SCAMS CHANGE. THE RULE DOESN'T.

COMPANION TOOLKIT

Printable Plans, Cards, Checklists, and Response Tools

For families protecting independence while preparing for unexpected money, identity, account, and device-access requests

Version 1.3.4 | 2026

How to Use This Toolkit

Print only what your family needs, or use the editable Word file.

THREE WAYS TO ENTER

- Something may be happening now: start with the Emergency Stop Page on page 7.
- You have one hour: use the Minimum Viable 60-Minute Setup on page 9.
- You are completing the full weekend: begin with the family plan on page 11 and follow the parts in order.

How the pages work

- [ ] means a family choice or action, not a test item.
- Blank cells are intended for typing or handwriting.
- “Owner” means the person responsible for follow-up. It creates no account or legal authority.
- Dates matter. A current route is more useful than a perfect-looking old one.
- When a provider controls a feature or process, use the provider’s current official instructions.

Print guidance

FULL-SIZE PAGES

- Print at 100% on US Letter paper.
- Keep the Emergency Stop Page visible.
- Store the working plan where the parent chooses.

QUICK CARDS

- Use the separate Large-Type Cards PDF for full-page or refrigerator copies.
- Cut or fold only after confirming the text is readable.
- Replace old copies when a route or instruction changes.

HOW THIS TOOLKIT WAS MADE

I used ChatGPT and Claude, which are AI tools, to draft and revise this toolkit. I chose the approach, made the final editorial decisions, and am responsible for what I publish. — Tommy Thurman

Privacy, Dignity, and Authority Rules

These rules apply to every page in the toolkit.

THIS TOOLKIT DOES	THIS TOOLKIT DOES NOT
• Create a pause before high-risk action. • Organize roles, known routes, and follow-up. • Support independent verification. • Keep the parent/account owner as decision-maker. • Provide a paper path when a phone or internet connection is unavailable.	• Create account access, ownership, or legal authority. • Assess capacity, competence, or vulnerability. • Authorize covert monitoring or device inspection. • Guarantee prevention, reversal, reimbursement, investigation, or recovery. • Replace emergency services, affected providers, qualified technical support, or legal advice.

Never write these in a family tool

- Passwords, password hints, master passwords, security answers, PINs, or one-time/recovery/backup codes.
- Full account or card numbers, balances, detailed transaction histories, Social Security numbers, seed phrases, or private keys.
- Identity-document images, medical conclusions, capacity opinions, private verification secrets, location data, recordings, or covertly obtained messages.

PARENT CONTROL

The parent chooses participants, voluntary sharing, safeguards, review timing, and what remains private. Formal provider arrangements change only through the provider’s process.

Contents

Pages 7–33

Contents

Pages 34–60

Contents

Pages 61–84

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.

Minimum Viable 60-Minute Setup

A practical starting point when you can't do the full weekend yet.

TIME	DO THIS	OUTPUT
0–5 min	Say why you're doing this and make clear that no one is taking over.	Shared purpose sentence
5–15 min	Choose the parent/account owner, primary trusted person, and backup.	Narrow roles
15–30 min	Choose the behaviors that always require a pause and second check.	Trigger list
30–45 min	Record known family and provider routes; do not record sensitive data.	First directory
45–55 min	Print or save the SAFE card and Emergency Stop Page.	Visible first-response tools
55–60 min	Assign unfinished work and put the next date on the calendar.	Owners and dates

Essential outputs

- [ ] One whole-family pause-and-verify rule
- [ ] Primary trusted person and backup
- [ ] First Trusted People & Known Routes Directory
- [ ] SAFE Wallet / Refrigerator Card
- [ ] Emergency Stop Page
- [ ] One next review date

SCOPE

Sixty minutes gives you a practical start. It doesn't secure every account, finish steps that depend on providers, or replace the full weekend.

Dignity-First Conversation Script

Open as a partnership, not a competency hearing.

OPENING

"I'm not asking to take over your accounts or test your judgment. I'd like us to make one rule the whole family follows, and to spell out exactly when I help, what I can see, and what stays private."

If your parent says…

CONCERN	RESPOND
"This is none of your business."	"Most of it isn't. You set the boundaries, and this role gives me no authority on its own."
"I do not want you monitoring me."	"I agree. Any visibility must be chosen, limited to a stated purpose, and reviewable, or it does not belong in the plan."
"You think I cannot handle my money."	"This is a whole-family rule. I follow the same pause and second-check rule."
"I do not have time for a weekend."	"Let's do the sixty-minute version and schedule only what still matters."

ROOM RULES

- The parent chooses participants and may skip or defer any question.
- No score, grade, capacity judgment, or risk rating.
- No passwords, balances, account numbers, codes, or identity images.
- An unfinished item becomes a next step, not evidence of failure.

Family Role Map

Write the minimum number of roles needed. A title creates no authority.

ROLE	PERSON	PURPOSE	MAY / MAY NOT
Parent / account owner		Owns decisions and chooses the plan	
Primary trusted person		First second-check call	
Backup trusted person		Substitutes when primary is unavailable	
Optional local support		In-person help when chosen	
Provider-call helper		Organizes or joins a provider call when allowed	
Recorder / coordinator		Tracks facts, case numbers, owners, and dates	

Who selected these roles?	
Review date or trigger	
How voluntary roles may be changed	

AUTHORITY BOUNDARY

A family title creates no account access, viewing rights, transaction authority, ownership, device-inspection rights, password access, power of attorney, or guardianship.

If neither chosen contact can be reached, keep the unexpected request paused. You can contact the affected provider through a route you selected independently to check the facts. Record what remains unresolved. An unavailable helper is not permission to send money, share information, change access, or install software. If something may already have moved or changed, use Branch B and contact the affected provider promptly.

Family Helper Boundary Record

This record sets boundaries for the helper's actions only.

THE HELPER WILL	THE HELPER WILL NOT
• Listen without blame. • Help locate an independent route. • Join a trusted-person or provider call when allowed. • Support the parent's decision-making. • Use the incident branch when required.	• Send or facilitate money. • Keep a transfer secret. • Contact or negotiate with the stranger for the parent. • Supply codes, credentials, documents, or account information. • Secretly monitor, record, track, inspect, or seize accounts or devices.

Helper	
Parent / account owner	
Specific help agreed	
Information voluntarily shared, if any	
Review date	

LIMIT

The helper may refuse to participate in a transfer or access request. That personal boundary does not create power to control the parent.

Twelve-Question Family Risk Review: 1

Planning review, not a test. Choose a status and a next step for each item.

ACTION STATUS
IN PLACE / WEEKEND PRIORITY / FOLLOW-UP / DISCUSS LATER / NOT APPLICABLE

QUESTION	FAMILY DECISION
1. Unexpected contacts **Which unexpected calls, texts, emails, pop-ups, social messages, ads, or new relationship approaches are most likely to get attention?**	Status: Next step / owner / date:
2. Decision boundary **Could an unexpected contact lead directly to a decision involving money, an account, a code, identity documents, or device access?**	Status: Next step / owner / date:
3. Money and access categories **Which categories are used often enough to need a second-check rule?**	Status: Next step / owner / date:
4. Second-check triggers **Which events always require the trusted person before anyone proceeds?**	Status: Next step / owner / date:
5. Known routes **Are independently sourced routes for trusted people and key providers saved on paper and on the phone?**	Status: Next step / owner / date:
6. Primary email priority **Does the primary email need a later review of unique credentials, recovery methods, and appropriate MFA?**	Status: Next step / owner / date:

Twelve-Question Family Risk Review: 2

Planning review, not a test. Choose a status and a next step for each item.

QUESTION	FAMILY DECISION
7. Financial-alert priority **Which institutions need their available login, transaction, transfer, or profile-change alerts reviewed?**	Status: Next step / owner / date:
8. Identity-protection priority **Should the family review new-credit protection and the limits of a credit freeze?**	Status: Next step / owner / date:
9. Device and remote-access priority **Do phones, computers, or tablets need a later update, lock-screen, backup, or unsolicited-remote-access review?**	Status: Next step / owner / date:
10. Prior incidents **Has a near miss, loss, code disclosure, remote-access event, or repeated contact changed what should be handled first?**	Status: Next step / owner / date:
11. Support and contact changes **Has a recent change made it useful to update roles, local support, or known routes?**	Status: Next step / owner / date:
12. Emergency readiness **Does everyone know the first immediate actions, who calls the provider, and who supports the parent?**	Status: Next step / owner / date:

DO NOT TOTAL THE ANSWERS

Use the statuses to decide what to do next. Never total or average them, or use them to judge the person answering.

Weekend Priority & Follow-Through List

Choose exactly three weekend priorities. Assign every other open item.

PRIORITY 1	
Priority 1: action	
Why selected	
Owner	
Target block / date	
Provider or later-step dependency	

PRIORITY 2	
Priority 2: action	
Why selected	
Owner	
Target block / date	
Provider or later-step dependency	

PRIORITY 3	
Priority 3: action	
Why selected	
Owner	
Target block / date	
Provider or later-step dependency	

Other follow-through

ACTION	STATUS	OWNER	TARGET DATE

Family Verification & Response Plan: 1

Record voluntary family rules and roles. This is not a legal instrument.

Shared purpose	
Parent / account owner	
Primary trusted person	
Backup trusted person	
Optional local support person	

Actions that always require a second check

[ ] Unexpected or urgent money movement
[ ] New recipient or unusual payment route
[ ] Gift card, cryptocurrency, cash, or gold courier request
[ ] Password, verification-code, or identity-document request
[ ] Software, screen sharing, or remote access
[ ] Instruction to keep the matter secret or stay on the line

Other family-selected triggers

Family Verification & Response Plan: 2

Complete roles, consent boundaries, review timing, and the emergency handoff.

CONSENT BOUNDARIES

Information voluntarily shared, if any	
Person receiving it	
Purpose	
What the person may do	
What the person may not do	
How the parent may change or stop it	

EMERGENCY AND REVIEW

Emergency provider-call helper	
Parent-support person	
Recorder / coordinator	
Reviewed together on	
Next review date or trigger	

NO SIGNATURE REQUIRED
Completing this plan creates no account access, ownership, transaction authority, power of attorney, or guardianship.

Trusted People & Known Routes Directory: People

Use known routes selected independently. Do not store credentials or sensitive identifiers.

ROLE / TYPE	NAME	KNOWN ROUTE	SOURCE	LAST VERIFIED
Primary trusted person				
Backup trusted person				
Local support, if used				
Close relative / emergency check				
Other chosen support				

Purpose or caution notes

____

____

____

____

NEVER RECORD

Passwords, codes, security answers, account numbers, balances, Social Security numbers, identity images, or the private family verification secret.

Trusted People & Known Routes Directory: Providers

Use the number on a card or statement, an official app opened independently, or prior verified correspondence.

PROVIDER / PURPOSE	KNOWN ROUTE	SOURCE USED	LAST VERIFIED	CAUTION / OWNER
Bank / credit union				
Card issuer				
Brokerage / retirement				
Primary email				
Mobile carrier				
Device / technical support				
Identity / credit route				
Other important provider				

KNOWN ROUTE RULE

The unexpected contact never supplies the route used to verify it.

Private Verification-Method Status Record

Do not write the phrase, question, answer, or secret on this page.

IMPORTANT
A matching phrase or answer is only an extra check. End the original contact and verify the person and claimed event independently through a known route.

Private method created	[ ] YES [ ] NOT YET [ ] DISCUSS LATER
People intended to know it	
Private storage approach (without the secret)	
Replacement trigger	[ ] possible disclosure [ ] family change [ ] unsafe storage [ ] other
Last reviewed	
Next review	

DO NOT UPLOAD THE SECRET
Record only whether a method exists, who should know it, how it’s stored privately, and when it should be replaced.

Pressure Pattern Decoder

Look past the story. Several stacked elements are enough to trigger a pause.

ELEMENT	QUESTIONS TO ASK	NOTES
Unexpected entry	Did the person initiate this contact? Which channel did they choose?	
Borrowed credibility	Whose name, authority, voice, brand, document, or personal detail is being borrowed?	
Emotional acceleration	What feeling is being intensified: fear, hope, urgency, affection, shame, relief?	
Isolation	Am I being kept on the line, told to keep a secret, or discouraged from asking anyone else?	
Unusual action	What is being asked to move: money, codes, documents, settings, software, or access?	
Escalation	Did a first step create pressure for another payment, code, fee, or request?	

INTERRUPTION PRINCIPLE

You do not need the scam's name. End the original contact, create time, use a known route, and involve the trusted person.

Known Unknowns Plan

List legitimate callers who may appear as unknown numbers.

CALLER TYPE	LIKELY REASON	KNOWN CALLBACK ROUTE	IF MISSED	LAST VERIFIED
Medical office				
Pharmacy / care service				
Delivery / building / gate				
Repair / contractor				
School / insurer / local service				
Relative with new number				
Other legitimate unknown				

ROUTING SHEET, NOT A RECORDS FILE

Do not record medical details, account numbers, or identity information.

Communication Screening Checklist: 1

Essential phone, text, and email setup. Menus and availability vary.

Essential today

[ ] Post the rule: AN UNEXPECTED CONTACT IS A NOTICE, NOT A DECISION CHANNEL.
[ ] Complete the Known Unknowns Plan before silencing or blocking unknown callers.
[ ] Confirm voicemail is set up, reachable, and understandable.
[ ] Turn on available caller-ID or spam labeling that the parent wants.
[ ] Choose the least restrictive unknown-call handling that solves the actual problem.
[ ] Locate filtered-call, unknown-message, spam, junk, and voicemail folders.
[ ] Adopt the rule: no click, no reply, no attachment, no callback number from an unexpected money/account/access message.

First-week false-positive review

Review date	
Wanted calls/messages caught	
Setting adjusted	
Owner	

SCREENING SORTS
A spam label, caller ID, saved number, familiar account, or lack of a warning label is not authentication.

Communication Screening Checklist: 2

Browser, pop-up, notification, social, landline, and privacy checks.

[ ] Confirm the browser’s pop-up blocker is on.
[ ] Review website-notification permissions separately; remove unrecognized or unused sites.
[ ] Never call a phone number displayed in a security warning or pop-up.
[ ] Reach technical support through an official route found independently.
[ ] Accept social requests only from people the parent actually knows.
[ ] Review who can see posts, personal details, family information, and friend lists where available.
[ ] Treat an unexpected money, investment, romance, prize, job, or access message from a familiar account as unexpected contact.
[ ] For landlines, ask the provider what labeling, blocking, and voicemail options exist before buying any optional device.

DISTINGUISH THE ACTIONS	STATUS
• BLOCK: restricts future contact where supported. • DELETE: removes the local message or conversation. • MARK NOT SPAM: restores a false positive where available. • REPORT: may transmit content and metadata to a platform or carrier.	• ESSENTIAL TODAY • RECOMMENDED • OPTIONAL BASED ON NEED • NOT AVAILABLE • DECLINED • NOT APPLICABLE

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	

False Proof Checklist

Convincing is not the same as independent.

CONTACT-SUPPLIED PROPS	WHAT TO DO INSTEAD
• Caller ID or familiar number • Familiar voice or live video • Badge, case number, warrant, letter, screenshot • Accurate personal details • Logo, email, social profile, or familiar thread • Real employee, adviser, agency, charity, or firm name • Transferred call or “supervisor”	• End the original contact. • Use a route selected independently. • Verify the person or organization. • Verify the claimed event separately. • Call the trusted person before any high-risk action. • Keep money, codes, documents, settings, and access still.

NARROW RULE

A real detail may still be delivered by the wrong person. Contact-supplied proof is not independent proof.

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.

What Stays Still Matrix

Use before anything moves. Categories matter more than the scam's story.

CATEGORY	STAYS STILL WHEN REQUEST IS UNEXPECTED / UNVERIFIED	FAMILY RULE
Money / value	Card, check, transfer, wire, app, gift card, crypto, cash, gold, brokerage move	Pause and verify
Credentials / codes	Password, security answer, one-time code, recovery code	Never disclose to unexpected contact
Identity	SSN, license/passport image, statement image, selfie, signature	Use only a process the parent started through a known route
Account settings	Recipient, beneficiary, email, phone, address, password, recovery factor	No change until provider/claim verified
Device access	Software, screen share, remote control, staying on line while accounts open	End contact and use known support route

Optional household dollar threshold (additional only)	
Optional cooling-off period for nonroutine, nonemergency decisions	
Trusted person	

Pressure-Response Scripts

A short statement of your rule helps you end the conversation. It doesn’t accuse the caller or reveal private family methods.

“I do not move money or share codes during unexpected contacts. I will call back through a number I already know.”

“I do not make payments while someone is waiting on the line.”

“I do not send test payments.”

“I do not give gift-card numbers, verification codes, or identity documents to an unexpected contact.”

“I do not install software or allow remote access from an unexpected contact.”

“I will discuss this with my trusted person before I act.”

“If this is real, I will reach the organization through my own route.”

Parent Guardrail Card

Guardrails support your decisions. They do not transfer control.

- You choose which safeguards are used, declined, or revisited later.
- Alerts help notice selected activity; they are not proof and may be delayed.
- A brokerage trusted contact is a limited contact role, not transaction authority.
- A credit freeze addresses new-credit access, not existing accounts.
- Any duplicate alert, statement, or visibility is voluntary and limited to a stated purpose.
- Provider features vary. “Not available” is a provider fact, not a family failure.
- No family checklist stores passwords, account numbers, codes, or identity documents.

ACTIVE-INCIDENT EXIT

If the review reveals an unfamiliar transaction, account, recovery change, disclosed code, installed software, remote access, missing device, or unexplained lockout: stop setup and use the Emergency Stop Page and Chapter 11; toolkit Exposure Sort (POST-01), First Response Card (POST-02), and Response Matrix (POST-04A/B).

Bank & Brokerage Safeguard Checklist

Confirm each feature with the actual institution. Nothing is selected by default.

ITEM	STATUS	OWNER / DATE
Contact information on file is current		
Known support route recorded		
Login/new-device/security-change alerts considered		
Transaction, transfer, wire, ACH, new-recipient alerts considered		
Cash/withdrawal/card-not-present alerts considered		
Brokerage trade/distribution/beneficiary-change alerts considered		
Brokerage trusted-contact status reviewed		
Provider restrictions or transfer controls explained before activation		
Selected alert volume reviewed after setup		

STATUS OPTIONS

IN PLACE / ACTION TODAY / PROVIDER FOLLOW-UP / DECLINED / NOT AVAILABLE / NOT APPLICABLE

Identity & Credit Checklist

Keep four different choices separate.

CHOICE	WHAT IT DOES	WHAT IT DOES NOT DO	STATUS / NEXT DATE
Credit freeze	Restricts access to credit reports, making new credit harder to open	Does not secure existing accounts	
Fraud alert	Tells prospective creditors to take added identity-verification steps	Does not freeze the report	
Credit-report review	May reveal unfamiliar accounts or inquiries	Does not authorize family access or copy report contents	
Existing-account safeguards	Alerts, account recovery, provider controls, device and email security	Do not replace new-credit protection	

PRIVACY

Record only whether a review occurred and the next date. Do not copy report details, identity documents, or sensitive identifiers into the toolkit.

Account & Device Checklist

Review the primary recovery chain first, using current provider instructions.

[ ] Identify the primary email account used for resets and notices.
[ ] Confirm recovery phone numbers and email addresses; remove stale routes where allowed.
[ ] Use a credential not reused elsewhere; consider a password manager if the parent wants one.
[ ] Use an MFA method the provider supports and the parent can keep using.
[ ] Confirm backup/recovery codes exist where offered and are stored privately, never in this toolkit.
[ ] Confirm device passcode/biometric lock and automatic screen lock.
[ ] Review operating-system and important-app updates.
[ ] Confirm a usable backup and recovery route.
[ ] Review carrier PIN, SIM, or port-out protection where available; understand legitimate-change consequences.
[ ] Note what remote-access software is present and why, without conducting forensics.

Provider/device follow-up owner	
Target date	
Current official instructions checked on	

Consent and Visibility Mini-Record

Use for every voluntary shared alert, statement, notice, or visibility arrangement.

Information category shared	
Person receiving it	
Purpose	
What the recipient may do	
What the recipient may not do	
Review date or trigger	
How the parent can change or stop it	

NO DEFAULT SHARING

This record does not create ownership, transaction authority, device-inspection rights, password access, power of attorney, or guardianship.

Provider Question Script

Ask before activating an alert, restriction, lock, trusted-contact role, or recovery feature.

OPENING

"I'm reviewing optional fraud and account-security safeguards. Please explain how this feature works without assuming I want to turn it on yet."

- What does it cover?
- What does it not cover?
- Does it block, delay, alert, or require confirmation?
- What legitimate activity could it interrupt?
- Who may turn it on, change it, or remove it?
- How quickly can normal access be restored?
- Does activating it share information with anyone else?
- Is there a lower-burden alternative?
- Where do the current official terms or instructions appear?

Provider / feature	
Answer and limitation	
Decision / next step	
Owner / date	

Secure Account Inventory: 1

Route-and-status tool, not a credential vault.

SERVICE / CATEGORY	VERIFIED SUPPORT ROUTE	ALERT / MFA / RECOVERY STATUS	TRUSTED CONTACT / DEVICE STATUS	LAST REVIEWED	OWNER / DATE
Bank / credit union					
Card issuer					
Brokerage / retirement					
Payment app					
Credit / identity route					

NEVER RECORD

Usernames; passwords or hints; account numbers; balances; transaction history; SSNs; PINs; codes; identity images; private verification secrets.

Secure Account Inventory: 2

Route-and-status tool, not a credential vault.

SERVICE / CATEGORY	VERIFIED SUPPORT ROUTE	ALERT / MFA / RECOVERY STATUS	TRUSTED CONTACT / DEVICE STATUS	LAST REVIEWED	OWNER / DATE
Primary email					
Mobile carrier					
Phone / tablet					
Computer / technical support					
Other important service					

NEVER RECORD

Usernames; passwords or hints; account numbers; balances; transaction history; SSNs; PINs; codes; identity images; private verification secrets.

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.

Emergency Role & Contact Plan

Assign one job to each person. One person may hold several roles.

ROLE	PERSON / ROUTE	JOB	LIMIT
Parent / account owner		States facts and participates when provider requires	Remains decision-maker
Parent-support person		Stays with parent and limits repeated retelling	No interrogation
Provider-call helper		Uses known route and records instructions	Only as parent/provider allow
Recorder		Keeps short timeline and case numbers	No sensitive data
Family coordinator		Prevents duplicate action and tracks follow-up	No authority created
Backup / local helper		Substitutes or assists when chosen	No broader permission

Primary affected provider route	
Next family check-in	

Minimum Evidence Notes

Preserve what already exists after safety and provider contact are underway.

Date / approximate time	
Contact route / sender / caller	
Claimed identity and event	
What was requested	
What was sent, shared, installed, approved, or changed	
Transaction / receipt / tracking information already at hand	
Providers contacted and case numbers	
Short chronology of family actions	

DO NOT

Call back, keep the person talking, click new links, download files, install “recovery” software, perform forensics, or delay provider contact to complete this page.

Incident-Specific Reporting Map

Calling a provider and filing a public report serve different purposes.

ROUTE	USE FOR	LIMIT
Emergency services	Immediate physical danger, suspected scam courier at the home or on the way, or credible threat	Not every scam call is a 911 matter
Affected provider	Transaction, account, access, carrier, platform, or device response	Use a known route; options vary
FTC ReportFraud	General consumer-fraud report and pattern information	Does not resolve an individual account
FBI IC3	Internet-enabled crime complaint	No status or outcome guarantee
IdentityTheft.gov	Identity-theft report and recovery plan	Match actions to actual exposure
Local/state/APS/elder services	Facts and jurisdiction warrant	Eligibility, process, and duties vary
SEC / FINRA	Securities, brokerage, or professional matters	Does not replace the firm call
CFPB / relevant financial regulator	Provider handling seems wrong: request an explanation/review; use the relevant regulator's complaint route.	Does not guarantee repayment or extend notice deadlines; account owner or authorized representative.

CURRENT CONTACTS

Use the Dated Public Resource Pages at the end of this toolkit. Reverify routes before use.

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.

Five-Minute Practice Drill

Practice the card, not the emergency details.

DRILL A: NOTHING MOVED	DRILL B: SOMETHING MAY HAVE MOVED
• Unexpected bank text. • No click, code, payment, or setting change. • End interaction; maintain FREEZE; call trusted person; use known bank route; Branch A.	• Hypothetical payment or code may have been sent. • Stop further action; select affected provider; activate roles; preserve minimum facts; Branch B and Chapter 11; toolkit Exposure Sort (POST-01), First Response Card (POST-02), and Response Matrix (POST-04A/B).

Which step was unclear?	
Which route was missing?	
Which role was overloaded?	
One card revision	
Next drill date	

NO SCORE

This drill tests whether the family can find and use the plan. It does not test the parent.

Scenario Practice Instructions & Template

Every scenario is constructed for teaching, not a real person or documented incident.

1. Read only the SETUP.
2. Stop at YOUR DECISION: STOP HERE.
3. Name what must remain still.
4. Name the exact known route.
5. Name the trusted person.
6. Ask whether anything moved or changed.
7. Reveal the recommended pathway.
8. Mark SAFE steps USED / MISSED / NOT NEEDED.
9. Record one plan improvement.

Scenario family	
What must remain still?	
Which exact known route?	
Trusted person	
Anything moved or changed?	[ ] NO [ ] YES [ ] NOT SURE
Branch	[ ] A [ ] B
SCREEN / AUTHENTICATE / FREEZE / ESCALATE	USED / MISSED / NOT NEEDED
One plan improvement	
Owner / date	

NEVER TOTAL OR GRADE

A missed step is information about the plan, not a verdict on a person.

Scenario 1: The Familiar Voice

CONSTRUCTED FOR TEACHING: NOT A REAL PERSON OR DOCUMENTED INCIDENT

SETUP

A late call sounds exactly like a grandchild. There has been an accident; money is needed before morning; secrecy is requested. The caller even answers the private family question correctly.

WHY IT FEELS CONVINCING

Voice, family details, fear, secrecy, and a matching answer.

YOUR DECISION: STOP HERE

What stays still? Which exact known route? Who is the trusted person? Did anything move or change?

RECOMMENDED SAFE PATHWAY

End the call. Call the grandchild at a saved number. If unanswered, reach another known family route. No money moves. Replace a possibly exposed private method later. Branch A.

SCREEN	USED / MISSED / NOT NEEDED
AUTHENTICATE	USED / MISSED / NOT NEEDED
FREEZE	USED / MISSED / NOT NEEDED
ESCALATE	USED / MISSED / NOT NEEDED
One plan improvement	

Scenario 2: The Investigator With a Case Number

CONSTRUCTED FOR TEACHING: NOT A REAL PERSON OR DOCUMENTED INCIDENT

SETUP

A caller claims federal authority, shows an agency name on caller ID, texts a badge image, gives a case number, and says money must be moved to a protected account. Cash, gold, and a courier are offered as alternatives.

WHY IT FEELS CONVINCING

Authority, fear, and official-looking props.

YOUR DECISION: STOP HERE

What stays still? Which exact known route? Who is the trusted person? Did anything move or change?

RECOMMENDED SAFE PATHWAY

Nothing moves. End the contact. Locate the agency through an official route selected independently and verify the office and claimed case. Call the trusted person. If a courier or threat appears, use the safety override.

SCREEN	USED / MISSED / NOT NEEDED
AUTHENTICATE	USED / MISSED / NOT NEEDED
FREEZE	USED / MISSED / NOT NEEDED
ESCALATE	USED / MISSED / NOT NEEDED
One plan improvement	

Scenario 3: The Technician on the Screen

CONSTRUCTED FOR TEACHING: NOT A REAL PERSON OR DOCUMENTED INCIDENT

SETUP

A full-screen warning says the computer is infected. A “technician” asks for software installation and remote control. Access is granted briefly before the parent disconnects.

WHY IT FEELS CONVINCING

The alarm appears to come from the device, and the caller sounds helpful.

YOUR DECISION: STOP HERE

What stays still? Which exact known route? Who is the trusted person? Did anything move or change?

RECOMMENDED SAFE PATHWAY

Remote access already occurred: Branch B. Stop further action. Use a known technical/provider route. Preserve minimum facts. Use the Emergency Stop Page and Chapter 11; toolkit Exposure Sort (POST-01), First Response Card (POST-02), and Response Matrix (POST-04A/B). Do not perform amateur forensics.

SCREEN	USED / MISSED / NOT NEEDED
AUTHENTICATE	USED / MISSED / NOT NEEDED
FREEZE	USED / MISSED / NOT NEEDED
ESCALATE	USED / MISSED / NOT NEEDED
One plan improvement	

Scenario 4: The Adviser Whose Record Is Real

CONSTRUCTED FOR TEACHING: NOT A REAL PERSON OR DOCUMENTED INCIDENT

SETUP

A group message promotes a private investment, gives a real adviser's name and registration number, promises high returns with little risk, and asks for a deposit to a supplied account.

WHY IT FEELS CONVINCING

A genuine registry record, testimonials, urgency, and social proof.

YOUR DECISION: STOP HERE

What stays still? Which exact known route? Who is the trusted person? Did anything move or change?

RECOMMENDED SAFE PATHWAY

The deposit and account details stay still. Check the registry, then contact the firm through the independently listed route. Registration does not authenticate the messenger or investment. Branch A unless money already moved.

SCREEN	USED / MISSED / NOT NEEDED
AUTHENTICATE	USED / MISSED / NOT NEEDED
FREEZE	USED / MISSED / NOT NEEDED
ESCALATE	USED / MISSED / NOT NEEDED
One plan improvement	

Scenario 5: Someone Who Matters

CONSTRUCTED FOR TEACHING: NOT A REAL PERSON OR DOCUMENTED INCIDENT

SETUP

After months of voice and video contact in a meaningful online relationship, the other person says there's a medical emergency overseas and asks for a wire transfer in secret.

WHY IT FEELS CONVINCING

Time, affection, privacy, and a relationship that genuinely matters.

YOUR DECISION: STOP HERE

What stays still? Which exact known route? Who is the trusted person? Did anything move or change?

RECOMMENDED SAFE PATHWAY

Do not judge the relationship. Verify this one request through an official route selected independently. Keep money, codes, documents, and access still. Call the trusted person. Branch A if nothing moved.

SCREEN	USED / MISSED / NOT NEEDED
AUTHENTICATE	USED / MISSED / NOT NEEDED
FREEZE	USED / MISSED / NOT NEEDED
ESCALATE	USED / MISSED / NOT NEEDED
One plan improvement	

Scenario 6: The Prize With a Fee

CONSTRUCTED FOR TEACHING: NOT A REAL PERSON OR DOCUMENTED INCIDENT

SETUP

A cheerful caller announces a major prize but says taxes and processing fees must be paid today and bank details are needed for the deposit.

WHY IT FEELS CONVINCING

Excitement, hope, a familiar brand, and urgency.

YOUR DECISION: STOP HERE

What stays still? Which exact known route? Who is the trusted person? Did anything move or change?

RECOMMENDED SAFE PATHWAY

No upfront payment or sensitive information. End the call and independently reach the real company if the parent wants to verify. Call the trusted person. Branch A if nothing moved.

SCREEN	USED / MISSED / NOT NEEDED
AUTHENTICATE	USED / MISSED / NOT NEEDED
FREEZE	USED / MISSED / NOT NEEDED
ESCALATE	USED / MISSED / NOT NEEDED
One plan improvement	

After-Action Worksheet & 60-Minute Practice Night

Choose three relevant scenarios; spend roughly 15 minutes on each and use the final 15 minutes for plan updates.

Scenario used	
What stayed still?	
Known route selected	
Trusted person	
Branch A / Branch B	
SAFE step missed or unclear	
One plan improvement	
Owner / date	

Practice-night plan

BLOCK	SCENARIO / TASK
0–15 min	Fear or authority scenario
15–30 min	Money or opportunity scenario
30–45 min	Technology or relationship scenario
45–60 min	Update plan, routes, roles, and next drill date

REAL INCIDENT EXIT

If practice uncovers a real unrecognized transaction, shared code, or remote access, stop the drill and use Branch B and Chapter 11; toolkit Exposure Sort (POST-01), First Response Card (POST-02), and Response Matrix (POST-04A/B).

One-Next-Step Conversation Guide

Use only when nothing moved and no immediate danger exists.

1. Acknowledge why the parent wants to stay in control or why the relationship matters.
2. Separate the person or relationship from the specific request.
3. State the whole-family rule.
4. Ask for one independent check.
5. Name what stays still while checking.
6. Identify the trusted person.
7. Schedule the next check-in.
8. Stop before the conversation becomes a trial.

PROMPT

"I am not asking you to decide what this person or relationship means today. Would you be willing to verify this one request with me through a route we choose ourselves?"

One proposed check	
Known route	
Trusted person	
Next check-in	

What We Know / What We Do Not Know / What Stays Still

Keep observable facts separate from open questions and safety boundaries.

WHAT WE KNOW	WHAT WE DO NOT KNOW
• Observable facts only • Exact request • Channel and approximate time • What the parent says occurred • Whether anything moved or changed	• Identity not independently verified • Claimed event not independently verified • Motive not known • No capacity, abuse, or criminal conclusion

WHAT STAYS STILL

[ ] Money
[ ] Codes and credentials
[ ] Identity documents
[ ] Account, recipient, beneficiary, or recovery changes
[ ] Software, screen sharing, or device access

Notes / one next step

____
____
____

Relationship-and-Request Separation Card

Respect the relationship. Independently verify the specific request.

RELATIONSHIP QUESTION	REQUEST QUESTION
• The parent decides what the relationship means. • The family does not diagnose motive. • A relationship may provide companionship, meaning, privacy, hope, or routine.	• The family verifies this specific emergency, payment, investment, identity, account, or access request. • Money and access stay still until the request is checked. • A relationship can matter and a request can remain unverified.

SCRIPT

"I am not asking you to decide what this relationship means today. I am asking us to verify this one request before money, information, or access moves."

Request being checked	
Independent route	
What stays still	
Next check-in	

Continuing-Engagement Plan

Use only when nothing moved and no immediate physical danger exists.

Relationship / contact may continue if parent chooses	[ ] YES [ ] NO DECISION TODAY
Money, codes, documents, settings, and device access stay still	[ ] AGREED
Trusted person for each new high-risk request	
Independent route for claimed events	
What remains private	
What may be shared voluntarily	
Next check-in date	
Branch B trigger	
Trigger for qualified outside help	

NO SURVEILLANCE

Continued contact alone does not authorize secret device monitoring, message reading, location tracking, recording, or an ultimatum.

Observable Concern Notes

Write a factual record the parent may see.

Date / time	
Channel or person category	
Exact observable request or behavior	
Facts the parent shared	
What may have moved or changed	
Independent routes used	
Provider / resource contacted	
Instructions received	
Owner / next date	

PROHIBITED

Diagnosis; capacity opinion; unsupported crime/abuse allegation; passwords or codes; account numbers or balances; identity images; medical records; covert screenshots, recordings, tracking, or secretly obtained messages.

Help and Referral Decision Map

Choose outside help by function, facts, and jurisdiction, not a fixed universal order.

SITUATION	ROUTE	LIMIT
Immediate danger / credible threat / suspected scam courier or incident-connected person at home	Emergency services	No confrontation
Money or access may have moved	Affected provider + Branch B + Chapter 11	Conversation work must not delay response
Ordinary disagreement / privacy concern	One-Next-Step Guide + scheduled follow-up	No covert monitoring
Possible known-person exploitation or coercion	Observable facts + appropriate local elder-services / legal / victim-support route	No automatic capacity, abuse, or mandatory-reporting conclusion
Parent wants neutral support	Current elder-fraud / support resource from dated pages	No investigation or recovery promise
Separate health concern	Appropriate qualified health professional	This toolkit does not diagnose

Chapter 10 Incident Exit

A difficult conversation stops being the right tool when value or access may already have moved.

DID ANYTHING MOVE OR CHANGE?

Money, code, credentials, identity information, account or recovery settings, software, screen sharing, or device access?

YES OR UNSURE	NO
• Stop the conversation worksheet. • Use the Emergency Stop Page. • Use Chapter 8 Branch B. • Call the affected provider through a known route. • 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).	• Keep value and access still. • Use relationship/request separation. • Choose one independent check. • Use trusted-person support. • Schedule the next check-in.

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.

What Moved? Response Matrix: 1

Contact each provider through a route selected independently. Outcomes and legal classifications vary.

METHOD	KNOWN PROVIDER	ASK
Card	Card issuer	Blocking, dispute, replacement, and account-protection options
ACH / bank transfer	Bank or credit union	Pending stop, completed recall/dispute, and account protection
Wire	Sending bank or wire service	Fraud flag and recall process
Check	Bank	Status, stop-payment, replacement, and account-protection options
Payment app	App/service + linked bank/card as applicable	What each layer can address; no universal first call

FACTS, NOT LEGAL LABELS

Describe exactly what happened, who initiated the transfer, and what permission the account owner gave. State clearly when the owner did not make or authorize it. Report suspected errors promptly. Do not guess a legal classification or promise reimbursement.

What Moved? Response Matrix: 2

Ask what options remain. Do not promise reversal, reimbursement, investigation, or recovery.

METHOD	KNOWN PROVIDER / ROUTE	ASK / LIMIT
Gift card	Gift-card issuer	Keep card and receipt when available; ask about freeze/refund options; no guarantee
Cryptocurrency / Bitcoin ATM	Sending service, exchange, ATM operator, funding provider	Typically difficult to reverse; ask what fraud/account options remain
Brokerage	Firm fraud/security/compliance route	Hold, recall, access, and account protection; trusted contact is not authority
Cash / gold / courier	Emergency, delivery, financial-provider, or law-enforcement route as facts require	Safety first; no confrontation or interception
Mailed cash / package	Carrier or delivery service through official route	Ask about intercept/status options; timing and service rules vary

REPORT THE FACTS PROMPTLY

A recall, dispute, freeze, intercept, or recovery request is not a promise of success. Report promptly; ask about deadlines and required written follow-up.

Credentials, Email, Phone, and Account Checklist

Use a known device not implicated in the incident where feasible.

[ ] End the contact and stop further access.
[ ] Identify the primary email and recovery chain.
[ ] Identify exposed passwords, codes, accounts, sessions, recipients, beneficiaries, addresses, or settings.
[ ] Contact affected provider(s) through known routes.
[ ] Ask what session sign-out, recovery-route, phone-number, account-setting, or access protections apply.
[ ] Contact the carrier through a known route when the number, SIM, account, or port-out controls may be compromised.
[ ] Follow provider instructions and keep the account owner involved as required.
[ ] Record case number, instructions, owner, date, and unresolved exposure.

DO NOT

Use the suspected contact’s link or support number; write credentials or codes in this form; or impose one universal account-recovery sequence.

Identity Exposure Checklist

Match the response to the information actually exposed.

[ ] Identify the category of identity information without copying the sensitive value here.
[ ] Use IdentityTheft.gov through a route selected independently.
[ ] Consider credit freeze or fraud-alert choices based on the actual exposure.
[ ] Review existing accounts separately; new-credit protections do not secure them.
[ ] Contact affected providers for existing-account or access concerns.
[ ] Record reports and provider case numbers.
[ ] Assign follow-up and next review date.

Identity category exposed	
Official route used	
Report / case number	
Existing accounts separately reviewed	[ ] YES [ ] NOT APPLICABLE
Owner / next date	

NEVER RECORD THE SSN OR DOCUMENT IMAGE HERE
This checklist stores categories and case numbers only.

Remote-Access and Device Response Card

Use provider or qualified technical support. Do not conduct amateur forensics.

1. Stop further action and end the session.
2. Do not re-engage the contact, even to “undo” the session.
3. Use a known device not implicated in the incident where feasible.
4. Contact a known provider or qualified technical-support route.
5. Identify accounts used, displayed, or plausibly accessible during the session.
6. Route affected email, banking, brokerage, payment-app, carrier, and identity exposure separately.
7. Follow provider-supported instructions.
8. Record who was contacted and what remains unresolved.

DO NOT

Diagnose malware, trace the attacker or cryptocurrency, inspect a device covertly, or apply one universal cleanup sequence.

Provider Contact Log / Family Action Log

Track provider instructions, owners, and dates. Keep sensitive data out.

DATE / TIME	PROVIDER / KNOWN ROUTE	FACTS REPORTED	REP / CASE NUMBER	INSTRUCTIONS / NEXT STEP	OWNER / DATE

DO NOT RECORD

Passwords, codes, security answers, full account numbers, SSNs, identity images, unsupported legal labels, diagnoses, or outcome guarantees.

First-Day and Seven-Day Follow-Up List

Complete only the actions that match the actual exposure and provider instructions.

FIRST DAY: AS APPLICABLE

- [ ] Finish provider-directed urgent actions.
- [ ] Contact connected providers identified during first calls.
- [ ] Secure the primary recovery chain through provider-supported steps.
- [ ] Complete applicable identity/credit actions.
- [ ] Preserve records and case numbers.
- [ ] Make applicable public reports.
- [ ] Assign unresolved items.

NEXT SEVEN DAYS: AS APPLICABLE

- [ ] Follow up on provider cases.
- [ ] Review affected accounts and alerts with the owner or authorized person.
- [ ] Complete provider-directed replacement or recovery steps.
- [ ] Review connected accounts and recovery routes.
- [ ] Complete credit/identity follow-up.
- [ ] Document new recovery offers.
- [ ] Update the family plan and schedule a no-blame review.

Unresolved item	
Owner	
Next contact date	
Case / reference number	

NOT A UNIVERSAL CHECKLIST

A gift-card incident does not automatically require device work. Follow only the branches that fit.

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.

Maintenance Dashboard

One current snapshot of the plan. No balances, credentials, or ratings of any person.

Last reset date	
Cadence selected	[ ] MONTHLY [ ] QUARTERLY [ ] OTHER
System status	[ ] STABLE [ ] OPEN ITEMS [ ] TARGETED REVIEW [ ] DEEPER REVIEW [ ] INCIDENT EXIT
Number of open actions	
Next review date	
Annual reset month	
Dated resource page last verified	
One current plan-improvement note	

INCIDENT EXIT

If money, credentials, identity information, account/recovery settings, software, screen sharing, or device access may have moved, stop maintenance and use Branch B and Chapter 11; toolkit Exposure Sort (POST-01), First Response Card (POST-02), and Response Matrix (POST-04A/B).

Open Actions & Owner Log

The assigned owner is responsible for following up, not for controlling the parent's account, device, or decision.

ACTION CATEGORY	SHORT ACTION	STATUS	OWNER	PERMISSION / PROVIDER DEPENDENCY	TARGET DATE	NEXT REVIEW

STATUS OPTIONS

OPEN / WAITING ON PROVIDER / COMPLETED / DECLINED / NOT AVAILABLE / NOT APPLICABLE

Roles, Consent, and Known Routes Check

Update family records and provider-recognized arrangements separately.

ITEM	STILL CURRENT?	CHANGE / OWNER / DATE
Parent/account owner and participants		
Primary trusted person		
Backup trusted person		
Optional local support		
Permissions and prohibitions		
Voluntary sharing arrangements		
Known family routes		
Bank/card/brokerage routes		
Primary email/carrier/device routes		
Emergency and local routes		

FORMAL CHANGE RULE

A family record does not change a provider role, account permission, ownership arrangement, power of attorney, or other legal status. Use the provider or legal process.

Guardrail & Recovery Status Check

Review status only. Never copy the credential, code, balance, or report contents.

CATEGORY	STATUS	BURDEN / CHANGE	OWNER / DATE
Selected account alerts			
Duplicate notice or visibility, if any			
Brokerage trusted contact			
Provider restrictions / transfer controls			
Credit freeze / fraud alert / credit-report choice			
Primary email / recovery phone or email			
MFA category			
Backup/recovery-code private storage status			
Device update / backup status			
Carrier / SIM / port-out status			

Trigger-Event Review Map

When something changes, decide whether it calls for a targeted review, a deeper review, or incident response.

ROUTE	USE WHEN	EXAMPLES
Targeted review	One part changed	Phone/number/carrier; email/recovery; bank/card/app; one trusted person; one alert burden; provider route
Deeper Chapter 3 review	Several parts changed or priorities no longer match real life	Multi-exposure incident; major move; household/caregiving transition; retirement; bereavement; extended hospitalization
Incident exit	Value or access may have moved	Unfamiliar transaction/account; code disclosed; recovery change; software or remote access; identity misuse

ROUTING FACTS, NOT CAPACITY SIGNALS

A new relationship, adviser, caregiver, charity, contractor, platform, or payment method may justify checking the request rule. It does not authorize surveillance.

Annual Full Reset Checklist

Review the whole system once each year on a date the family will keep.

[ ] Parent confirms participants and cadence.
[ ] People and roles reviewed.
[ ] Consent and voluntary visibility reviewed.
[ ] Known routes reverified.
[ ] Communication-screening choices reviewed.
[ ] Financial alerts and provider guardrails reviewed.
[ ] Identity/credit choices and planned report review addressed.
[ ] Primary email and recovery chain reviewed.
[ ] Phone/carrier and devices reviewed.
[ ] Emergency page, incident card, and provider directory reviewed.
[ ] Open actions resolved or reassigned.
[ ] Obsolete routine copies retired.
[ ] One constructed scenario drill completed.
[ ] Next annual reset scheduled.

Annual reset date	
One plan improvement	
Owner / date	

Annual Scenario Drill Card

Use a constructed scenario. This tests the plan, not the person.

Scenario used	
What stays still?	
Which known route?	
Who is the trusted person?	
Did anything move or change?	[ ] NO [ ] YES [ ] NOT SURE
Branch	[ ] A [ ] B
SCREEN	USED / MISSED / NOT NEEDED
AUTHENTICATE	USED / MISSED / NOT NEEDED
FREEZE	USED / MISSED / NOT NEEDED
ESCALATE	USED / MISSED / NOT NEEDED
One plan improvement	
Owner / date	

NEVER TOTAL THE MARKS

No score, grade, pass/fail result, capacity inference, vulnerability rating, or effectiveness claim.

Dated Resource & Source Refresh Register

The last-verified date tells you when a route was checked; it doesn't guarantee the route is still current.

FUNCTION / RESOURCE	OFFICIAL ROUTE / SOURCE	LAST VERIFIED	NEXT CHECK	OWNER	STATUS

VOLATILE DETAILS

Phone numbers, URLs, hours, portal steps, platform menus, carrier features, and provider procedures require periodic and upload-day refresh.

Record Retirement & Incident File Guide

Keep one current routine set and keep incident/provider records separate.

ROUTINE PLAN RECORDS	INCIDENT / PROVIDER RECORDS
• Keep one current family-plan set. • Mark replaced copies SUPERSEDED. • Remove obsolete duplicates from routine use. • Never let the current set become a credential vault.	• Keep case/reference numbers. • Keep incident chronology and preserved original communications. • Keep provider instructions and applicable reports. • Keep dispute, insurance, tax, legal, or law-enforcement records where applicable.

NO UNIVERSAL DESTRUCTION DATE

Do not destroy an incident or provider record while it may still be needed. Follow provider instructions and applicable qualified legal, tax, insurance, or professional advice.

Current routine set location	
Incident file location	
Last version review	
Next review	

Dated Public Resources: Immediate & Federal

Public routes checked 2026-09-10. Confirm the official route before use.

RESOURCE	CURRENT ROUTE	PURPOSE / LIMIT
Emergency services	911 or appropriate local emergency service	Immediate physical danger, suspected scam courier at the home or on the way, or credible threat; not every scam contact is a 911 matter
FTC ReportFraud	https://reportfraud.ftc.gov/	General consumer-fraud reporting; not individual account resolution
IdentityTheft.gov	https://www.identitytheft.gov/	Identity-theft report and tailored recovery plan; match actions to exposure
FBI Internet Crime Complaint Center	https://www.ic3.gov/	Internet-enabled crime complaint; no status or outcome guarantee
CFPB financial-product complaints	https://www.consumerfinance.gov/complaint/	Scam routing and complaints about covered financial products; contact the affected provider promptly. A complaint does not guarantee repayment or extend deadlines.

PROVIDER FIRST WHEN MONEY OR ACCESS MAY BE AT RISK
Use the number on a card or statement, an official app opened independently, or another route your family already verified.

Dated Public Resources: Support & Local

National routes checked 2026-09-10. State and local eligibility and process vary.

RESOURCE	CURRENT ROUTE	PURPOSE / LIMIT
National Elder Fraud Hotline	833-372-8311 Mon–Fri, 10 a.m.–6 p.m. ET	Federal support and referral for adults age 60+ affected by financial fraud; not emergency services
Eldercare Locator	800-677-1116 https://eldercare.acl.gov/	Find local aging-network resources; availability varies
Adult Protective Services	Use current official state/territory route or national locator	Possible abuse/exploitation where facts and local eligibility fit; age or disagreement alone is not enough
Social Security scam information	https://www.ssa.gov/scam/ https://oig.ssa.gov/report/	SSA scam information and OIG reporting; verify current route independently
Local police / state attorney general	Use the current official local or state route	Use as facts, jurisdiction, danger, and documentation needs warrant; no universal order

SUPPORT IS NOT A PROMISE

A hotline, agency, or support resource cannot guarantee investigation, resolution, reimbursement, or recovery.

Dated Public Resources: Financial & Platform

Public routes checked 2026-09-10. Verify provider and platform details separately.

RESOURCE	CURRENT ROUTE	PURPOSE / LIMIT
SEC / Investor.gov help	https://www.investor.gov/contact-us 800-732-0330	Investor help and complaint information; contact actual firm first when money or access is at risk
FINRA BrokerCheck	https://brokercheck.finra.org/	Check broker/firm records; a genuine record does not verify the messenger
AnnualCreditReport	https://www.annualcreditreport.com/	Authorized free credit-report route; availability/frequency may change
FTC credit freeze / fraud alert	https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts	Explains new-credit protections; does not secure existing accounts
Affected provider	Card/statement number, official app, prior verified correspondence, or family directory	First operational route for affected accounts, transactions, carrier, platform, or device
Official platform support	Official Apple, Google, Microsoft, Meta, carrier, bank, or brokerage support page reached independently	Use for current menus, features, recovery, and provider procedures; never use a contact-supplied link

Version and Refresh Notice

Version 1.3.4 | 2026. Public resource routes checked 2026-09-10; verify current provider and local instructions before use.

WHAT THIS VERSION IS

Printable family plans, cards, checklists, and response tools for Scams Change. The Rule Doesn't. Use the full toolkit as a reference and print the pages your family needs.

Book and toolkit contact

Tommy Thurman
secondcheckpress@gmail.com

Questions about the book, a missing file, or a broken link are welcome.

This inbox is not an emergency response service. If money or access is at risk, use the response steps and contact the affected provider through a known route.

Keep your family's completed worksheets and incident records private.

Do not email passwords, verification codes, account numbers, or other sensitive details.

When replacing a toolkit copy

- Mark the old routine copy SUPERSEDED.
- Keep incident/provider records separate.
- Update the last-verified date.
- Do not destroy records that may still be needed.

NO GUARANTEE

The toolkit cannot guarantee that a scam is recognized, prevented, stopped, reversed, reimbursed, investigated, prosecuted, or recovered. It is designed to create time, known routes, and prepared support.

Scams Change. The Rule Doesn't.: Companion Toolkit | Version 1.3.4 | 2026