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	BRANCH B: YES OR UNSURE
• 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.	• 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.