NOYACK

Post-Scam Rapid Response Checklist

Post-Scam Rapid Response Checklist

If you suspect you've been scammed, every minute counts. The steps you take in the first hours can make the difference between recovering your funds and losing them permanently.

This checklist is designed to guide you calmly through the process. Keep a printed copy somewhere visible so that you can follow it without second-guessing yourself in a stressful moment.

Step 1: Freeze Funds

☐ Contact your bank or brokerage immediately
☐ Freeze debit and credit cards
☐ Lock crypto accounts or exchanges

Step 2: Secure Accounts

☐ Reset email and financial passwords
☐ Enable MFA (multi-factor authentication)
☐ Revoke suspicious app permissions

Step 3: Document the Scam

☐ Take screenshots of messages, emails, TXIDs, caller IDs
☐ Save suspicious invoices, receipts, or call logs

Step 4: Report the Incident

☐ File with FBI IC3 (ic3.gov)
☐ Report to the FTC (reportfraud.ftc.gov)
☐ Call your bank's fraud department
☐ Notify local law enforcement if applicable

Step 5: Alert Your Circle

☐ Notify spouse, assistant, family, or team
☐ Warn them not to act on urgent requests without voice confirmation

NOYACK

Post-Scam Rapid Response Checklist

Next Steps

If you followed these steps, you've done the critical damage control. In the days that follow, review your Personal Scam Exposure Map and Digital Hygiene Checklist to prevent repeat incidents.

Store both a printed and digital copy of this checklist in an easy-to-reach location. Preparation turns panic into a plan — and protects your wealth.

Keep these numbers visible in case of emergency:

Emergency Hotlines	
Bank Fraud Dept: (varies, check card)	Credit Freeze:
FTC Fraud Hotline: 1-877-382-4357	• Equifax: 1-800-685-1111
FBI IC3: www.ic3.gov	• Experian: 1-888-397-3742
IRS Fraud Hotline: 1-800-366-4484	• TransUnion: 1-800-916-8800
SSA Fraud Hotline: 1-800-269-0271	