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	NEXT SEVEN DAYS: 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.	• [ ] 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.