Checklist for Victims

1 Cease All Communication

- Stop all contact with the scammer immediately.
- Do not respond to further messages, emails, or calls.

2 Secure Your Accounts

- Change passwords on all online accounts (email, banking, social media).
- Enable two-factor authentication (2FA) on important accounts.

3 Report the Scam

- **Local Authorities:**
  - File a report with your local police department.
- **Federal Agencies:**
  - Federal Trade Commission (FTC): Report online at: www.ReportFraud.ftc.gov
  - FBI's Internet Crime Complaint Center (IC3): Report cyber-related crimes at: www.ic3.gov
  - U.S. Postal Inspection Service: If mail fraud is involved, report at: www.uspis.gov
  - Securities and Exchange Commission (SEC): If the scam involves investments, report at: www.sec.gov

4 Contact Your Bank or Financial Institution

- Inform your bank, credit card issuer, or payment platform.
- Request to stop or reverse unauthorized transactions.

5 Notify Credit Bureaus if a Financial Crime

- Contact major credit bureaus to report fraud and place alerts:
  - Experian: www.experian.com or call 1-888-397-3742.
  - Equifax: www.equifax.com or call 1-800-525-6285.
  - TransUnion: www.transunion.com or call 1-800-680-7289.
- Consider freezing your credit to prevent new accounts.

6 Check For Unauthorized Transactions

- Review bank statements, credit card bills, and other accounts.
- Dispute any fraudulent transactions immediately.

7 Scan Devices for Malware

- Run a full virus and malware scan on your devices.
- Update your antivirus software and security settings.

8 Monitor Your Identity

- Use an identity theft monitoring service or check your credit report regularly.
- Watch for new credit cards, loans, or accounts opened in your name.

Checklist for Victims

Document Everything

9

- **Communications with the Scammer:**
  - Save all emails, text messages, and chat logs.
  - Take screenshots of conversations, phone numbers, usernames, and email addresses.
  - Record dates, times, and contents of any phone calls (if legally allowed).
- **Transaction Records:**
  - Save all receipts, bank statements, and transaction details.
  - Document cryptocurrency transactions, including wallet addresses and transaction IDs.
  - Keep receipts for cash deposits, noting location and time.

- **Notifications to Credit Bureaus:**
  - Keep records of fraud alerts and credit freezes.
  - Save confirmation emails or letters from credit bureaus.
- **Screenshots of Scam Websites or Social Media Profiles:**
  - Capture scammer websites, social media profiles, or ads.
  - Document URLs and details of the scammer's online presence.
  -

- **Additional Expenses Incurred:**
  - Record costs associated with the scam, such as legal fees, monitoring services, or repairs.
  - Keep receipts or invoices for related expenses.
- **Personal Notes and Timelines:**
  - Maintain a timeline of scam events and actions taken.
  - Note any changes in the scammer's behavior or contact attempts.

10

- **Reports Filed with Authorities:**
  - Keep copies of reports filed with police and federal agencies, including case numbers.
  - Save confirmation em**ails or screenshots of submitted reports.**
- **Correspondence with Financial Institutions:**
  - Record all communications with banks, credit card companies, or payment platforms.
  - Save emails, chat logs, and correspondence records.

- **Evidence of Malware or Device Compromise:**
  - Save reports from antivirus scans showing detected malware or suspicious activity.
  - Note device changes, unauthorized access, or unusual account behavior.
- **Identity Theft or Fraudulent Activity Alerts:**
  - **Keep alerts from identity theft monitoring services.**
  - **Document suspicious activity or unauthorized accounts opened in your name.**
  -

Seek Support

- Reach out to victim support organizations for guidance and emotional support.
- Contact local consumer protection agencies.

Consider Purchasing
an Identify Theft Protection Program

- Look into services like LifeLock, IdentityGuard, or other similar programs for ongoing monitoring and protection.

11

Educate Yourself
and Spread Awareness

- Learn about common scams and fraud prevention tips.
- Share your experience to help educate others.

12

Post-Recovery Actions

- **Update Security Settings**
  - Regularly update security settings on all online accounts.
- **Stay Vigilant**
  - Be wary of unexpected messages, calls, or emails asking for personal information or payments.

13

14

- **Be wary of anyone claiming to be able to recover all of your money for a fee!**

These are often additional scams that prey on desperate victims. Always verify the legitimacy of recovery services through trusted sources and never pay upfront fees.

Important Notes

- **If the scam involved cryptocurrency, speed and thorough documentation are of the essence!**

The faster you act, the better the chances of tracing and potentially recovering lost funds.