THE ESSENTIAL SCAM RECOVERY GUIDE

Step-by-Step Guide on how to Get Your Assets Back From Scams

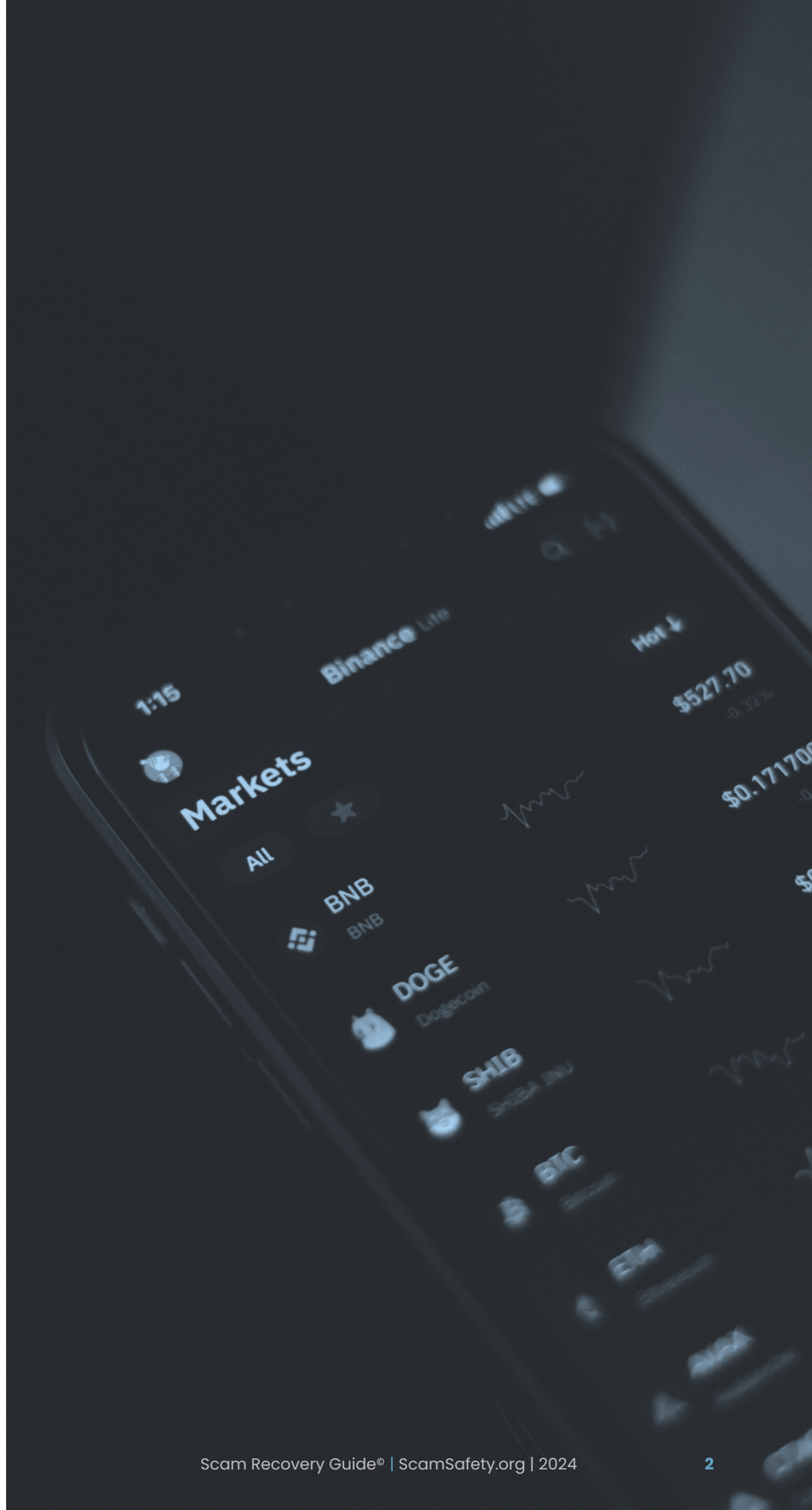
ScamSafety.org

Updated for 2024

Welcome

Dear Friend, first and foremost I want to personally commend you on taking the first and important step to recovering your assets. No matter your background, level of wealth, or where you are located, I know firsthand being scammed is a devastating experience. It can leave you feeling violated, angry, and ashamed. As a result, you may be struggling with financial hardship and emotional trauma, so I want you to know, **you are not alone**. This guide is carefully packaged with important information to give you a fighting chance at **getting your assets back as quickly as possible**. Essentially the information provided to you here is the information I wish I had when I started my asset recovery journey.

In an era marked by unprecedented connectivity, the global prevalence of scams has become a concerning reality. According to statistics published by Group-IB in *The Global State of Scams Report*[1], an estimated **$55 billion was lost globally in 2022 from online scams**, and this number continues to grow. Behind these numbers lie countless individuals who have experienced the emotional and financial toll of falling victim to scams. Today, the lack of awareness and prevention education surrounding scams has created a perfect storm for scammers to prey on unsuspecting victims. This guide aims to help change these alarming statistics and help you navigate the complex and tricky aftermath of being scammed.



1. *The Global State of Scams Report*—Group IB

Purpose of this Guide

This comprehensive recovery guide is specifically designed to help you navigate the complex and overwhelming aftermath of scams, empowering you with the knowledge and resources to **improve your chances at getting your money back**. It is also crafted with the understanding that recovery extends beyond financial restitution— encompassing **rebuilding trust**, **reclaiming control**, and **emerging stronger**. While this guide provides you with the *step-by-step* instructions to give you a fighting chance at recovering your assets, you can start at any point where you think is most effective to your current situation.

Who this is For

People Who

1. Have **lost money or crypto** to a scam.
2. Want an **effective approach** to recovering their funds as quickly as possible.
3. Want to know how to document their evidence and create a detailed **Incident Report** to provide to police, banks, exchanges, and law firms.
4. Want to know how to **secure their digital wallets**.
5. Want to **avoid asset recovery scams**.
6. Want to learn a simple and effective way to **trace their lost crypto** on the blockchain to assist with the recovery process.
7. Want to know how to **engage with their bank**.
8. Want to know how to **engage with law enforcement**, and who to contact locally and internationally.
9. Want to know how to **engage with exchanges**.
10. Want to know how to **engage with legitimate crypto tracing services.**
11. Want to know how to **engage with the right law firm**

Important Things to Keep in Mind

- The sooner you report the scam, the higher your chances of minimizing losses and potentially recovering your funds.
- Provide as much detail as possible about the scam, including any emails, phone conversations, or transaction information you have.
- Follow up with your bank or credit card company to get updates on the investigation and keep them informed if you discover any new information.

Disclaimer

Important Information

- **This guide is for informational purposes only and does not constitute legal advice.** Please consult with a qualified legal professional for any specific legal questions or concerns related to your individual situation.
- **The success of any recovery efforts is highly dependent on the specific circumstances of each case and cannot be guaranteed.** This guide provides general information and strategies but may not be applicable to all situations.
- **We make no promises or guarantees of any financial recovery or reversal of losses incurred.** The strategies outlined in this guide are provided in good faith but may not be successful in all cases.
- **We assume no responsibility for any consequences arising from the use of this guide.** You are solely responsible for the outcomes of any actions you take based on the information provided herein.
- **This guide is protected by copyright and intellectual property laws.** Unauthorized reproduction or distribution of this guide is strictly prohibited.

Additional Information

- **Always report scams to the appropriate authorities.** This includes notifying your bank, law enforcement agencies, and relevant consumer protection agencies.
- **Be cautious of anyone offering "guaranteed" scam recovery services.** Legitimate recovery efforts can be complex and time-consuming, and there is no magic bullet or quick fix.
- **Protect your personal information.** Be wary of sharing sensitive information with anyone you don't know and trust, especially online.
- **Stay informed about current scams.** Scammers frequently adapt their tactics, so it's important to stay updated on the latest trends and threats.

Contents

What to do Immediately

- ❑ Stop Sending Any More Money.
- ❑ Secure Your Compromised Accounts.
- ❑ Secure Your Digital Wallets.
- ❑ Document Your Evidence.
- ❑ Build Your TimeLine.
- ❑ Build an Incident Report.
- ❑ Contact Your Bank.
- ❑ Contact an Ombudsman.
- ❑ Contact Law Enforcement.
- ❑ Contact Your Exchanges.
- ❑ Asset Recovery Services.

Tracing Your Funds

- ❑ Crypto Tracing.
- ❑ Using Blockchain Explorers.
- ❑ Tracing Your Funds.
- ❑ Crypto Tracing Services
  - What is a Crypto Tracing Service?
  - How a Crypto Tracing Service Can Help.
  - Risks and Limitations to Consider.
  - Example of a Blockchain Transaction Analysis.
  - Tips for Engaging with a Crypto Tracing Service.
  - Key Questions to Ask.

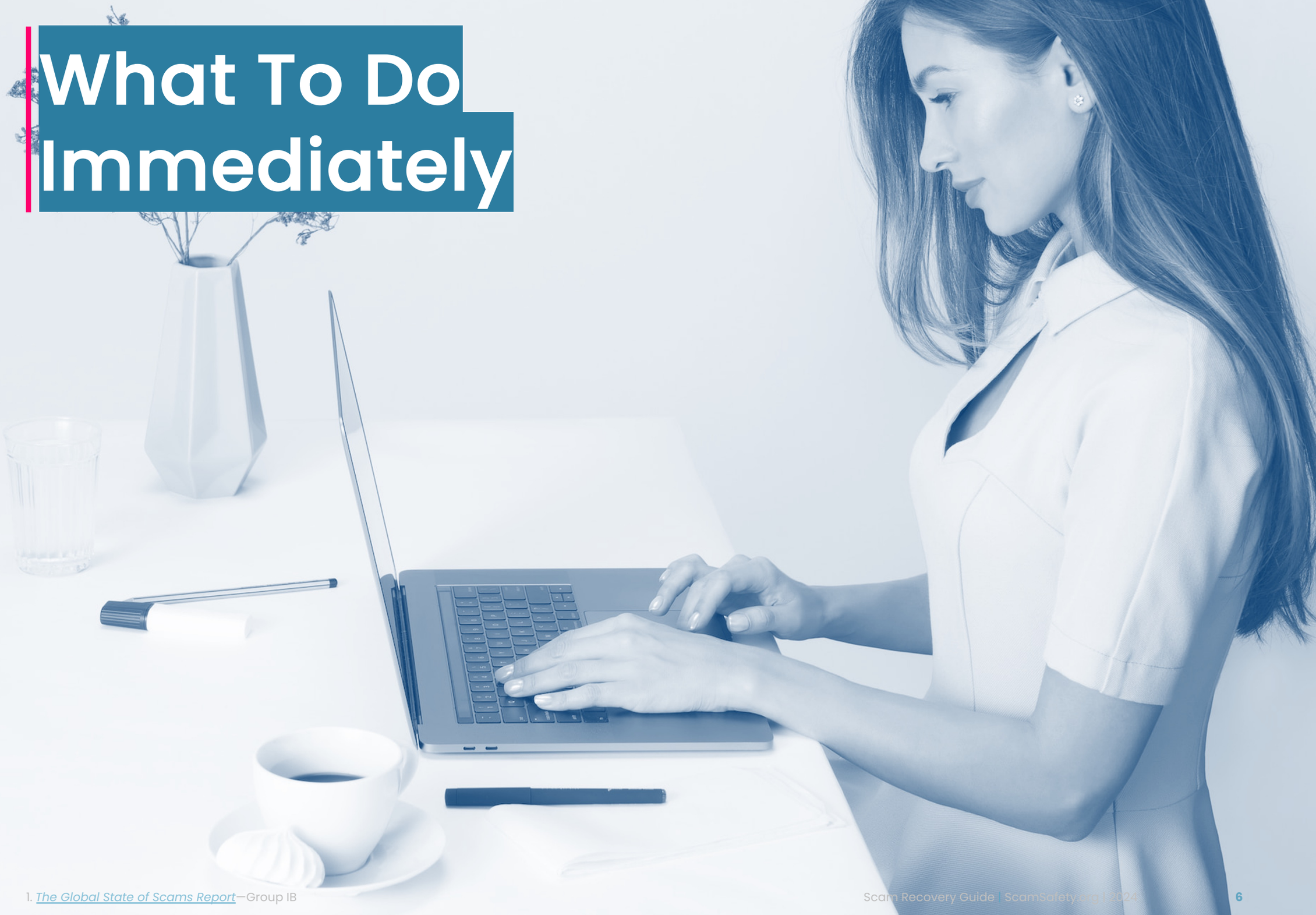
Obtaining Legal Assistance

- ❑ Legal Services.
  - Purpose of Engaging a Law Firm.
  - How a Law Firm Can Help.
  - Risks and Limitations to Consider.
  - Tips for Engaging with a Law Firm.
  - Key Questions to Ask.

Additional Resources

- ❑ Personalized assistance with engaging crypto tracing and professional legal services.
- ❑ From Local Authorities.
- ❑ From Exchange Services.

What To Do Immediately



1. *The Global State of Scams Report*—Group IB

Stop Sending Any More Money

If whoever you are dealing with is asking you to send more money whether it be in the form of crypto currency or fiat currency, **do not send any more funds to them**. For example, no legitimate company should be asking you to send them *more* money for you to get access to your money again. Deny the request and ask for information as to why they are asking you to send more money. Get them to explain it in detail and for them to provide you with their company documentation as this information may be useful to provide to law enforcement and to a law firm if needed later down the track.

It is also important to remember you should **never give out your personal information**, such as your government ID number, credit card number, and bank details to anyone you do not know. If someone asks you for this information, it is a possible sign they are trying to scam you.

- If you are unsure whether someone is legitimate, it is always best to err on the side of caution and **to not** send them any money. Instead, contact the company directly and ask them to send evidence that verifies they are a legitimate entity and that they are authorized to collect payments on behalf of the company. This evidence could include a copy of the company's business license, a tax identification number, or a letter from the company's president or CEO.
- If you are still unsure whether the person or company is legitimate, you can also contact the Better Business Bureau (BBB) or the Federal Trade Commission (FTC). These organizations can provide you with information about the company's history and complaints that have been filed against them.

If you are in a situation where someone is asking you to send them more money, whether it be in the form of crypto currency or fiat currency, it is important to **be very careful**. There are many scammers out there who will try to take advantage of people by asking them to send money for various reasons. Things to keep in mind if someone is asking you to send them money:

- **Never send money to someone you don't know**. This is a basic rule of thumb that you should always follow, no matter how urgent the situation seems. If you don't know the person or have never met the person, there's no way to know if they're legitimate or not.
- **Be suspicious of anyone who asks you to pay with cryptocurrency**. Cryptocurrency is a relatively new and unregulated form of currency, which makes it a popular choice for scammers. If someone is asking you to pay with cryptocurrency, be sure to do your research first to make sure they're legitimate.
- **Ask for more information**. If someone is asking you to send them money, don't be afraid to ask for more information about why they need the money and how they'll use it. This will help you to determine if the request is legitimate or not.
- **Trust your gut**. If something doesn't feel right, don't do it. If you're feeling pressured or suspicious, it's best to walk away.

Secure Your Compromised Accounts

Securing your compromised accounts is paramount to **minimize further damage** and **protect your financial well-being**. It is crucial, therefore, to take swift and decisive action so outlined below are the steps on what you should do:

1. **Change Your Passwords**
   Changing your passwords is crucial to prevent ongoing unauthorized access. Scammers may have gained access to your accounts through compromised login credentials, therefore consider changing your passwords to ensure your accounts are secure. Where possible, enable Two-Factor Authentication (2FA) as an additional layer of security to your accounts.

2. **Contact Your Bank and Credit Card Companies Immediately**
   Informing your bank and credit card companies promptly allows them to implement security measures and investigate any unauthorized transactions. This immediate action helps to prevent additional financial losses, secures your accounts against further exploitation, and possibly reverse transactions made.

3. **Have Details Prepared**
   Having specific details prepared streamlines the resolution process.
   - Be ready to provide information on suspicious transactions, including **dates**, **amounts**, and any relevant transaction **reference numbers**.
   - Having your account information, such as account numbers and associated contact details, readily available assists in quickly identifying and addressing the issues. More on this, on pages 10-12.

4. **Report Fraudulent Transactions and Block Further Unauthorized Access**
   Reporting fraudulent transactions promptly is your first line of defence.
   - Contact your bank's fraud department and credit card issuer through their designated channels.
   - Clearly communicate the details of the scam, emphasizing the urgency of blocking any further unauthorized access.
   - Request a freeze or block on your compromised accounts to prevent additional transactions.
   - Ask your bank or credit card company for any additional security measures that can be taken to ensure comprehensive protection against potential scams in the future.
   - Swift and proactive reporting is your first line of defence in reclaiming control over your compromised accounts.

It is important to take these steps promptly because online **scammers often act quickly**, and delaying your response may allow them to exploit your accounts further. By acting swiftly, you not only protect your financial assets but also contribute to the ongoing investigation and prevention of similar scams affecting others. Your proactive approach is crucial in reclaiming control and mitigating the impact of the scam on your financial security.

Secure Your Digital Wallets

Digital wallets, also known as e-wallets or electronic wallets, are software-based tools that allow users to *store*, *manage*, and *transact* with their digital assets. These assets can include various forms of currency, loyalty points, payment cards, and, in the context of cryptocurrencies—digital tokens. Digital wallets provide a secure and convenient way for users to access and utilize their financial resources in the digital realm and come in two forms, **Custodial** and **Non-Custodial**.

- **Custodial Digital Wallets:** In custodial wallets, users trust a third-party service provider (such as a bank or exchange) to manage their private keys and secure their digital assets. Users create accounts with these providers, and the provider holds custody of the private keys.

- **Non-Custodial Digital Wallets:** Non-custodial wallets, on the other hand, give users full control over their private keys. Users are responsible for storing and securing their private keys, and they can transact directly on the blockchain without relying on an intermediary.

Types of Digital Wallets

Custodial	Non-Custodial
Examples include wallets provided by banks, online payment platforms, and centralized cryptocurrency exchanges.	Examples include software wallets (desktop, mobile, or web-based), hardware wallets, and paper wallets designed for managing cryptocurrencies.

Ownership and Control

Custodial	Non-Custodial
Users of custodial wallets rely on the service provider to safeguard their private keys. While this can offer convenience, it also means that users are dependent on the security measures implemented by the custodian.	Users in non-custodial wallets have sole ownership and control of their private keys. This decentralization aligns with the principles of cryptocurrencies, emphasizing user autonomy and reducing reliance on centralized entities.

Security Considerations

Custodial	Non-Custodial
Security in custodial wallets is primarily managed by the service provider. Users trust the provider's security infrastructure to protect their assets.	Security in non-custodial wallets is more user-dependent. While users have greater control, they must take proactive measures to secure their private keys, such as using hardware wallets, secure backup solutions, or following best practices for key management.

Secure Your Digital Wallets

The following are general guidelines to securing both *custodial* and *non-custodial* wallets. Specific steps may vary based on your type of wallet and the service provider therefore, we advise you refer to the specific security recommendations provided by your digital wallet or platform provider.

If you still have digital assets or NFTs tied to your compromised account that you cannot transfer out, you can **use this form** to get help from a group of Whitehat's organized by *Flashbots* with recovering your remaining assets.

Steps for Securing Custodial Wallets

1. **Contact Customer Support**
   Immediately contact the customer support team of the custodial wallet service. Report the scam, provide details of the incident, and inquire about the steps they recommend for securing your account.
2. **Change Passwords**
   Change your account passwords associated with the custodial wallet. Use strong, unique passwords and avoid using the same password across multiple platforms.
3. **Enable Two-Factor Authentication (2FA)**
   If not already enabled, activate 2FA on your custodial wallet account. This adds an extra layer of security by requiring a secondary verification method, such as a code from a mobile app.
4. **Review Account Activity**
   Regularly monitor your account activity for any suspicious transactions. Most custodial wallet platforms provide tools for tracking and reviewing your transaction history.
5. **Check Linked Email Security**
   Ensure the email account linked to your custodial wallet is secure. Change the email password, enable 2FA on the email account, and review security settings.

Steps for Securing Non-Custodial Wallets

1. **Access Wallet Safely**
   If you use a software or mobile-based non-custodial wallet, ensure that your device is secure. Use secure passwords and enable biometric authentication if available.
2. **Secure Private Keys**
   If your non-custodial wallet uses a *seed phrase* or *private key*, ensure it is stored securely offline. Avoid storing it on easily accessible digital devices or cloud storage.
3. **Change Wallet Passwords**
   If your non-custodial wallet has a password, consider changing it to a new, strong password. Ensure that the new password is not easily guessable.
4. **Review and Secure Backup**
   If you have a backup of your wallet (e.g., a hardware wallet or paper wallet), ensure it is secure. Review backup procedures and create a new backup if necessary.
5. **Check for Unauthorized Access**
   Review your wallet activity and check for any unauthorized access or transactions. Many non-custodial wallets provide transaction history and account activity logs.
6. **Update Wallet Software**
   Ensure that you are using the latest version of your non-custodial wallet software. Developers often release updates with security improvements.
7. **Consider Hardware Wallets**
   If security is a top priority, consider using a hardware wallet for your non-custodial wallets. Hardware wallets provide an extra layer of physical security, and we recommend the Trezor Safe 3.

Document Your Evidence

Collecting thorough and accurate evidence is **crucial to build your case**, report your incident to authorities, and potentially recover your lost funds. The following are the types of evidence you should collect with a brief explanation to why they are important. The following page provides a template to collect this information.

Communication Records

- **What to Collect:** Save copies of all communications with the scammer, including emails, text messages, or chat logs.
- **Why it's Important:** Communication records provide a timeline of interactions, helping to establish the scam's progression. They also serve as evidence of any false promises, misrepresentations, or fraudulent activities.

Transaction Details

- **What to Collect:** Record details of financial transactions related to the scam, including dates, amounts, transaction IDs, and account information.
- **Why it's Important:** Transaction details are crucial for authorities and financial institutions to investigate and trace the flow of funds. They provide concrete evidence of the financial impact of the scam.

Bank Statements and Financial Records

- **What to Collect:** Secure copies of relevant bank statements and financial records (e.g., international transfers, and credit card transactions linked to your funds) showing transactions related to the scam
- **Why it's Important:** Bank statements and financial records serve as concrete evidence of financial loss and can be crucial when reporting the scam to financial institutions and law enforcement. They can also serve as critical "entry" points invaluable for forensic analysis and to provide investigators the records they need to prove ownership of the funds.

Legal and Reporting Documentation

- **What to Collect:** Keep records of any reports filed with law enforcement agencies, regulatory bodies, or consumer protection organizations.
- **Why it's Important:** Legal and reporting documentation establishes a formal record of the scam, facilitating investigations and providing a basis for potential legal action.

Screenshots and Website URLs

- **What to Collect:** Critical to building your case will be the evidence you will provide so taking screenshots/images of everything related to the scam is important. Below is a list of what you should take screenshots of. It is not an exhaustive list so ensure to include screenshots of anything else you think is relevant to your case.
  - ❑ All transactions made with your wallet.
  - ❑ All transactions made with your exchange.
  - ❑ All transactions made with the platform, program, website you were interacting with.
  - ❑ All communications with the scammers including with their customer support through online chat or email. Be sure to include any other relevant communications that may have occurred on other platforms (e.g., WhatsApp, Facebook, Instagram, etc.).
  - ❑ All relevant webpage's and/or the app.
  - ❑ The URL of the website or app.
  - ❑ Any emails, text messages, and records of phone calls.
  - ❑ Any social media posts related to the scam.
  - ❑ Any advertisements that led you to the scam.
  - ❑ The platform, program, website you were interacting with.
- **Why it's Important:** Screenshots and URLs serve as visual evidence of the scam's online presence. They can be used to demonstrate deceptive practices, fake websites, or misleading content.

Social Media Screenshots

- **What to Collect:** Capture screenshots of any social media interactions (e.g., through Facebook or Instagram) related to the scam, including messages, profiles, and posts.
- **Why it's Important:** Social media evidence can help establish the scammer's identity and activities. It may also demonstrate the scam's impact on the victim's social network.

Email Headers

- **What to Collect:** Extract and save the email headers of any scam-related emails.
- **Why it's Important:** Email headers contain metadata that can help trace the origin of emails. They can be crucial for authorities in identifying the source and investigating the scam.

Witness Statements

- **What to Collect:** If there were witnesses to the scam, obtain statements from them describing what they observed or experienced.
- **Why it's Important:** Witness statements provide additional perspectives on the scam, corroborating the victim's account and potentially strengthening the case.

Thank You.

Dear Friend,

You've reached the end of the first 10 pages of the full guide, and we hope this preview has given you a taste of the valuable insights and actionable steps you can take to recover your funds. We didn't get to the best parts, but we hope it's given you a sense of having the full roadmap to navigate the complex asset recovery process and **reclaim what's rightfully yours**.

The full guide delves deeper, equipping you with:

- **Proven Strategies**: Uncover effective methods tailored to your specific situation, increasing your chances of success.
- **Expert Insights**: Learn from experts and my experience and gain invaluable knowledge to empower your ability to recover your funds.
- **Step-by-Step Guidance**: Eliminate confusion with clear instructions, ensuring you move forward with confidence.

Can you afford to let this opportunity slip away? Are you willing to do what it takes to give yourself the best chance at recovering your funds? If so, take the next step in your asset recovery journey and get the complete guide today. **Thank You** for taking this initial step–now, let's unlock your full potential for recovery.

Best Wishes.

Scam Safety