Z ADVISORY INNOVATIONS

Fraud-Proofing Your Financial Life

Z A.I.

10 practical habits that make scams harder to pull off.

THE BEST TIME TO BUILD FRAUD BARRIERS IS BEFORE THE PRESSURE STARTS.
Scammers rely on urgency, confusion, isolation, and access. Small rules set up in advance can interrupt all four.

VERIFY PEOPLE, NOT JUST STORIES

1 USE THE CALLBACK RULE

Unexpected call, text, or email? Do not move money or share information. Hang up and contact the organization through its official app, a recent statement, or the number on the back of your card.

2 SAVE TRUSTED NUMBERS NOW

Store your bank, credit-card company, financial professional, and key family contacts in your phone. This reduces the chance you will rely on a fake number or paid search ad when you are under pressure.

3 CREATE A FAMILY VERIFICATION PHRASE

Agree on a private phrase or verification question for emergency calls. AI can imitate a familiar voice, so verify the person through a number or contact method you already know.

4 KEEP SECURITY CODES PRIVATE

Never read a one-time login or verification code to someone who contacted you. Do not approve a sign-in prompt you did not initiate, even if the caller claims to be stopping fraud.

5 REFUSE REMOTE ACCESS

Do not install remote-control software or give screen access to an unexpected caller. A legitimate fraud department does not need control of your computer or phone to protect your account.

THREE RULES WORTH MEMORIZING

URGENCY	Slow down.
SECRECY	Involve someone.
MONEY MOVEMENT	Verify independently.

Z ADVISORY INNOVATIONS

Lock Down Accounts Before Trouble Starts

These steps focus on identity theft, account takeover, and unauthorized money movement - risks that investment structure alone does not address.

BUILD PROTECTION INTO THE ACCOUNTS THEMSELVES

6 FREEZE YOUR CREDIT

When you are not applying for new credit, consider freezing your credit with Equifax, Experian, and TransUnion. A freeze is free to place or lift and can help block new accounts from being opened in your name.

7 TURN ON REAL-TIME ALERTS

Use the alerts your bank and card issuers offer for purchases, transfers, new payees, logins, password changes, and profile changes. The sooner you see unusual activity, the sooner you can act.

8 PROTECT YOUR EMAIL FIRST

Your email often controls password resets for other accounts. Use a unique password, a reputable password manager, and multifactor authentication on email and financial accounts.

9 PROTECT YOUR MOBILE NUMBER

Ask your wireless carrier what extra account protections it offers, such as an account PIN or port-out lock. SIM-swap and port-out fraud can let criminals intercept calls and text codes.

10 CREATE A PERSONAL COOLING-OFF RULE

For an unusual transfer, investment, purchase, or emergency request, create a standing rule: no same-day decision. Verify independently and discuss it with one trusted person before money leaves.

10-MINUTE FRAUD-PROOFING CHECK

- ☐ Transaction alerts are on
- ☐ MFA is on for email and banking
- ☐ Credit freeze considered
- ☐ Family verification phrase set
- ☐ Trusted numbers saved
- ☐ Carrier PIN/protection reviewed

IF SOMETHING FEELS OFF

Stop the transaction. Contact the financial institution using a number you already trust. Change compromised passwords and enable MFA. If identity theft is suspected, consider a credit freeze and use IdentityTheft.gov for a recovery plan.

SOURCE GUIDANCE

Federal Trade Commission: unexpected-call verification, family emergency scams, credit freezes, and identity theft. Cybersecurity and Infrastructure Security Agency: strong passwords, password managers, MFA, and software security. Federal Communications Commission: SIM-swap and port-out fraud. Accessed August 2026.

MAKE FRAUD HARDER BEFORE IT STARTS.

MICHAEL ZOELLNER | Director of Insurance

248-886-8190 | ZOE.AI.MICHAEL@GMAIL.COM | ZoellnerWholeFinancial.com

FRAUD PREVENTION RESOURCE CENTER