PROTECTING YOURSELF AGAINST FRAUD

A guide on keeping your finances safe
(and what to do if they're compromised)

Fulton Bank

TABLE OF CONTENTS

Scammers are constantly evolving their tactics and finding new ways to target potential victims. Fortunately, there are ways you can stay a step ahead. But if you find you are a victim of fraud, there are things you can do to minimize the impact.

10 WAYS TO
SAFEGUARD YOUR PRIVATE INFORMATION

Six hours. That's how much time the average person spends online each day. While you're shopping, using social media, or streaming a favorite video, you may be unknowingly giving cyber criminals the opportunity to steal your personal information. If they get their hands on personal data, the crimes that an identity thief is able to commit include: Applying for a credit card, poaching your tax refund, or selling your information.

According to Internet Security Threat Report by Symantec, cybercriminals are diversifying their targets and using a variety of methods like formjacking (the use of malicious code to steal credit card details and payment forms on the checkout web pages) and fraudulent emails posing as invoices or receipts to commit identity theft and fraud. Typically, they look for:

- **Usernames**
- **Passwords**
- **Date of birth**
- **Social Security number**
- **Bank account numbers**
- **Driver's license number**
- **Credit/debit card numbers**
- **Home address**
- **Cell phone number**
- **Answers to common security questions, like your father or mother's birth name, favorite color, or the street where you grew up**

1 MAKE SURE YOUR DEVICES ARE UP TO DATE.

For your financial security, it's important to keep your computers, tablets, and phones up to date. Install the latest operating system and security software for your device. Don't jailbreak or root your mobile device to work around limitations set by your carrier or device manufacturer because it will remove important protections.

2 CREATE STRONG PASSWORDS

Choose passwords for your financial accounts that include a combination of upper- and lowercase letters, numbers, and special characters. Don't use the same password for every account. You may be required to set them periodically, but it's a good security habit to update them every three to six months. If you have your web browser remember passwords, you can review those through your browser settings.

3 OPT IN FOR ALERTS TO TRACK ACCOUNT ACTIVITY.

Set up email and text alerts for your bank and credit card accounts to notify you of new transactions, including debits, credits, and transfers. This is an easy way to monitor your accounts without having to log in to check them.

4 BE SOCIAL MEDIA SAVVY

Your social media accounts can provide clues about your personal information that cyber thieves can use to unlock your financial information, such as your zip code, date of birth, or your mother's maiden name. Set your account to private, only connect with people you know, and be selective about the personal information you share with your followers.

5 AVOID SCAMMERS IN YOUR INBOX

Scammers often use email phishing scams to steal personal and financial information. If a suspicious email lands in your inbox, don't click on any links or reply to it, even if it comes from someone in your contact list. Report any suspicious emails as spam to your email provider and block the sender for good measure

6 REVIEW STATEMENTS, CREDIT REPORTS REGULARLY

Check your financial statements each month to make sure your transaction history is correct, and there are no suspicious purchases or credits. Review your credit report at least once a year for potential signs of identity theft, such as unfamiliar new accounts or credit inquiries.

7 STICK WITH SECURE WI-FI

Public Wi-Fi is convenient when you're on the go, but those networks aren't always secure. Anyone might be able to see the personal or financial information you send. A safer option is to travel with a password-protected mobile hotspot, or tether your laptop to your smartphone and use your phone's mobile data to go online. If you do use public Wi-Fi, avoid accessing websites that could expose your personal or financial information.

8 INSTALL ANTIVIRUS AND ANTI-MALWARE

Online criminals can peek at your personal and financial information using viruses and malware on websites, emails, and apps. By installing antivirus, anti-malware, and anti-spyware software on all your devices, you make it more difficult for someone to remotely install information-stealing files.

9 NEVER GIVE PERSONAL DATA OVER THE PHONE

When you get a call from a company or number you don't recognize, do not give your personal information. Don't engage with the scammer; simply hang up and dial the customer service number of the company to determine if the call you received is legitimate.

10 BE SELECTIVE ABOUT APPS

There's an app for just about anything these days, but not all of them are safe. Before downloading any app, especially those you can link to your financial accounts like a shopping or coupon app, read the fine print to make sure it's from a trusted source.

TIPS ON HOW TO
PREVENT CREDIT CARD FRAUD

Sometimes it's barely noticeable. You're scanning your credit card statement and you see a purchase in a city you've never visited. You may begin to notice additional charges from distant stores or unfamiliar online purchases. Chances are, you could be a victim of credit card fraud.

Maybe this has already happened to you. After all, more than 167,000 people filed reports with the U.S. Federal Trade Commission in 2018 claiming they were targeted by credit card fraudsters. With EMV chip technology protecting credit cards at physical locations, thieves are committing more of their crimes online. Illegal credit card account creation, the number one kind of identity theft, was up 24% in 2018 over the previous year. Data breaches are climbing as well: High-profile breaches at Capital One, Equifax, and Target were just a few of the recent ways fraudsters captured consumers' personal information.

If your credit card or account details are compromised, follow these tips on what you need to do, as well as how to help prevent fraud from happening in the first place.

1 LOOK BEFORE YOU ENTER YOUR INFORMATION

Before you enter your personal information, such as a Social Security number, into a website, make sure the site's URL begins with "https" rather than "http," or look for the icon of a closed padlock at the top or bottom of the browser.

2 DON'T SHARE PERSONAL DATA IN AN UNSECURED EMAIL/TEXT

Never put your personal or credit card information in an email or text message. If someone emails you with a request for updated card information, be wary: It could be a classic phishing scam. Call the company to verify if the request is legitimate.

3 EXAMINE CARD READERS AND LOOK FOR SIGNS OF TAMPERING

Check for obvious signs of tampering on the card reader—different colors or materials, or graphics that seem out of place.

4 COVER ANY VIEWS WHEN YOU INPUT PIN NUMBERS

Use your hands to cover any views when you input your pin number. Assume someone is always looking.

5 SET UP ALERTS TO MONITOR CARD ACTIVITY

You can customize alerts to monitor card transactions, so you can immediately catch unexpected purchases.

6 DON'T PROVIDE INFORMATION OVER THE PHONE

Never give your personal information over the phone unless you initiated the request.

7 CHANGE YOUR PASSWORDS REGULARLY

Create strong passwords with letters, numbers, and symbols—and change them at regular intervals.

STEPS TO TAKE IF YOUR PERSONAL DATA IS COMPROMISED ONLINE

Unfortunately, data breaches have become a common feature of modern life in our always-connected world of online services; everyone in the U.S. is at risk of having their data stolen. However, even if your data is compromised in a data breach, you don't have to become a victim. There are several steps you can take to contain the damage and keep your personal finances, credit score, and identity safe from criminals.

If you find out that a company you do business with—or an online service that you use—has suffered a data breach, here are a few steps to take right away:

1 CHANGE ALL YOUR PASSWORDS.

It's a good idea to keep changing your password on a regular basis, but in the aftermath of a data breach, it's especially important to change your passwords to something strong, secure, and unique. And you should have multiple passwords, not just one. Do not use the same password for all of your online accounts. In general, a strong password is at least eight characters with a mixture of letters, numbers, and symbols. Consider using a password manager to help generate and keep track of your passwords.

2 SIGN UP FOR TWO-FACTOR AUTHENTICATION

In addition to changing your passwords, sign up for two-factor authentication (also known as "2FA" or "two-step verification") wherever possible. This is an added layer of security for your account logins, and many services such as Gmail and Facebook now offer it. With two-factor authentication, your online account will require you to enter an additional level of identification to access your account—such as a code texted to your phone. This means that even if hackers get your email and password, they can't get into your account without that second factor of identity verification.

3 CHECK FOR UPDATES FROM THE COMPANY

If your data is involved in a major data breach, the company will likely post ongoing updates and disclosures about which customers were affected. For example, after a recent Facebook data breach, the company automatically logged out the users whose accounts were affected and sent them messages via the platform about what had happened and what to do next. After the Equifax data breach, the Federal Trade Commission (FTC) offered a series of advisories and steps that people could take to protect themselves.

4 WATCH YOUR ACCOUNTS, CHECK YOUR CREDIT REPORTS

After a data breach, it's essential to be vigilant and pay extra attention to your account activity—that includes your account at the company that suffered the breach, as well as your bank account and other financial accounts. Read your credit card statements and watch for suspicious transactions. Also, sign up for your free annual credit report to check your credit reports from each of the three credit reporting bureaus.

5 CONSIDER IDENTITY THEFT PROTECTION SERVICES

If you want additional peace of mind, you can consider signing up for identity theft protection services. However, these services are not cheap, and you can do many of the actions yourself. Often when there is a significant data breach, the company involved will give affected customers a free year of credit monitoring.

6 GO TO IDENTITYTHEFT.GOV

If you are affected by a data breach, there is a government website that can help you assess the situation and understand your options for what to do next. There are a variety of resources with tips and advice on what to do if your personal information was lost or stolen.

Being affected by a data breach can be alarming, and in the worst-case scenario, it can lead to identity theft and financial complications. But if you know what to expect, and you take a few simple steps to protect yourself and stay vigilant, you can overcome the risks and hassles of a data breach.

7 FREEZE YOUR CREDIT

Another step you can take, whether you're affected by a data breach or not, is to freeze your credit. You can do this by contacting each of the three credit bureaus (Equifax, Experian, and TransUnion) and asking to freeze your credit. There is no cost to freeze your credit, and it will prevent any new credit accounts from being opened in your name. Even if identity thieves have access to all of your personal data, they can't open new accounts under your name if your credit is frozen. The only drawback of freezing your credit is that it prevents you from applying for new credit too—so don't do it if you are expecting to need a new car loan, home loan, or credit card account. You can un-freeze your credit at any time.

CHECKLIST FOR RESPONDING TO FRAUD OR IDENTITY THEFT

Once you realize that you are a victim of fraud, review the following tips and procedures to help resolve any issues with your creditors, remove inaccurate information from your credit report, and prevent any further fraud.

☐ **First, contact your bank, financial institution, or companies where the fraud occurred.**
Part of this step may include closing or freezing your accounts that have been compromised.

If available, have your bank or credit card statement (online or paper) to discuss the dates and amounts of the breach.

Notes: _____

☐ **Change your password for the compromised site.** If they allow you to change your username, do that as well.

For an added measure of security, change the passwords for other sites—especially if you are using the same username as the compromised site.

Notes: _____

☐ **Change your security questions, too (if applicable).**

Notes: _____

☐ **Review your other credit card and bank accounts to check for unauthorized transactions.**

When reviewing your transactions, look for both big dollar amounts and smaller amounts that may appear more than once.

Notes: _____

☐ **Contact at least one of the three major credit reporting agencies: Equifax (www.equifax.com • 1-888-548-7878), Experian (www.experian.com • 1-888-397-3742), or TransUnion (www.transunion.com • 1-800-916-8800).**
The agency you contact is required to contact the other two and share information.

After placing the initial fraud alert, you can request a free copy of your credit report from each credit reporting agency. We recommend checking all three reports to help ensure you're not missing anything important – because each agency's report may be different.

Notes: _____

☐ **Contact the IRS to make sure you aren't the victim of tax-related identity theft.** A fraudster with a combination of your name, date of birth, and Social Security number could file a tax return in your name, hoping to receive a refund.

Notes: _____

☐ **Alert your health insurance company and medical care providers.** If you're a victim of identity theft, you may also want to contact your medical care providers to ensure that your identity isn't being used to receive healthcare or pharmacy services in your name.

Notes: _____

CHARITABLE DONATIONS:
4 TIPS FOR SAFE GIVING

It's important to ensure that your donated dollars are going to the right place and being used appropriately. Use these four tips to help tell the difference between a reputable organization or a fraudster.

1 RESEARCH YOUR CHARITY'S REPUTATION

Technology has made it very easy for scammers to create sophisticated websites, launch robocall campaigns, and troll for dollars via text message or social media. **Before donating money, spend some time researching the organization to ensure it's authentic.**

- Look up the charity on a government or watchdog site like the Better Business Bureau (BBB) Wise Giving Alliance, Charity Navigator, Charity Watch, or GuideStar. Be cautious if a charity isn't listed, but also know that a non-rating isn't necessarily an indicator of fraud. To vet these entities, Charity Navigator suggests asking for the nonprofit's IRS-issued employer identification number (every organization should have one) and then reviewing its annual Form 990, which details its finances and governance practices.
- Check out the organization's website and carefully review the web address. Swindlers sometimes create sites that appear almost identical to that of a well-known, credible charity. Look for small misspellings or sound-alike names, and note the URL (most charitable sites use .org instead of .com).

- Research social media requests, even when it comes from a friend. A well-meaning family member or colleague may have been duped and unknowingly passed along a fraudulent request. Don't assume crowdfunding sites are legitimate; ask the person about the information they shared or donate directly on the charity's website.

2 BE WARY OF DOOR-TO-DOOR, TELEPHONE, AND EMAIL SOLICITATIONS

Sophisticated scammers know how to replicate the practice or appearance of a bona fide charity whether in person, over the phone, or through an email request. In-person appeals can be particularly difficult to research, especially since practiced door-to-door solicitors know how to make small talk, develop rapport, and apply the subtle pressure that could lead to an on-the-spot "donation." **Look for these red flags:**

- A canvasser with no identification, badge, or marketing material. Always ask for the name, address, phone number, and registration number of the charity. Then, verify the information later, after the canvasser has left your property.
- A canvasser who pushes for a cash-only donation. Instead, mail a check or make a credit card donation directly to the charity—and not to the person standing in front of you.
- An unsolicited donation request via email. Most charities don't use email to pursue first-time donors (but many may use it for repeat requests).
- A telephone solicitor who pushes for an immediate donation. Instead, tell the caller you'd like time to research the organization before making a final decision.

3 FIND OUT HOW CHARITABLE DONATIONS ARE SPENT

Before giving, know how much of your donation goes to the program you want to support. Even the most benevolent charities must pay their staff and overhead costs. But some charities allocate a greater percentage of a contribution to the cause in question than others. Charities on the up-and-up will set aside no more than 35% to administrative costs. Ideally, that number should be less than 25%. This information can be found on an organization's IRS Form 990, which can often be found on GuideStar's searchable database.

4 REPORT SUSPICIOUS ACTIVITY

If you uncover a scam, report it to the Federal Trade Commission and your state charity regulator. Share any information you have, including the name of the charity or fundraiser, contact details, and even the specifics of the fraudster's pitch. By sharing the information, you may help shut down sham organizations, which can increase the ability for donated dollars to get to their intended recipients.

Your charitable gift can have a powerful impact. That's why it's so important to ensure that the organization you plan to support is reputable and your money is going to help those in need. By following these four tips, you can feel confident that your donation is making a difference.