Emergency Stop Page

Use this page when a scam or access incident may be happening now.

1: ARE YOU IN IMMEDIATE PHYSICAL DANGER?

• Suspected scam courier or person connected to the incident at the home or arriving?
• Threat of physical harm or coercive presence?

YES: Call 911 or the appropriate local emergency service. Do not confront, follow, detain, or physically engage. Move to safety when possible.

2: END THE ORIGINAL CONTACT

• Hang up. Stop replying. Close the chat or message.
• Do not accept a transfer, callback number, link, or new path supplied by the contact.

3: STOP ANYTHING ELSE FROM MOVING

No more money. No more codes. No more identity information. No more account changes. No more software, screen sharing, or remote access.

4: DID ANYTHING MOVE OR CHANGE?

NO: BRANCH A	YES OR UNSURE: BRANCH B
• Keep FREEZE active. • Call the trusted person. • Authenticate through a known route.	• Call the affected provider through a known route now. • Activate family roles. • Use Chapter 11; toolkit Exposure Sort (POST-01, page 60), First Response Card (POST-02, page 61), and Response Matrix (POST-04A/B, pages 63–64).

FIRST WORDS

“Thank you for telling me. You are not in trouble. We are stopping anything else from moving. We will take the next step together.”

Prepare this page before you need it. Keep your chosen contacts, known provider routes, and post-incident response pages with it. Do not delay a provider call to find or finish a worksheet.

SAFE Wallet / Refrigerator Card

Use the separate Large-Type Cards PDF for full-page or refrigerator copies. Compact reference formats are separate; print at 100%.

S	**SCREEN:** An unexpected contact is a notice, not a decision channel.
A	**AUTHENTICATE:** End the original contact. Verify the person, organization, and claimed event through a route you selected independently.
F	**FREEZE:** Nothing of value moves while the request is unverified: no money, codes, documents, account changes, software, or device access.
E	**ESCALATE:** Bring in the trusted person and, when something may have moved, the affected provider and the prepared incident route.

UNIVERSAL FAMILY RULE

No one sends or moves money, buys gift cards or cryptocurrency, hands over cash or gold, shares a password or verification code, sends identity documents, or installs remote-access software because of an unexpected contact until the request is independently verified and discussed with the designated trusted person.

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

Authentication Decision Tree

The original contact cannot verify itself.

1. End the original contact completely.
2. Choose a new route the family already knows or independently establishes.
3. Verify the person or organization through that route.
4. Verify the claimed event separately.
5. Involve the designated trusted person before any high-risk action.
6. Only then decide whether anything needs to happen.

SAME CHANNEL IS NOT INDEPENDENT

A transfer, conference call, supplied callback number, link, QR code, search phrase, or second person introduced by the contact still comes from that contact. It isn’t an independent route.

Person / organization verified?	[ ] YES [ ] NO [ ] NOT YET
Claimed event verified?	[ ] YES [ ] NO [ ] NOT YET
Trusted person involved?	[ ] YES [ ] NOT REQUIRED BY PLAN
Decision	

FREEZE Decision Card

FREEZE is a family behavior, not a bank, brokerage, or credit-bureau status.

FREEZE MEANS NOTHING MOVES YET

Until the original contact ends, the person and claimed event are independently checked, and the trusted-person rule is satisfied, no value or control moves.

[ ] No money, transfers, wires, checks, payment-app transactions, cash, gold, gift cards, or cryptocurrency.
[ ] No passwords, security answers, verification codes, recovery codes, or credential changes.
[ ] No identity documents, Social Security number, selfie, signature, or account statement image.
[ ] No recipient, beneficiary, mailing address, recovery route, profile, or access change.
[ ] No software installation, screen sharing, remote control, or contact-directed support session.

LEGITIMATE LIFE CONTINUES

Planned payments, known recipients, and support sessions the parent initiated through a verified provider remain ordinary life. FREEZE targets unexpected or unverified requests.

Ten-Minute Incident Response Card

Ten minutes describes action order, not resolution time.

1. SAFETY: Immediate physical danger, a suspected scam courier at the home or on the way, or a credible threat? Call 911. Do not confront.
2. END CONTACT: Hang up, stop replying, close the chat, reject supplied callback paths.
3. STOP FURTHER MOVEMENT: No more money, information, approvals, installs, or access.
4. ASK THE BRANCH QUESTION: Did anything move or change? If unsure, use Branch B.
5. CONTACT THE AFFECTED PROVIDER: Use a known route before generic reporting.
6. ACTIVATE FAMILY ROLES: Parent/account owner, support, provider caller, recorder, coordinator.
7. PRESERVE MINIMUM FACTS: Do not delay the provider call.
8. USE THE INCIDENT-SPECIFIC REPORTING MAP AND CHAPTER 11.

NO GUARANTEE

This card does not promise that a call, hold, recall, report, containment step, or recovery will finish within ten minutes.

Branch A / Branch B Decision

One first question sorts prevention from incident response.

DID MONEY, A CODE, CREDENTIALS, IDENTITY INFORMATION, AN ACCOUNT OR RECOVERY SETTING, SOFTWARE, SCREEN SHARING, OR DEVICE ACCESS MOVE OR CHANGE?

BRANCH A: NOTHING MOVED

- End the contact.
- Keep FREEZE active.
- Call the trusted person.
- Authenticate through a known route.
- Preserve the message only if useful.
- No report-everything rule.

BRANCH B: YES OR UNSURE

- Stop further action.
- Call the affected provider through a known route.
- Activate family roles.
- Preserve minimum facts without delay.
- Use the Emergency Stop Page and Chapter 11; toolkit Exposure Sort (POST-01), First Response Card (POST-02), and Response Matrix (POST-04A/B).

SAFETY OVERRIDE

Suspected scam courier or person connected to the incident at the home, or immediate physical threat: call 911, do not confront, and move to safety where possible.

Parent Disclosure & No-Blame Card

The first response matters.

SAY FIRST

THANK YOU FOR TELLING ME.
YOU ARE NOT IN TROUBLE.
WE DO NOT HAVE TO SOLVE EVERYTHING BEFORE WE TAKE THE NEXT USEFUL STEP.

Then ask

DID ANYTHING MOVE OR CHANGE?

IF YES OR UNSURE	IF NO
• Use Branch B. • Call the affected provider through a known route. • Use the Emergency Stop Page and Chapter 11; toolkit Exposure Sort (POST-01), First Response Card (POST-02), and Response Matrix (POST-04A/B).	• Keep money, codes, documents, settings, and access still. • Choose one independent verification step. • Keep the parent as decision-maker.

Avoid

- "How could you fall for this?"
- "I told you so."
- "Give me all your passwords."
- Family group interrogation before the first useful action.

What Moved? Exposure Sort

Check every category that may apply, even if you aren't sure.

MONEY / FINANCIAL VALUE	ACCESS / IDENTITY / DEVICE
• [ ] Card • [ ] ACH / bank transfer • [ ] Wire • [ ] Check • [ ] Payment app • [ ] Gift card • [ ] Cryptocurrency / Bitcoin ATM • [ ] Brokerage • [ ] Cash / gold / courier • [ ] Mailed cash / package	• [ ] Password or credential • [ ] Verification/recovery code • [ ] Primary email / recovery route • [ ] Phone / SIM / carrier • [ ] Recipient / beneficiary / profile setting • [ ] Identity information or document • [ ] Software / screen sharing / remote control

What may still be live?	
Affected provider(s)	
Known route(s)	
Account owner / parent available?	

SAFETY FIRST

Suspected scam courier, person connected to the incident, or credible threat: move to safety when possible and call 911. Do not confront.

First Response Card

Start the right actions without building a perfect timeline.

1. Safety: immediate danger, a suspected scam courier, or a credible threat? Call emergency services and do not confront.
2. End the unexpected contact.
3. Stop further money, information, approvals, installs, or access.
4. Identify what moved or changed.
5. Contact affected provider(s) through known routes.
6. When possible, have available helpers handle different exposures at the same time.
7. Preserve minimum facts.
8. Use applicable reporting and follow-up routes.

PROVIDER-CALL SCRIPT

“I am reporting a suspected scam or unauthorized access. Here are the facts I know, including what moved, when, and how. Please tell me what immediate options apply, what you need from the account owner, what other connected providers I should contact, and what case or reference number I should record.”

ASK WHAT IS POSSIBLE, NOT WHAT IS GUARANTEED

Record instructions and a reference number. Family role titles create no provider or legal authority.

Multiple-Exposure Priority Card

There is no universal bank-first, email-first, app-first, or device-first order.

WHAT IS STILL LIVE RIGHT NOW?

- Money still moving
- Caller still connected
- Remote access still active
- Recovery email/phone already changed
- Reset attempts continuing
- Courier present or arriving
- Identity exposed but no current account movement known

If capable helpers are available

- Parent/account owner participates as required.
- One person contacts the provider controlling live money movement.
- One person uses a known, unimplicated device to contact the recovery/account provider.
- One person records case numbers and unresolved items.

If one person is alone

- Safety first. Stop further action.
- Address the exposure with the most immediate potential for additional movement, lockout, or loss.
- Ask each provider what connected account or provider requires prompt contact.
- Record what remains unresolved.

Recovery-Scam Warning Card

A new offer to recover a loss may be another scam.

STOP WHEN AN UNEXPECTED PERSON OR COMPANY

- Demands an upfront fee tied to promised recovery.
- Guarantees a result.
- Requests passwords, codes, account numbers, identity documents, cryptocurrency, seed phrases, private keys, or remote access.
- Claims special access to law enforcement, a bank, an exchange, or a government fund.
- Pressures secrecy or immediate action.

DO THIS INSTEAD

Use a route the solicitor did not supply. Independently verify the organization. Do not send more money or information because someone promises recovery.

A legitimate professional may charge for legitimate work. This warning concerns unexpected solicitation, guaranteed recovery, advance payment tied to a promised result, and demands for sensitive access.

Fifteen-Minute Reset Card

This reviews the plan, not the person. Fifteen minutes is a coordination target, not a test.

TIME	REVIEW
0–3 min	Open actions: status, owner, target date, provider dependency, item no longer needed
3–6 min	People and routes: trusted people, known provider/emergency routes, consent, formal-provider changes
6–10 min	Guardrails and recovery: alerts, primary email, recovery, MFA, phone/carrier, devices, updates, backup, provider follow-up
10–13 min	Changes and triggers: incident, near miss, repeated contact, move, new device/number/account/provider/adviser/caregiver, breach
13–15 min	Record only needed actions; give each an owner and date; set next review; stop

NO SURVEILLANCE

No transaction-by-transaction audit, hidden account review, message reading, device inspection, location tracking, relationship monitoring, score, or capacity test.