Identity Theft & Fraud Prevention

RESPONSE QUICK GUIDE

If you suspect fraud, **act immediately.** Use this checklist to know where to start.

1. REPORT ONLINE FRAUD / CYBER CRIME

- IC3 (FBI Internet Crime Center): https://www.ic3.gov
- BEC (Business Email Compromise Reporting): https://bec.ic3.gov

2. CONTACT FINANCIAL INSTITUTIONS

If wire instructions, bank transfers, or account access may be compromised:

- Notify the bank immediately
- Request a fraud hold
- Ask if a wire recall is possible
- Document every communication and timestamp

3. NOTIFY AUTHORITIES

Depending on the situation:

- Local Police Department
- FBI Field Office
- U.S. Postal Inspection Service (mailbox theft / mail fraud)
- Federal Trade Commission: https://www.identitytheft.gov

4. SECURE ACCOUNTS & DEVICES

- Change passwords immediately
- Enable multi-factor authentication
- Review recent login activity
- Check email for forwarding rules or spoofing indicators
- Run anti-malware scans if needed

5. PRESERVE EVIDENCE

Do NOT delete suspicious emails or texts.

Keep:

- Email headers
- Screenshots
- Documents
- Recorded conversations (if applicable)
- A written timeline of what happened

6. ADVISE CLIENTS TO:

- Freeze credit (Experian, Equifax, TransUnion)
- Enable fraud alerts
- Monitor accounts for at least 90 days