I THINK I MAY HAVE BEEN SCAMMED. WHAT DO I DO IN THE FIRST HOUR?

FIRST

1. Stop further payments and stop communicating with the scammer.
2. Contact the bank, card company, or payment provider using official contact information you find yourself.
3. Ask whether a payment can be stopped, reversed, or flagged. Speed matters.

THEN

- Secure your email account and change exposed passwords.
- Review multi-factor authentication and deny unknown sign-ins.
- Freeze or lock cards if appropriate.
- Preserve messages, numbers, receipts, transaction details, and screenshots.

IF PERSONAL INFORMATION WAS EXPOSED

Contact the relevant account providers and consider a fraud alert or credit freeze through official channels.

IF A COMPUTER OR PHONE WAS REMOTELY ACCESSED

Disconnect it from the internet, remove remote-access software with trusted help, and change important passwords from a device you trust.

IF MONEY WAS SENT

Tell the financial institution immediately. Recovery is not guaranteed, but speed can matter.