



Data
Forensics®

Investigation Summary
Initial Report

Prepared by
DataForensics

Prepared for [REDACTED]
[REDACTED] 2025

Disclaimer

This report has been prepared exclusively for [REDACTED] and their legal representative. No material in this report may be distributed or reproduced without written permission, except for use by law enforcement. Without limitation, this report does not offer any legal guidance or advice of any kind on any subject. In no event shall DataForensics be liable for any damages resulting from, arising out of, or in connection with the use of the information in this report.



**Data
Forensics**

Table of Contents

Terminology.....	3
Preventive measures.....	4
Investing Scam Statistics.....	6
Information From The Client.....	7
Key Findings:.....	8
Investigation Tree Overview.....	9
Phone number analysis.....	10
Further phone analysis:.....	11
Person name analysis.....	12
Domain Investigation.....	15
Domain analysis.....	15
Further domain analysis:.....	16
Conclusion.....	18
Crypto Wallets Overview.....	19
Conclusion.....	20
Summary Of The Findings.....	21



Terminology

OSINT: Open source intelligence

Scam: A fraudulent scheme designed to deceive individuals into providing money, personal information, or both, often under false pretenses.

Crypto Tracing: The process of tracking cryptocurrency transactions and ownership to uncover fraudulent activities or verify financial transactions.

Transaction ID: A unique identifier assigned to a transaction for tracking and verification purposes.

Data Breach: An incident where unauthorized individuals gain access to confidential or protected data, often leading to identity theft or financial loss.

Identity Theft: The unauthorized use of someone else's personal information to commit fraud or other crimes.

Phishing: A type of cyber attack where attackers impersonate legitimate entities to trick individuals into divulging sensitive information, such as passwords or financial details.

Malware: Malicious software designed to harm, exploit, or otherwise compromise a computer system or network.

Ransomware: A type of malware that encrypts a victim's files, demanding payment (ransom) to restore access.

Social Engineering: Manipulating individuals into divulging confidential information or performing actions that compromise security, often through deception.

Fake Credentials: False or misleading information used to deceive others, such as fake job qualifications or financial documents.

Remote Access Software: Programs that allow users to control another computer or device from a distance, often used in tech support scams.

Forensic Analysis: The process of examining and analyzing data to uncover evidence related to cyber crimes or fraud.



Preventive measures

Verify Before You Invest

- Research the Platform: Before investing, conduct thorough research on the investment platform. Look for reviews, regulatory approvals, and whether the platform is registered with financial authorities. Be cautious of new platforms with little or no online presence.
- Verify the Person's Identity: If someone approaches you online with investment advice, verify their identity and credentials. Legitimate financial advisors will have a verifiable track record and will be registered with regulatory bodies.

Be Skeptical of High Return

- High Returns with Low Risk Don't Exist: Be wary of any investment promising high returns with minimal or no risk. Legitimate investments come with risks, and any claim otherwise is a red flag.
- Consult a Financial Advisor: Seek advice from a certified financial advisor before making investment decisions, especially if they involve significant amounts of money.

Avoid Upfront Fees for Withdrawal

- No Legitimate Investment Requires Fees for Withdrawal: Be suspicious if an investment platform asks for fees to release your funds. Legitimate platforms typically do not require additional fees to process withdrawals.
- Question Additional Fees: If asked to pay extra fees, question their necessity and legitimacy. Contact regulatory bodies to verify if such fees are common or required.



Use a Secure Payment Method

- Avoid Cryptocurrency Payments to Unknown Entities: Cryptocurrency transactions are often irreversible, making it difficult to recover funds. Avoid using cryptocurrencies for investments unless you are confident in the platform's legitimacy.
- Use Credit Cards for Protection: When possible, use credit cards for transactions, as they offer more protection against fraud and allow for chargebacks in case of disputes.

Be Wary of Social Media Interaction

- Limit Sharing Personal Information: Avoid sharing sensitive personal or financial information on social media. Scammers can use this information to gain trust or manipulate you.
- Report Suspicious Accounts: If you encounter a suspicious account or receive unsolicited investment offers, report the account to the social media platform and block them.



Investing Scam Statistics

1. Reported Losses and Number of Victims:

- In 2022, nearly \$3.8 billion was lost to investment scams, with over 50,000 reported victims. These scams have surged in recent years, particularly those involving cryptocurrency, where victims reported a median loss of around \$10,000. As the popularity of online investing and digital currencies has grown, so too has the frequency of scams targeting new or inexperienced investors.

2. Methods and Tactics:

- Investment scammers often lure victims through social media, emails, or fraudulent websites promising guaranteed high returns with little to no risk. Common platforms like Facebook, Instagram, and WhatsApp are used to promote fake investment opportunities, particularly in areas like cryptocurrency, forex trading, or real estate. Scammers may pose as legitimate financial advisors or influencers, convincing victims to invest in fraudulent schemes. They might also use fake trading platforms where victims can "invest" and see supposed returns before being asked to add more money, only for the platform to disappear or prevent withdrawals.

3. Common Lies and Schemes:

- A frequent tactic is the promise of "risk-free" investments with quick, guaranteed returns, which don't exist in legitimate investing.
- Scammers often encourage victims to invest in fake cryptocurrency platforms or pump-and-dump schemes where the scammer artificially inflates the value of a stock or currency before suddenly selling, leaving victims with worthless assets.

4. Impact and Demographics:

- New or inexperienced investors, particularly those drawn to high-risk markets like cryptocurrency, are among the most frequent victims. Young adults (ages 18–35) are often targeted due to their growing interest in digital currencies and online trading.



Information From The Client

Summary of The Story – According to The Client:

██████████ joined a trading group via Facebook and WhatsApp under the names "██████████" and "██████████". Initially, she was able to make small withdrawals using the █████ platform. She later joined a "██████████" program, depositing \$50,000 and being pressured to pay further upgrade and service fees, totaling well over \$100,000.

The group simulated profits, showing over \$4.2 million in her account, but repeatedly blocked withdrawals with new demands, including a \$49,000 wire that was never acknowledged. When she refused to pay a final \$13,000, her account was frozen. She later realized many interactions were likely staged, and now believes the entire operation was a scam.

Type of Scam: Investment Scam

How Much Money Was Lost Total: 400,000\$

Names Associated To The Scam:

1. ██████████ (assistant)
2. ██████████ (group leader)
3. ██████████ (alleged member)
4. ██████████ (alleged lawyer)

Leads Given By The Client:

Phone Numbers:

- ██████████ (WhatsApp)
- ██████████ (WhatsApp)
- ██████████ (WhatsApp – old number)
- ██████████ (WhatsApp – old number)

Scam Website Domain Addresses: ██████████

Scam Crypto Wallets: ██████████
██████████



Key Findings:


- **Image Reuse Across Multiple Social Media Accounts**

The WhatsApp profile picture was identified in several unrelated social media accounts under different names. These accounts were short-lived and inactive, indicating the likely use of fake or disposable identities.

- **Strong Chinese Indicators Across the Infrastructure**

Multiple references to the Chinese language and structure were found in the site's metadata and API responses, including untranslated menu items and placeholders. This suggests the platform may originate from or be operated by a Chinese-speaking group.

- **Suspicious Domain Network**

The domain .com was found to be structurally and functionally similar to other suspicious domains. The pattern suggests it may be part of a broader scam network employing template-based scam websites.

- **False Association with Regulatory Bodies**

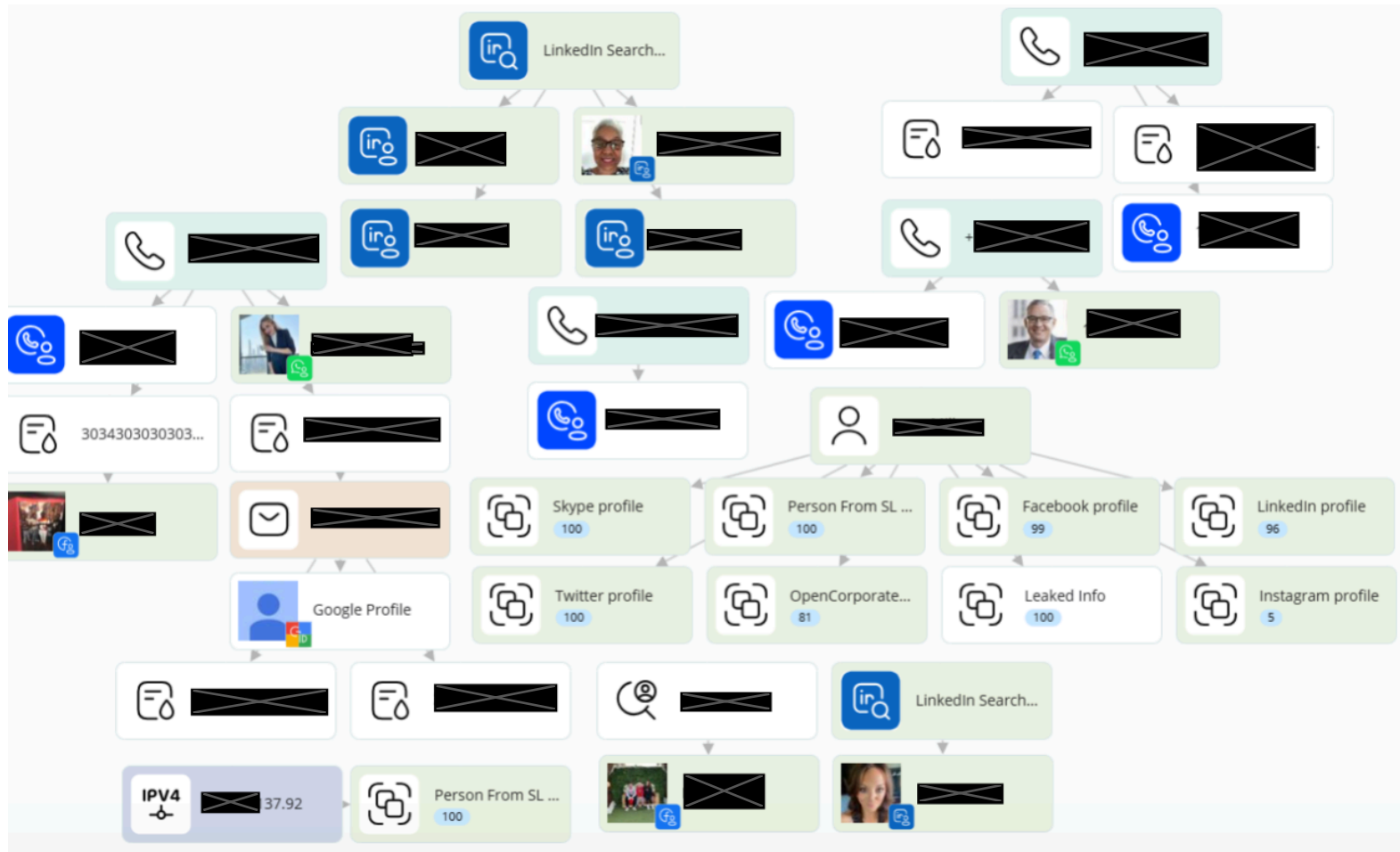
The domain falsely claimed registration with the U.S. National Futures Association (NFA), which was proven to be fabricated through validation on official sources.

- **Centralized Exchange Exposure**

The scammer's wallet sent 97.87% of funds to centralized exchanges. This offers a potential legal pathway for KYC-based identification and asset freezing.



Investigation Tree Overview



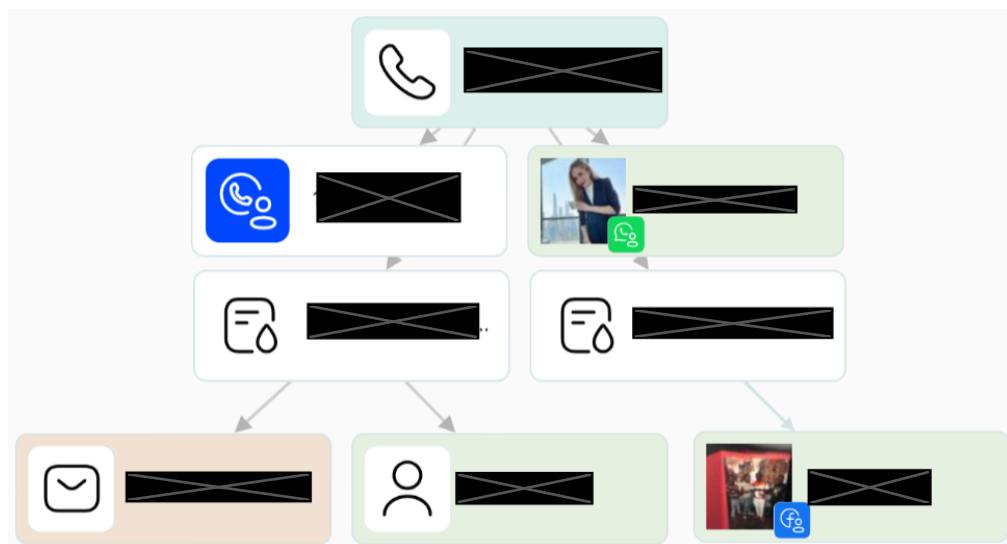
Phone number analysis

+1 [REDACTED]

An analysis of the last phone numbers [REDACTED] revealed connections:

- Trucaller profile:
 - Telecommunication company: T-mobile USA, Inc.
 - Location: Milwaukee, Wisconsin
- Leaked Information: eatstreet.com (2020-05-08)
 - Name: [REDACTED]
 - Email: [REDACTED]
 - Registered date: 2017-03-25
- Leaked Information: Facebook Data (2021-03-09)
 - Facebook id: [REDACTED]
 - Person name: [REDACTED]

The only post associated with this Facebook profile was published on September 8, 2018, and does not reveal any useful information, like location or individual face.



Source: www.facebook.com



Further phone analysis:

The email [REDACTED]@gmail.com was linked to the following findings:

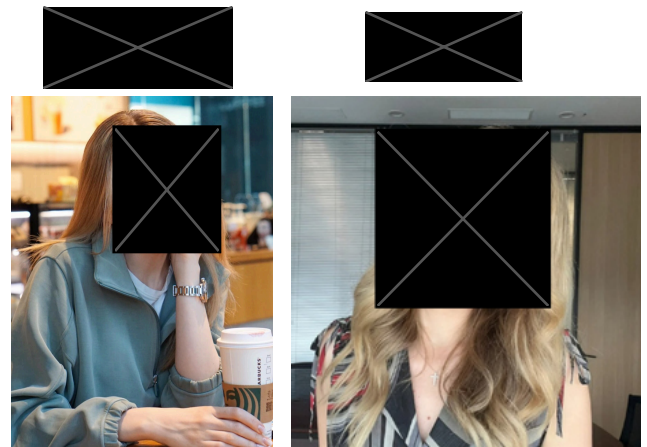
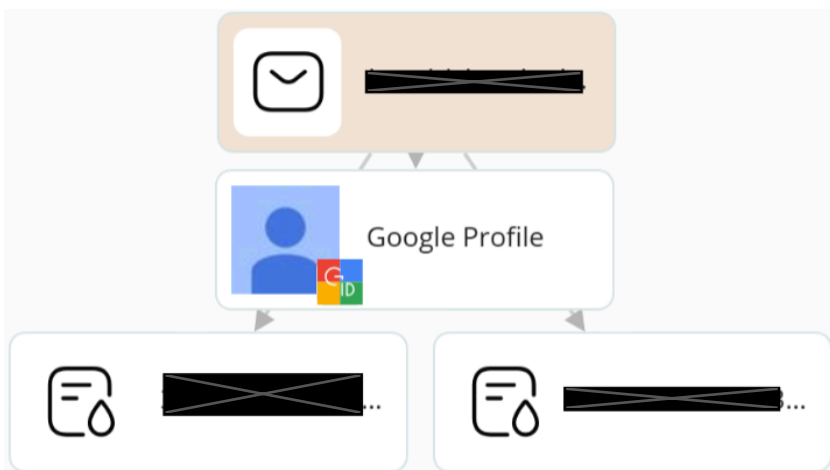
1. A Google profile exists but contains no reviews or significant public data.
2. Email address was found in a leak from [REDACTED].com, registered with the same nickname ([REDACTED]) and a password.
3. It also appeared in a **2020-07-13 data feed** linked to public IP address [REDACTED].137.92, which belongs to **T-Mobile USA Inc.**, located in **Chicago, Illinois, United States**.

The WhatsApp profile picture appears to have been taken in **Shanghai, China**. Distinct architectural landmarks in the background include the **Shanghai Tower**, **Shanghai World Financial Center**, and the **Jin Mao Tower**



Reverse image searches revealed that this photo has been used in multiple recently created social media accounts under different names. These accounts appear to have short lifespans and limited activity, which is consistent with usage in fraudulent identity schemes.

At this stage, we were unable to identify the true identity of the person in the image. The evidence suggests that the photo is being repurposed by scammers to create a false sense of authenticity and trust.



Source: [threads.net/\[REDACTED\]](#) [instagram.com/\[REDACTED\]](#) [threads.net/\[REDACTED\]](#) [xing.com/\[REDACTED\]](#) [z, vk.com/\[REDACTED\]](#)



Person name analysis



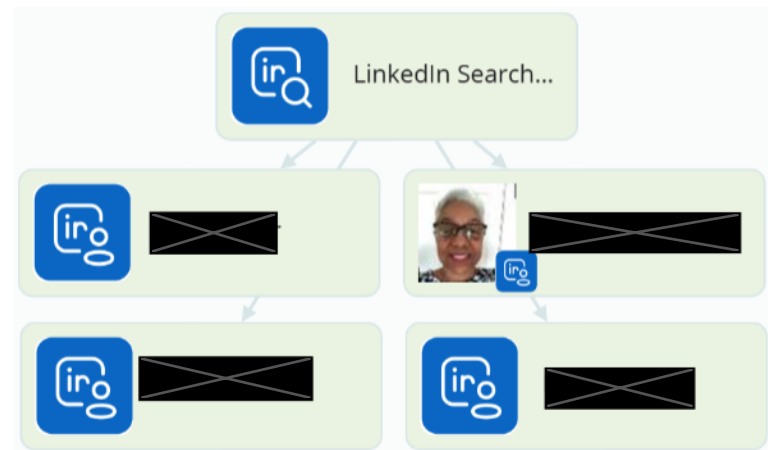
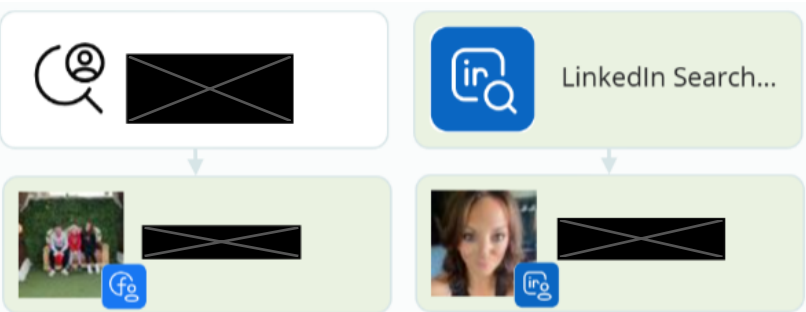
An analysis of the name [REDACTED] as provided by the client, revealed over **500 profiles** across various social media platforms.

The large volume of results makes it difficult to determine which, if any, are connected to the scam.

Searches combining the name with locations identified via phone number yielded:

1. One Facebook and LinkedIn profile in Milwaukee, Wisconsin
2. Four LinkedIn profiles in Chicago, Illinois

However, no direct connection could be established between any of these profiles and the scam. Therefore, there is a strong likelihood that the name is either **fake, fabricated, or potentially legitimate but misused** by scammers.



Source: [facebook.com/\[REDACTED\]](https://facebook.com/[REDACTED]), [linkedin.com/\[REDACTED\]](https://linkedin.com/[REDACTED])
[linkedin.com/in/\[REDACTED\]](https://linkedin.com/in/[REDACTED])



[REDACTED]

An analysis of the last phone numbers [REDACTED] revealed connections:

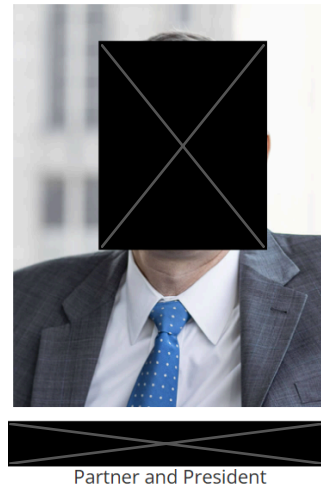
- Trucaller profile:

- Telecommunication company: [REDACTED]
- Location: Miami, Florida

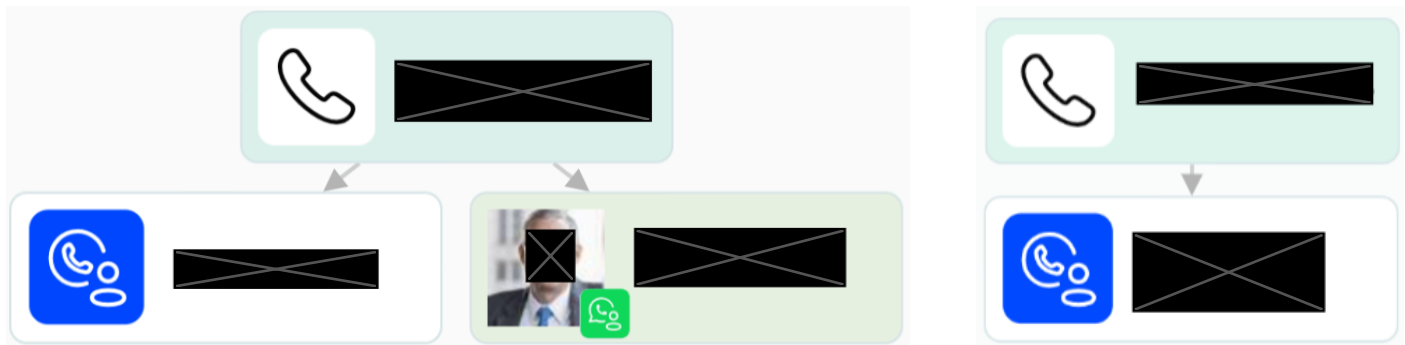
A reverse image search associated with this number led to the identification of [REDACTED] who is publicly listed as the [REDACTED] as seen on the firm's official website and LinkedIn profile.

- Trucaller profile: [REDACTED]

- Telecommunication company: T-mobile USA, Inc.
- Location: Denver, Colorado



No additional connections to data breaches, online accounts, or public profiles were found for either number. This limited digital footprint suggests these numbers have seen **minimal reuse or exposure in known scam networks**, and may not have been previously associated with fraudulent activities.



Source: [linkedin.com/in/\[REDACTED\]/\[REDACTED\].com](https://www.linkedin.com/in/[REDACTED]/[REDACTED].com)



- Trucaller profile: [REDACTED]
 - Telecommunication company: Aerial Communications, Inc.
 - Location: Westerville, Ohio

- Leaked Information: China_phone_number (2019-12-10)

- Name: [REDACTED]

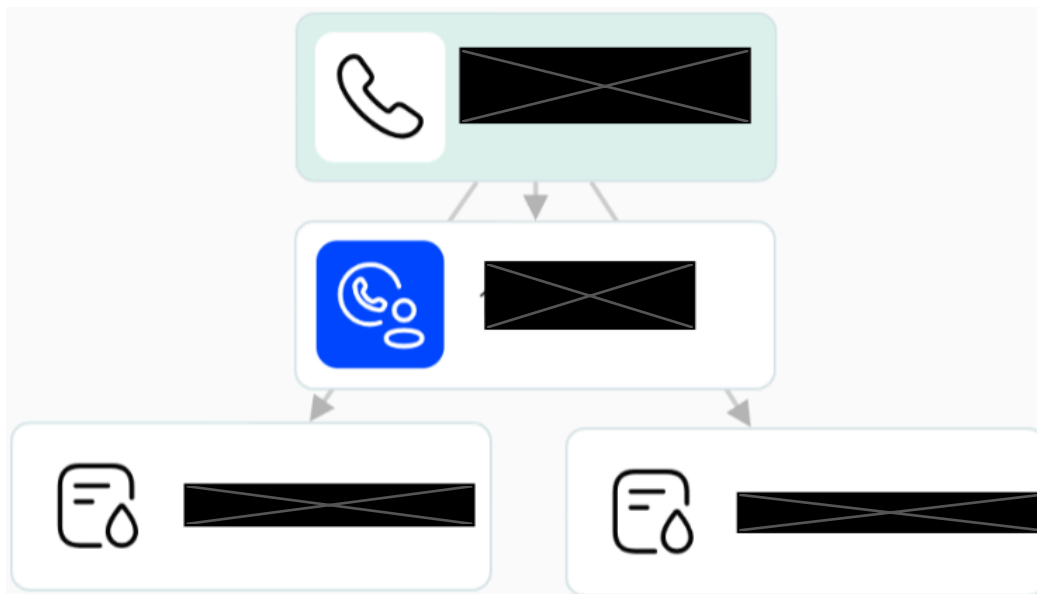
- Leaked Information: shunfeng.csv (2022-07-14)

- Name: [REDACTED]
- Listed Address: [REDACTED]
[REDACTED]

Despite the name match, there is strong reason to believe that the leaks refer not to the U.S. number [REDACTED] but to a Chinese number [REDACTED]

([REDACTED]', N'[REDACTED]', N'', N'', N'', N'[REDACTED],

The number [REDACTED] is registered with China Mobile and geolocated in Guangdong Province. It matches the data in the leaked records, address, and formatting — making it the more likely subject of the leak.



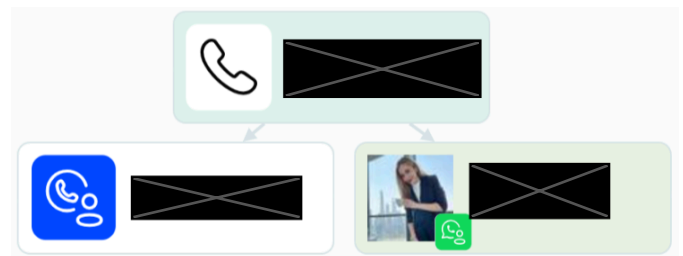
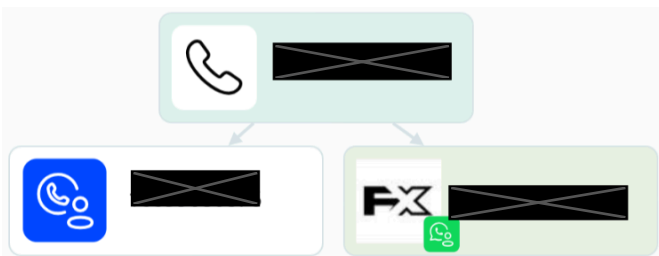


Analysing of the phone numbers provided by the client:

- Trucaller profile: +[REDACTED]
 - Telecommunication company: [REDACTED]
 - Location: New York City, NY
- Trucaller profile: [REDACTED]
 - Telecommunication company: [REDACTED]
 - Location: Atlantic City, New Jersey

Both numbers are active on WhatsApp. +[REDACTED] uses a widely circulated **stock** [REDACTED] **logo**, while [REDACTED] shares the same unique profile photo as [REDACTED]. Since the image is not found in open sources, this strongly suggests both numbers are controlled by the same individual or group.

We also identified a document titled *"Month of July 2021 PG Scholarship Payment Status"*, where Student IDs appear in a format similar to U.S. phone numbers. However, further investigation suggests these are likely just **unique student identifiers** and not linked to any real phone numbers.



1071	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	12400
1072	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	12400
1073	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	12400

Source: aicte-india.org/sites/default/files/



Domain Investigation

Domain analysis

Domain Name: [REDACTED].com

Name Servers:

- mike.ns.cloudflare.com
- paloma.ns.cloudflare.com

Domain Timeline:

- Creation Date: 2024-08-30
- Last Updated Date: 2024-08-30
- Expiration Date: 2025-08-30

Registrar Information:

- Registrar: GoDaddy.com, LLC
- Registrar URL: www.godaddy.com
- Registrar WHOIS Server: whois.godaddy.com
- Registrar IANA ID: 146
- Registrar Abuse Contact Email: abuse@godaddy.com
- Registrar Abuse Contact Phone: +1.4806242505

Registrant Information:

- Registrant information is not disclosed in the available WHOIS data.

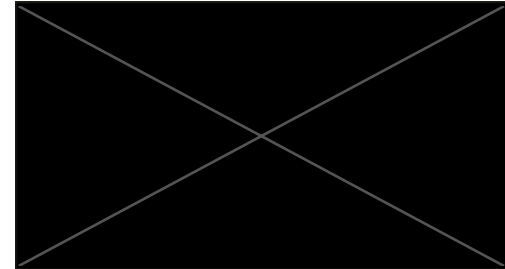


Further domain analysis:

Using browser inspection tools (██████████), we analyzed network activity on the website ██████████.com/#/ and identified connections to multiple related domains

1. Most of the website's images are loaded from these two domains. Both serve assets such as logos and UI elements, indicating shared backend infrastructure.

- a. ██████████.com
- b. ██████████.com



2. During an XHR request (getBasicInfo), the API exposed a service email address: support@██████████.com

Domains such as ██████████.com and ██████████.com display identical frontend structures, offering what appears to be the same trading platform—under slightly different domain names. These operate as variants of a scam-style deployment strategy: one subdomain for mobile (m.), and one for desktop (pc.).

Additionally, the domain ██████████.com appears in the API response, but the domain itself is currently inactive. Archived versions exist in the Wayback Machine, though they contain limited information. On that archived site, FXCC Markets Ltd claims registration with the **National Futures Association (NFA)** under ID: **0563357**. However, no such company is found on the official NFA registry under that ID, suggesting the claim is false or fabricated.

```
"service_link": "support@██████████.com",  
"created_at": "2023-03-16 09:27:49",  
"updated_at": "2024-12-17 17:56:21",
```

██████████ Committed to providing customers with a secure, compliant, and trustworthy trading environment, we are currently under the supervision of the National Futures Association of the United States (NFA, NFA ID: 0563357)

Source: [web.archive.org/██████████.com/](https://web.archive.org/web/20241217175621/https://██████████.com/), ██████████.com, ██████████.com



During the investigation, we identified numerous backend elements and messages written in **Chinese**, suggesting possible origin or operation by Chinese-speaking individuals.

- Several admin and agent URLs within the domain infrastructure lead to **Chinese-language login panels**, as shown in the screenshots.
- These panels appear to be part of an internal management system used by administrators or agents involved in the platform's operation.
- The API response also returns status messages in Chinese, further indicating the backend localization.

This pattern strongly implies that the domain and scam infrastructure may be operated or developed by individuals fluent in Chinese or located in a Chinese-speaking region.



Two blacked-out rectangular areas at the top of the page.

用户名

密码

谷歌验证码

邮箱验证码 发送验证码

登入



One large blacked-out rectangular area at the top of the page.

用户名

密码

☐ 记住密码 忘记密码?

登入

```
code": 1,  
msg": "请求成功",  
data": {  
  "type": 1,  
  "status": 1,  
  "loss_url": "https://m.[redacted].com/",  
  "company": null
```

Source: [admin.\[redacted\].com/admin](#), [agent.\[redacted\].com](#)



Conclusion

The domain analysis uncovered a network of interconnected domains including ██████████.com, ██████████.com, ██████████.com, and ██████████.com, all of which exhibit identical frontend structure and functionality. These domains serve variations of the same ██████ trading interface, distributed under different domain names and subdomains (e.g., m. for mobile, pc. for desktop). This pattern is a hallmark of scam deployment strategies that aim to reduce traceability and extend platform lifespan.

All the analyzed domains were registered recently, between mid to late 2024, with expiration set for one year, suggesting short-term use consistent with fraudulent schemes. The domains are registered under different names but share the same Cloudflare infrastructure and backend API patterns. Some of the content—including login panels and internal messages—was discovered to be written entirely in Chinese, strongly indicating that the operation is maintained or developed by Chinese-speaking individuals.

Additionally, the API response references an inactive domain (██████████.com) and falsely claims registration with the National Futures Association (NFA) under ID 0563357. No such record exists in the official NFA registry, confirming that this claim is fabricated.

The coordinated structure, language usage, registration patterns, and impersonation of regulatory credentials collectively point to an organized scam network.



Crypto Wallets Overview

Wallet Address:



Activity: Aug 14, 2024 – Mar 26, 2025

Transfers: 83

Balance: 0.004961 ETH

Sent: 177.743133 ETH

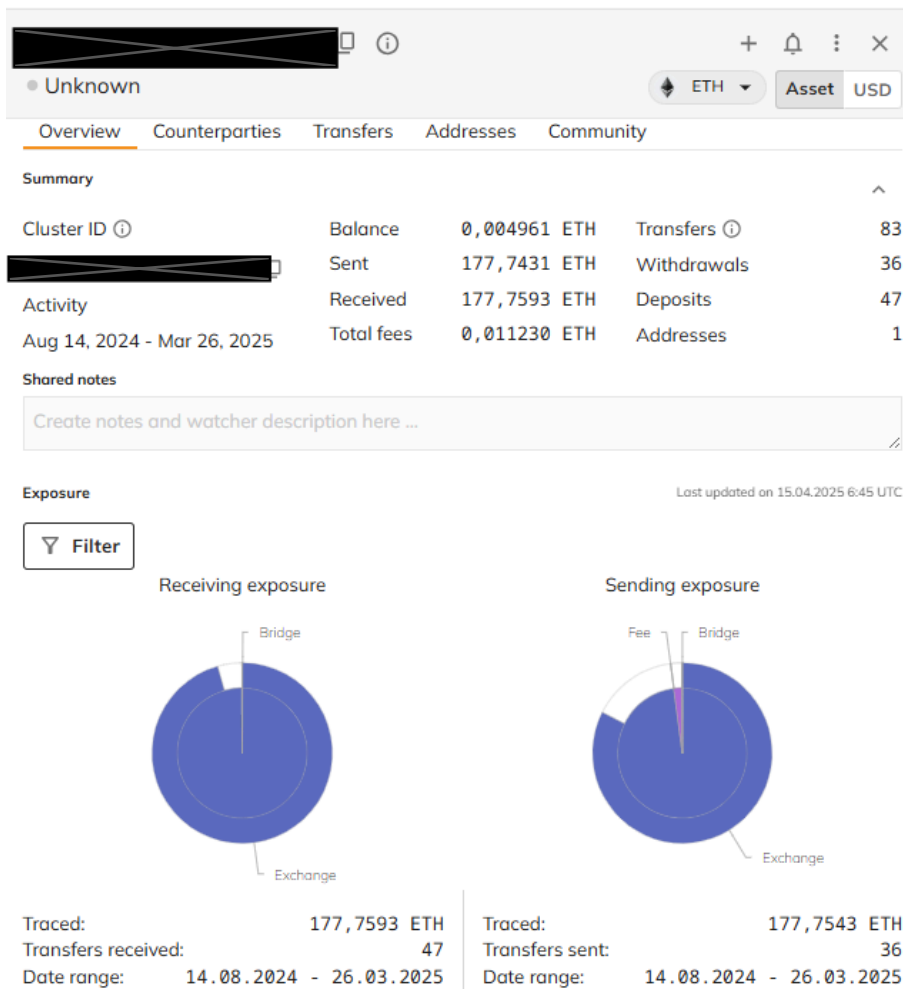
Received: 177.759325 ETH

Sending exposure:

97.87% Centralized Exchange

1.99% Smart contract

0.01% Fee



Data
Forensics

Conclusion

We successfully extracted the sending exposure of the wallet linked to the suspected scam activity. Our analysis revealed that **97.87%** of the funds were transferred to **centralized exchanges**, which significantly increases the chances of identifying the individuals behind the transactions.

We were able to trace the flow of assets to specific wallet addresses hosted by these exchanges, providing a clear opportunity for law enforcement to initiate further investigation. These platforms typically operate under **Know Your Customer (KYC)** regulations, allowing authorities to request verified user data tied to the accounts in question.

Such information could include the scammer's name, address, government-issued ID, and other identifying details. These insights are critical to unmasking the individual or group responsible and may support efforts to **freeze the remaining funds** and hold the perpetrators legally accountable.



Summary Of The Findings

Person Information Investigation:

1. Phone Number: [REDACTED]
 - Registered with T-Mobile USA, located in Milwaukee, Wisconsin.
 - Found in a leaked EatStreet dataset under the name [REDACTED] linked to the email [REDACTED]@gmail.com.
 - Also found in a Facebook data leak associated with the profile [REDACTED] (Facebook ID: [REDACTED]).
2. Email Address: [REDACTED]@gmail.com
 - Registered on Dubsmash using the same username and password.
 - Linked to a T-Mobile IP address ([REDACTED]92) in Chicago, IL.
3. WhatsApp Profile Photo
 - Contains identifiable architecture of Shanghai, China.
 - Image reused in multiple social media accounts ([REDACTED], [REDACTED], [REDACTED]) under various names such as [REDACTED] and [REDACTED] indicating use in fake identity schemes.
4. Name: [REDACTED]
 - Over 500 results across social networks.
 - No verified links to the scam despite searches in Milwaukee and Chicago.
5. Phone Number: +[REDACTED]
 - Belongs to [REDACTED] (Florida).
 - The WhatsApp photo showing the identity of [REDACTED]
6. Phone Number: [REDACTED] Registered with T-Mobile USA, Denver, Colorado.
7. Phone Number: +[REDACTED]
 - Traced to Aerial Communications, Inc. in Westerville, Ohio.
 - Name similarity in a Chinese leak ([REDACTED]) was determined to be unrelated, and instead matched a Chinese number +[REDACTED]
8. Domain: [REDACTED].com
 - Newly registered in August 2024, expires in one year.
 - Connected via API calls to related domains: [REDACTED].com, [REDACTED].com, and [REDACTED].com.



- Backend contains Chinese-language elements and admin panels, indicating possible Chinese operators.

Domain Investigation

9. Possibly a fraudulent domain. .com

10. Registrant and Technical Contact Info:

- Registrant information is not disclosed in the available WHOIS data

Crypto Wallets Investigation

11. Wallet overview – Sent and Received:

- Balance: 0.004961 ETH
- Sent: 177.743133 ETH
- Received: 177.759325 ETH

12. Sending Exposure:

- 97.87% Centralized Exchange
- 1.99% Smart contract
- 0.01% Fee



Confidential note

All information contained in this report is confidential and may not be disclosed without prior written authorization, except when shared by law enforcement as part of an investigation.

