If something feels wrong

Safety first. Immediate physical danger, a suspected scam courier at your home or on the way, or a credible threat? Move to safety when possible and call 911 or local emergency services. Do not confront or follow anyone. A scam contact alone is not a 911 emergency.

End the contact. Hang up. Stop replying. Do not accept its callback number, link, or transfer.

Stop further movement. No more money, codes, documents, account changes, software, or remote access.

Did anything move or change?

NO: Keep the pause. Call your designated trusted person. Check the person and claimed event through a route you already know.

YES OR UNSURE: Use the First Response Card (LARGE-04). If money or account/device access may be involved, call the affected provider through a known route promptly. Do not delay to complete a worksheet.

You remain the decision-maker. Asking for help does not give someone control over your accounts.

Four steps. One shared rule.

SCREEN

An unexpected contact is a notice, not a place to make a decision.

AUTHENTICATE

End that contact. Check both the person and the claimed event through a route you selected independently.

FREEZE

Keep money, information, settings, and access still while the request is unverified. This is a family pause, not a bank or credit-bureau action.

ESCALATE

Bring in your designated trusted person. If anything may have moved or changed, use the affected-provider response path on LARGE-04.

> An unexpected request is not a reason to move value or give access until it has been independently verified and discussed with your designated trusted person.

The rule applies to everyone in the family. It is not a verdict on anyone’s judgment.

Nothing moves until we check.

For an unexpected or unverified request, keep these still until the request and claimed event are independently checked and your trusted-person rule is satisfied:

Money: transfers, checks, payment apps, gift cards, cryptocurrency, cash, or gold.

Secrets: passwords, verification or recovery codes, and security answers.

Identity: Social Security numbers, identity documents, selfies, signatures, or account images.

Settings: recipients, beneficiaries, mailing addresses, recovery routes, and account access.

Devices: software installations, screen sharing, remote control, and contact-directed support.

Ordinary life continues. This pause does not prohibit planned payments to known recipients or support you initiated through an independently verified provider.

If anything already moved or you are unsure, stop setup and use LARGE-01 and LARGE-04.

First Response Card

1. Immediate physical danger? Call 911 or local emergency services. Do not confront.
2. End the unexpected contact.
3. Stop further money, information, approvals, or access.
4. Identify what moved or changed; uncertainty counts.
5. Call affected providers through known routes, as applicable.
6. With permission, split simultaneous tasks when feasible.
7. Keep minimum facts, instructions, and case numbers.
8. Use the applicable identity, reporting, and follow-up routes.

On the provider call: State what happened, who initiated the transfer, and whether the owner authorized it. Ask about immediate options, deadlines, required follow-up, and a case number.

The provider may require the account owner or a formally authorized person. Family role titles create no account authority.

Use toolkit Exposure Sort (POST-01), Response Matrix (POST-04A/B), and Provider Contact Log (POST-08). Keep credentials and full account or identity numbers out of family tools.