GRIMES
AND COMPANY

grimesco.com

09.09.26 I FINANCIAL LITERACY

Protecting Your Identity: Simple Steps You Can Take Today

Michael Davide – Chief Compliance Officer

Protecting your personal and financial information is a shared responsibility, and one that we take seriously. At Grimes & Company, safeguarding our clients' information and helping clients understand ways to protect their financial identities are important parts of the trust you place in us.

Identity theft can happen in many ways. A criminal may try to open a credit card in your name, access an existing financial account, file a fraudulent tax return using your Social Security number, or use stolen personal information for other purposes.

While no individual or organization can eliminate the risk of identity theft entirely, taking proactive steps can make a meaningful difference. We encourage you to remain vigilant, use the protections available to you, and act promptly if something does not look right.

1. CONSIDER FREEZING YOUR CREDIT

One of the strongest preventive measures available is also free: placing a security freeze on your credit reports.

A credit freeze restricts access to your credit report, making it much more difficult for an identity thief to open a new credit account in your name. A freeze does not affect your credit score, and you can temporarily lift it when you legitimately need to apply for credit.

You need to place the freeze separately with each of the three major credit bureaus:

- **Equifax:** 800-685-1111
- **Experian:** 888-397-3742
- **TransUnion:** 800-916-8800

Keep in mind that a credit freeze is primarily designed to prevent **new accounts** from being opened. It does not prevent fraudulent transactions involving your existing bank, investment or credit card accounts.

2. REVIEW YOUR CREDIT REPORTS

Regularly reviewing your credit reports can help you identify suspicious activity before it becomes a larger problem. In particular, look for accounts you don't recognize, credit inquiries you didn't authorize, incorrect addresses or personal information, loans or credit cards you didn't open, and collection accounts that aren't yours.

You can obtain your credit reports through www.AnnualCreditReport.com, the federally authorized website for free credit reports.

Because information can differ among the three credit bureaus, consider reviewing reports from Equifax, Experian and TransUnion, rather than relying on just one.

3. PROTECT YOUR TAX IDENTITY WITH AN IRS IP PIN

Identity theft isn't limited to credit cards and bank accounts. Criminals can also use stolen Social Security numbers to file fraudulent tax returns.

The IRS offers an additional layer of protection called an Identity Protection PIN, or IP PIN.

An IP PIN is a unique six-digit number known only to you and the IRS. It helps the IRS verify your identity when a federal tax return is filed using your Social Security number.

Anyone with a Social Security number or Individual Taxpayer Identification Number who can verify their identity can request an IP PIN. A new PIN is generated each year.

You can learn more and enroll through the IRS website at www.IRS.gov/IPPIN.

Important: Treat your IP PIN like a password. Do not provide it in response to an unsolicited phone call, email or text message. The IRS will not contact you by phone, email, text or social media to ask for your IP PIN.

4. MONITOR THE ACCOUNTS YOU ALREADY HAVE

A credit freeze won't stop someone who has gained access to an existing account. Make a habit of reviewing your bank accounts, credit cards, investment accounts, and retirement accounts.

Many financial institutions also allow you to establish automatic alerts for transactions, transfers, password changes or other account activity. Consider turning these alerts on.

If you notice a transaction you don't recognize, contact the financial institution promptly using the telephone number or website you know to be legitimate.

5. BE SUSPICIOUS OF UNEXPECTED EMAILS, TEXTS AND PHONE CALLS

Identity thieves frequently create a sense of urgency.

You might receive a message claiming, *"Your account has been compromised. Click here immediately."*

Instead of clicking the link, independently contact the organization using a telephone number or website you know is legitimate.

The same principle applies if you receive an unexpected collection notice for a debt you don't recognize. Don't automatically pay it or provide personal information. Contact the collection agency independently and request information validating the debt and identifying the original creditor.

6. STRENGTHEN YOUR ONLINE ACCOUNTS

Good online security habits can make stealing your information considerably more difficult. Consider taking a few basic precautions:

- Use strong, unique passwords for important accounts.
- Don't reuse the same password across multiple websites.
- Consider using a reputable password manager.
- Enable multifactor authentication (MFA) whenever available.
- Never provide a password or authentication code to someone who unexpectedly contacts you.
- Keep computers, phones and other devices updated.

Pay particular attention to your email account. Because email is frequently used to reset passwords for other accounts, someone who gains access to your email may be able to compromise additional accounts.

7. KNOW WHAT TO DO IF SOMETHING LOOKS WRONG

If you discover an account or transaction that you believe resulted from identity theft, act promptly.

The Federal Trade Commission maintains www.IdentityTheft.gov, where you can report identity theft and receive a personalized recovery plan.

Depending on what occurred, additional steps may include:

- Contacting the affected financial institution
- Disputing fraudulent accounts or debts
- Freezing your credit
- Placing a fraud alert on your credit reports
- Changing compromised passwords
- Reporting tax-related identity theft to the IRS

Keep copies of correspondence and maintain notes regarding who you contacted and when.

8. USE STRONG, UNIQUE PASSWORDS

Using the same password across multiple websites can create unnecessary risk. If one website experiences a data breach and your password is exposed, criminals may try that same email address and password combination on your banking, email, shopping and other accounts.

Instead, use a **different, strong password for each important account**. Since remembering dozens of unique passwords can be difficult, consider using a reputable **password manager** (sometimes called a **password vault** or **password locker**). A password manager securely stores your passwords and can generate strong, unique passwords for each account, so you only need to remember the master password for your password manager.

For additional protection, enable **multifactor authentication (MFA)** whenever it is available. This requires an additional verification step beyond your password and can help protect your account even if your password is compromised.

Simple rule: One website, one unique password—and use MFA whenever possible.

9. WHAT ABOUT IDENTITY-MONITORING SERVICES?

Commercial identity-protection and monitoring services can provide another layer of protection. Depending on the provider and service level, these services may monitor certain information for suspicious activity and provide assistance if identity theft occurs.

These services can be helpful, but they should generally be viewed as supplemental protection rather than a substitute for good security practices.

Before paying for a service, understand what it monitors, what alerts it provides, what recovery assistance or insurance may be included, and what limitations apply.

A SIMPLE IDENTITY-PROTECTION CHECKLIST

If you're not sure where to begin, start with these five steps:

1. Freeze your credit with Equifax, Experian and TransUnion
2. Review all three of your credit reports
3. Consider obtaining an IRS Identity Protection PIN
4. Turn on multifactor authentication for important accounts
5. Set up alerts and regularly review your financial accounts

Identity protection doesn't have to be complicated. A few preventive measures—combined with regularly monitoring your accounts and being cautious about unexpected communications—can significantly improve your ability to detect and respond to suspicious activity.

If you have questions about identity protection, notice suspicious activity, or simply aren't sure where to start, please reach out to your Grimes team. We are committed to helping you navigate these issues and identify resources that may help protect you and your financial information.

Your financial well-being–and the security of the information you entrust to us–remain paramount priorities at Grimes & Company.

IMPORTANT DISCLOSURES:

This information is provided for general educational and informational purposes only and is not intended as legal, tax, cybersecurity or identity-theft recovery advice. The appropriate steps may vary based on individual circumstances. If you believe you have been the victim of identity theft or fraud, consider contacting the appropriate financial institution, credit bureau, government agency and/or qualified professional promptly.