last? An initial fraud alert will be active for 90 days, but it could be renewed for another 90 days after the first alert expires. You also have the option to apply for an extended fraud alert that will last for seven years.

Credit Freeze: With a credit freeze, access to your credit report is blocked and you must contact the credit bureaus to lift the freeze to apply for new credit.

To place a credit freeze, you must contact each of the three credit reporting agencies separately at the companies' credit freeze websites. A freeze might be free, depending on your state and circumstances.

How long does it last? If you place a credit freeze, you'll get a PIN number to use each time you want to freeze, unfreeze and refreeze the account. In almost all states, a credit freeze lasts until you temporarily lift it or permanently remove it.

Step 3 File a complaint with the Federal Trade Commission.

File an FTC Identity Theft Report online at www.identitytheft.gov or by phone at 1-877-ID-THEFT (438-4338).

Date reported: _____

FTC Report ID: _____

Step 4 Submit your case to the Internet Crimes Complaint Center (IC3) if cyber/crypto-related.

File an Internet Crimes Complaint Center(IC3) Report at www.IC3.gov.

Date reported: _____

IC3 Report ID: _____

TIPS:

- What information should I provide? The most important information you can provide are transaction details. Transaction details include cryptocurrency addresses, amount and type of cryptocurrency, date and time, and transaction ID (hash). These unique identifiers vary in length and look like long strings of random letters and numbers.
- What other information should I provide? Provide any other information you may have about the scam : where and how you encountered the scammer, your communications with the scammer (for example, emails or texts) and associated identifiers such as names, e-mail addresses, and phone numbers, what domain names, website addresses, or applications the scammer instructed you to use, any two-factor authentication or "one time passcode" information, which cryptocurrency exchanges you used to send or receive funds, the timeline of the scam.
- What if I do not have transaction information? If you do not have transaction information, still submit a report and provide as much information as you have.

Step 5 Make a report with local law enforcement. File a sworn statement to help protect yourself.

HERE'S WHAT YOU'LL NEED:

- ☐ A copy of your Federal Trade Commission (FTC) Identity Theft Report.
- ☐ A government-issued photo ID (driver's license, passport, U.S. military ID).
- ☐ Proof of address (mortgage statement, rental agreement, utility bill).
- ☐ Evidence of the theft (credit card statements showing fraudulent transactions, credit reports, collection letters)

TIPS:

- Ask for a copy of the report to keep for your records.
- You may need to provide copies of this report to credit agencies or creditors.
- If local law enforcement is unable to take your report as an identity theft report, file it as a miscellaneous incident report.
- If you have trouble filing a report, contact your state Attorney General's office.

City or town police department: _____

Date reported: _____

Case number: _____

FRAUD AND IDENTITY THEFT
Resource and Information Guide

Middlesex Savings Bank®

Whether you've been a victim of identity theft, fraud, phishing or other financial crime, we hope this information can help you recover and rebuild, and protect you from future harm.

ADDITIONAL RESOURCES

- Visit our fraud resource center: www.middlesexbank.com
- Federal Trade Commission: reportfraud.ftc.gov
- Federal Bureau of Investigation: FBI.gov/scams-and-safety
- Consumer Financial Protection Bureau: Consumerfinance.gov/fraud

You can always count on us to be right there with you.

BRANCH LOCATIONS

Acton
Ashland
Bedford
Bellingham
Boxborough
Concord
West Concord
Framingham, Nobscot
Framingham, Route 9
Franklin
Groton
Holliston
Hopkinton
Hudson
Littleton
Maynard Crossing
Maynard, Powdermill
Medfield
Medway
Millis
Natick
Needham
Sherborn
Southborough
Sudbury
Walpole
Wayland
Wayland Center
Wellesley
Westborough
Westford
Worcester

Find your closest branch.

Schedule an appointment.

Log in to your account and send us a secure message.

1.877.463.6287

BEST PRACTICES

Follow these steps consistently to help keep your accounts safe.

- Monitor your accounts regularly through online and mobile banking and set up alerts to watch your balances and notify you about transactions clearing your accounts.
- Don't share personal information online such as your address, phone numbers, social security number, birth date, or birth place.
- Store sensitive personal and financial documents in a secure location, and shred them prior to disposal.
- Review your credit reports regularly.
- Avoid clicking on a link or opening an attachment within an email, text message, or pop up screen unless it's from a known source.
- Keep your electronic devices up to date by having automatic updates activated.
- If unsure of a caller asking for information, hang up and call them back at a trusted phone number (such as on the back of a credit/debit card or from the company's website, not from a google search).