

Protecting Your Finances

A Guide to Fraud,
Identity Theft, and
Account Security



Introduction

Imagine someone drains your bank account, opens a credit card in your name, or files your taxes to get your refund – all without ever meeting you.

That's not a worst-case scenario. It happens more often than you'd think.

The good news is that most fraud is preventable. And you don't have to be a tech expert to protect yourself. You just need to know what to look for and what to do if something doesn't feel right.

Contents

- 02** How Fraud Happens Today
- 04** Understanding Identity Theft
- 06** Security Basics Everyone Should Use
- 08** Common Scams to Watch For
- 10** What to Do If Something Goes Wrong
- 11** How Financial Institutions Protect You
- 12** Final Thoughts

01 How Fraud Happens Today

Most financial fraud doesn't involve a hacker breaking into a system. It involves a scammer convincing you to let them in.

It often looks like this:

- A text arrives that looks like it's from us and other financial institutions you work with.
- A call comes in from what appears to be a government agency.
- An email tells you there's been suspicious activity on your account and you need to act now.



These messages are designed to feel real and create urgency – so you act before you have time to think it through.

How Fraud Usually Happens

- 1 Your information is already out there.** Data breaches happen constantly. Even companies you've trusted for years can be compromised, and your name, email, or account details can end up in the wrong hands without you doing anything wrong.
- 2 You're convinced to do something.** This could be clicking a link, sharing a code, or approving a transfer. Fraudsters are skilled at creating situations that feel legitimate and urgent. Once you act, they move fast.
- 3 They get into your account.** Once a scammer has enough of your information, getting into your accounts can be surprisingly easy. And when they do, they don't waste time.

How Criminals Find Your Information

- ✓ Data breaches from businesses you've used
- ✓ Phishing emails or fake websites that look like the real thing
- ✓ Information you've shared publicly on social media
- ✓ Malware installed through unsafe downloads or links

What Scammers Do Once They Have It

- ✓ Log in to your accounts
- ✓ Reset your passwords to lock you out
- ✓ Open new accounts or apply for loans in your name
- ✓ Transfer or spend your money before you notice



THE BOTTOM LINE

Fraud today is less about breaking in and more about being let in.
Awareness is one of the simplest and most effective ways to protect yourself.

What to Do Next

- ✓ Avoid clicking links in unexpected messages; go directly to the source instead.
- ✓ Use official apps and websites rather than following links from texts or emails.
- ✓ Pause when something feels urgent – that pressure is often the warning sign.
- ✓ Check your accounts regularly so you catch anything unusual early.

02 Understanding Identity Theft

Most people think of identity theft as something dramatic, like a stranger pretending to be you, living a double life. The reality is a lot quieter, and that's what makes it so frustrating.

Identity theft is when someone uses your personal information as if they were you. This could mean using your Social Security number, date of birth, or address to open an account, get a loan, or make purchases. You might not find out for weeks or months. By the time you do, there may already be damage to sort through.

What Identity Theft Could Look Like

- ✓ A credit card that you never applied for shows up on your credit report.
- ✓ You get a bill for a loan you didn't take out.
- ✓ Charges appear on an account you haven't used recently.
- ✓ The IRS tells you a tax return has already been filed in your name.

Types of Identity Theft

Account takeover. A criminal gets into an account you already have – your bank account, a credit card, even a streaming service – and changes the credentials to lock you out.

Tax identity theft. Someone files a tax return in your name to grab your refund before you do. You often find out only when the IRS rejects the real return you tried to file.

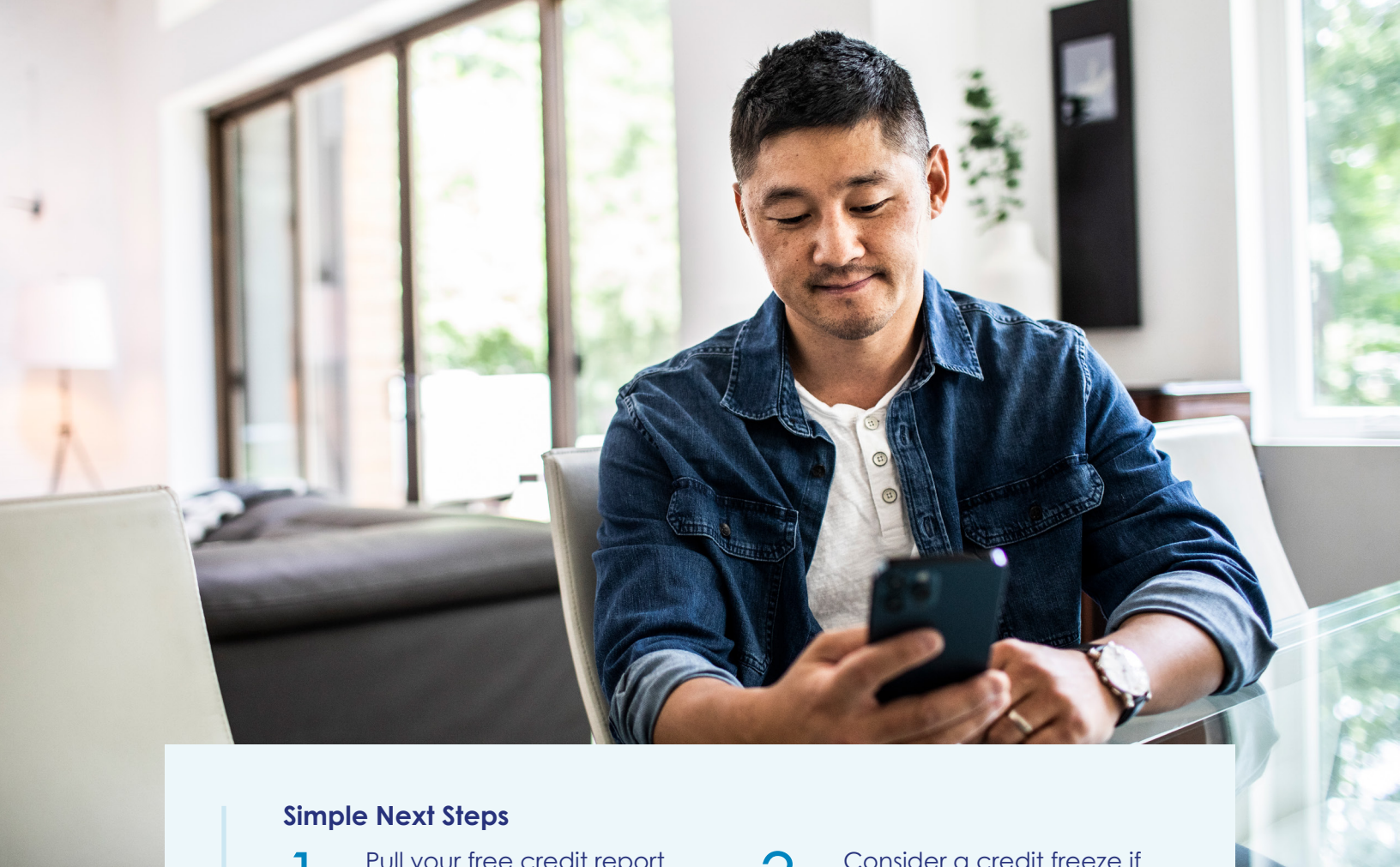
Personal identity theft. Your information is used for non-financial purposes – to get medical care, apply for a job, or collect government benefits in your name.

New account fraud. Someone uses your personal details to apply for new credit cards, loans, or lines of credit. This one can be especially damaging because it can take a while to show up.



WHY FRAUD IS SO HARD TO CATCH

Most fraud happens in the background. You won't always get a notification that says, "Hey, someone just applied for a credit card using your information." **That's why staying aware and checking in regularly matters.**



Simple Next Steps

- 1** Pull your free credit report at [AnnualCreditReport.com](https://www.annualcreditreport.com) at least once a year and look for anything unfamiliar.
- 2** Turn on account alerts so you're notified of activity as it happens.
- 3** Consider a credit freeze if you're not actively applying for new credit. It's free and effective.
- 4** Review your statements regularly, even if everything seems fine.

03 Security Basics Everyone Should Use

You don't need to overhaul your entire digital life to protect yourself. A handful of consistent habits go a long way – and most of them take just a few minutes to set up.

FIVE TIPS FOR BETTER SECURITY



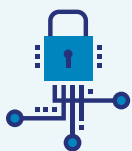
Strong, unique passwords. Reusing passwords is one of the most common ways accounts get compromised. If one account gets breached, every account with the same password becomes vulnerable. Use a different password for each account and find a password manager to keep track of them.



Multifactor authentication (MFA). When MFA is turned on, logging in requires something beyond just your password, like a code sent to your phone. Even if someone gets your password, they won't get into your account without completing that second step.



Account alerts. Turn on notifications to get account alerts for transactions, logins, and account changes. A real-time alert is often the fastest way to catch something suspicious.



Secure connections. Public Wi-Fi is convenient, but it's not safe for anything sensitive. Avoid logging in to financial accounts on public networks – only use a trusted home connection.



Device protection. Software updates often include security patches for newly discovered vulnerabilities. Keep your phone and computer updated and use a lock screen for an extra layer of protection.

DO'S AND DON'TS

DO

- ✓ Use different passwords for each account.
- ✓ Enable MFA.
- ✓ Turn on alerts.
- ✓ Keep devices locked and updated.

DON'T

- ✗ Reuse passwords.
- ✗ Share login credentials or one-time codes with anyone.
- ✗ Ignore unfamiliar activity.
- ✗ Access financial accounts on public Wi-Fi.

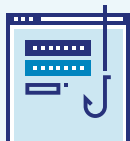
Quick Ways to Protect Yourself

- ✓ Update any weak or reused passwords, starting with your most important accounts.
- ✓ Enable MFA on your checking account, email, and other financial accounts.
- ✓ Turn on transaction and login alerts through our app or website.
- ✓ Check your security settings, as many accounts have protections that aren't turned on yet.

04 Common Scams to Watch For

Scammers are creative, and their tactics are always evolving. But if you look closely, most scams follow the same basic playbook. Once you recognize the patterns, they're much easier to spot.

FOUR TYPES OF SCAMS



Phishing (email and text). You get a message that appears to come from us, another financial institution, a retailer, or a government agency.



Spoofing. A call comes in from a number you recognize, but the caller ID has been faked. The caller claims there's fraud on your account and asks you to confirm some details to "secure" it. This is the scam.



Impersonation scams. Someone poses as us, a government agency, or a company you use.



Payment scams. You're asked to send money quickly, usually through a wire transfer, payment app, or gift cards. Scammers like these methods because they're fast and hard to reverse.

Red Flags

- ✓ Language that feels urgent or threatening
- ✓ Requests for personal information, passwords, or verification codes
- ✓ Pressure to act right now, without time to think or verify
- ✓ Links that look slightly off or don't match the company's official website
- ✓ Any request to pay with gift cards (no legitimate organization ever asks for this)



Remember: We'll never call or text you to ask for your password, a one-time verification code, or your full account number. If someone asks for any of those, that's your cue to hang up and call us directly using the number on the back of your card.

Protect Yourself in the Moment

- 1** When something feels off, take a step back. Urgency is a tactic, not a reason to act.
- 2** Verify any unexpected requests by contacting the company directly through official channels, instead of replying or clicking through to a link.
- 3** Never send money under pressure, especially via wire transfer, app, or gift card.
- 4** Report anything suspicious to us right away.

05 What to Do If Something Goes Wrong

Even when you do everything right, fraud can still happen. If it does, the most important thing is to act quickly.

If You Suspect Fraud

- ✓ Contact us immediately, or any financial institution where the fraud occurred. You can find our phone numbers and branch hours at [ridgewoodbank.com/home/contact-us/locations-hours](https://www.ridgewoodbank.com/home/contact-us/locations-hours).
- ✓ Ask to lock or freeze the affected accounts right away.
- ✓ Change your passwords – starting with the affected account and any others sharing it.
- ✓ Review your recent transactions and flag any you don't recognize.

If Identity Theft Occurs

- ✓ Place a fraud alert or free credit freeze with all three major credit bureaus – Equifax, Experian, and TransUnion – as well as other credit reporting companies, like ChexSystems. A freeze prevents most new accounts from being opened in your name.
- ✓ Visit [IdentityTheft.gov](https://www.identitytheft.gov), a free resource run by the Federal Trade Commission that walks you through a personalized recovery plan, step by step.
- ✓ Document everything during the process, including who you spoke with, when you called, what was said, and what actions were taken.
- ✓ Monitor your accounts and credit closely, even after the issue seems resolved.



Fraud is stressful, but it's also something millions of people recover from every year. You're not on your own here. The sooner you reach out, the sooner you can get the help you need.

Stay One Step Ahead

1. Save our contact information, available at [ridgewoodbank.com/home/contact-us/locations-hours](https://www.ridgewoodbank.com/home/contact-us/locations-hours).
2. Learn how to quickly lock your accounts.
3. Report anything that looks suspicious and let the experts help you assess it.
4. Watch your account in the days following any suspicious activity.

06 How Financial Institutions Protect You

Financial institutions work continuously to help keep your money safe. Your transactions are monitored around the clock, and systems are in place to flag unusual activity. In some cases, issues are identified before you even notice them.

What's Happening Behind the Scenes

- ✓ Fraud monitoring systems analyze transactions in real time and flag anything that looks out of place.
- ✓ Identity verification tools confirm it's really you before allowing account changes.
- ✓ Secure login technology uses encryption and biometric access to help protect your accounts.
- ✓ Transaction and login alerts notify you of activity as soon as it happens.



Keep in mind: Security is a partnership. Alerts only help if you see them, and a flagged transaction is easy to miss if your contact information is outdated or your notifications are turned off. A few minutes spent on your settings can make a real difference.

Next Steps to Take

- ✓ Review your notification settings and turn on all available alerts.
- ✓ Download the official app, which is the most secure way to access your account.
- ✓ Ask what fraud protection tools are available and make sure you're using them.
- ✓ Keep your contact information current so you can be reached quickly if needed.

Final Thoughts

Protecting your finances doesn't require perfection – just awareness and a few good habits.

Most fraud relies on people being busy, distracted, or caught off guard. When you know what to look for and take a few simple steps to protect yourself, you become a much harder target.

The goal isn't to live in fear. It's to feel confident and prepared. Understanding the risks, how to respond, and what's already in place to protect you helps take the uncertainty out of it.



Stay aware, slow down when something feels urgent,
monitor your accounts, and use the tools available to you.

We're Here to Help

Have questions or want to take the next step to better protect your accounts? Reach out today or explore our security tools and resources in our Security Center at ridgewoodbank.com/home/contact-us/security.



ridgewoodbank.com



This guide is prepared by a third party. Ridgewood Savings Bank is not responsible for the content in the guide. This guide is provided for informational purposes only and is not intended to provide specific advice or recommendations to any individual. The information is subject to change and may not be applicable to your personal situation. Links to third-party articles and/or websites are for general information purposes only.