

Community reporting checklist

Reviewed October 1, 2026

Use this handout after a suspicious message, call, website, payment request, account alert, mailed notice, or QR code.

First, stop the urgent action

- Do not send more money.
- Do not share more codes, passwords, card numbers, account numbers, or identity numbers.
- Do not install remote-access software.
- Do not call back using the number in the urgent message.

Save useful evidence

- Screenshots of messages, emails, profiles, websites, QR notices, and payment requests.
- Phone numbers, email addresses, usernames, websites, wallet addresses, invoice details, tracking numbers, or order numbers.
- Dates, times, payment methods, receipt numbers, and the amount requested or sent.
- A short description of what the person or message asked you to do.

Choose the first reporting path

- Fraud attempts or money losses: <https://reportfraud.ftc.gov/>
- Identity information shared: <https://www.identitytheft.gov/>
- Cyber-enabled loss, account takeover, online fraud, or crypto transfer: <https://www.ic3.gov/>
- Mail fraud or suspicious mailed notices: <https://www.uspis.gov/report>
- Local immediate danger: call local emergency services.
- Bank, card, payment app, marketplace, email, or social account: contact that provider directly through its official app, website, or saved support number.

Recovery notes

- Payment recovery depends on the payment method and how quickly the provider is contacted.
- No outside person can promise to recover lost money for an upfront fee.
- Use a different trusted device when changing passwords if the affected device may be compromised.
- Turn on two-factor authentication where available, but never share one-time codes with unexpected contacts.

Group-use reminder

This handout is educational. It is not legal, financial, law-enforcement, medical, or emergency advice. For account, money, identity, or safety issues, contact the relevant provider, agency, or emergency contact directly.

Sources and sharing

FTC recovery guidance: <https://consumer.ftc.gov/articles/what-do-if-you-were-scammed>

FBI reporting guidance: <https://www.ic3.gov/>

Prepared by Olevo / Infrol Labs LLC; no agency endorsement. Print and share unchanged with credit, date, and sources. Label adaptations.

Updates: <https://olevo.app/community-resources>