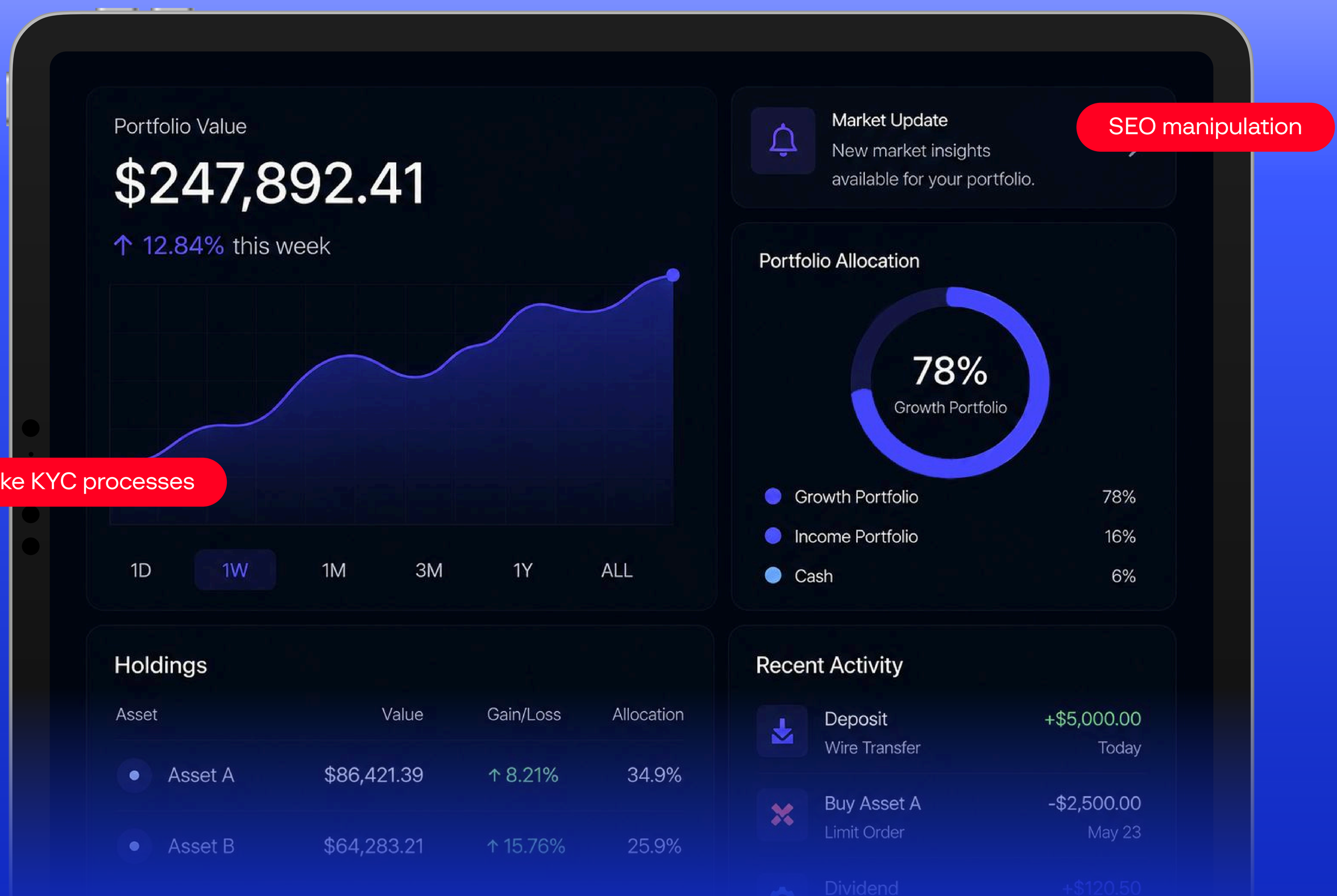
GROUP-IB



Fraud Research

Part 2 of investment scams targeting the United States and Australia

Inside the Fake Investment Platform Economy

How Fraudsters Built a $187M Crypto Scam Network targeting Australia and the United States

GROUP-IB.COM

Table of contents

01 Disclaimer 03

02 Acknowledgements 04

Authors 00
Contributors 00

03 Introduction 05

Further Reading 07

04 Key findings 07

05 Attribution 08

Threat Actors 08
Scam Profiles 09
Victimology 10

06 Fake or unlicensed investment platform scheme 11

Stage 0: Reconnaissance & Resource Development 13
Stage 1: Initial Lure & Social Engineering 18
Stage 2: Onboarding & Initial Investment on Fake Platform 19
Stage 3: Withdrawal Obstruction & Escalation Tactics 23
Stage 4: Cash-Out & Money Laundering 24
Stage 5: Recovery Scam (Secondary Victimisation) 27

07 Towards a predictive defence: Group-IB's Cyber Fraud Fusion Approach 28

Scenario 2: Cyber Fraud Fusion Applied to Fake Investment Platforms 29
Why Cyber Fraud Fusion Matters 30

08 Conclusion 31

09 Recommendations 32

For Individuals 32
For Trading Platforms 32
For Financial Institutions 33
For the Ecosystem 33

10 Indicators of Compromise (IOCs) 35

01 Disclaimer

01	This report is provided for informational purposes only. The findings, assessments, and recommendations are based on data available at the time of publication and are subject to change as new intelligence emerges.
02	While every effort has been made to ensure the accuracy of the information, Group-IB makes no warranties, express or implied, regarding completeness, reliability, or suitability for any particular purpose.
03	Readers are permitted to download, review, and cite this report for personal or educational use, provided that proper attribution is given to Group-IB and a link to the original source is included. Any commercial use or redistribution of the report without prior written consent from Group-IB is strictly prohibited.
04	This report may reference legitimate third-party services such as WhatsApp, Facebook, and others, solely to illustrate cases where threat actors have abused or misused these platforms.
05	This report is protected under applicable copyright and intellectual property laws. All trademarks referenced herein are the property of their respective owners and are used solely for informational purposes, without any implication of affiliation or sponsorship.
06	Unauthorized reproduction, distribution, or other use of the report, in whole or in part, without written consent from Group-IB, may result in legal action, including claims for damages.
07	All forensic activities described were conducted under client authorization and in compliance with applicable laws. This report is provided for informational and defensive purposes only, and its recommendations must be applied in accordance with legal requirements.
08	This report may reference legitimate and/or legal third-party services solely to illustrate how threat actors misuse or abuse such platforms or services. All trademarks are property of their respective owners.

02 Acknowledgements

We would like to express our sincere gratitude to all teams whose expertise and dedication made this report possible. This investigation was a collaborative effort led by Group-IB's Fraud Protection team, involving analysts from Investigations, Threat Intelligence, and its Computer Emergency Response Team (CERT-GIB). Their combined work in analyzing, correlating, and contextualizing data played a critical role in uncovering the tactics, techniques, and procedures of the threat actor. This report is a testament to the power of cross-functional collaboration in the face of complex adversarial threats.

Authors



Yuan Huang
Senior Fraud Analyst



Afiq Sasman
Head of CERT-GIB, Asia-Pacific



Aleksandr Sychev
Senior Cyber Investigation Specialist

Contributors



Zafar Astanov
Deputy Head of Fraud & Financial Crime Solutions



Vladimir Kalugin
Operational Director of Group-IB's Unified Products



Dmitry Pisarev
Product Manager, Fraud Intelligence



Nikita Rostovtsev
Technical Head, Attack Surface Management, Threat Intelligence and Digital Risk Protection, Asia-Pacific



Jia Hwei Soh
Head of High Tech Crime Investigations, Asia-Pacific

03 Introduction

(ACCC) reported that Australian consumers suffered a total of US$2.18 billion in scam-related losses across all categories, with investment scams accounting for US$837.7 million — the single highest-loss scam type, representing over a third of all reported losses. In the United States, the U.S. Federal Trade Commission (FTC) reported that consumers in the United States reported US$7.9 billion in losses to investment scams in 2025, with a median individual loss of US$10,000. While these figures reflect the aggregate impact across all investment scam typologies, a significant and growing proportion of losses are attributable to fraudulent cryptocurrency investment platforms operating entirely outside regulatory frameworks.

These platforms represent a distinct evolution in investment fraud. Unlike schemes that exploit legitimate trading infrastructure, fake investment platforms construct an entirely parallel financial ecosystem, complete with professional-looking websites, fabricated portfolio returns, fake KYC processes, and tiered investment plans offering mathematically unsustainable daily returns.

All transactions are conducted exclusively in cryptocurrency, making fund recovery exceptionally difficult. What makes them particularly dangerous is not just their individual deceptiveness, but in its scale. Threat actors operate networks of dozens or hundreds of interconnected platforms, ensuring that the operation continues even when individual domains are identified and taken down.
This report—the second in a two-part series on investment scams targeting Australia and the United States—provides a comprehensive examination of this fake platform scheme.

Through Group-IB's investigations, our analysts identified a single confirmed fraudulent platform (tetherglobalItd[.]com) that shares identical contact information with 23 other fake investment platforms, and shares the same hosting IP address with 208 additional domains. On-chain cryptocurrency analysis of the confirmed platform revealed over US$90,000 in identifiable deposits across BTC, ETH, and USDT-TRC20 addresses active since 2022. Extrapolating across the connected network yields an estimated total revenue of approximately $187 million gained by the fraudsters from only one identified cluster.

The report further examines how Group-IB's Cyber Fraud Fusion (CFF) approach, one that unifies Digital Risk Protection, Threat Intelligence, Fraud Protection, Cyber Fraud Intelligence Platform and Investigation capabilities, can expose and disrupt these platform networks at scale, intercept victim deposits before they are laundered, and trace stolen funds to the identifiable individuals behind the operations.

Further Reading

This report is a two-part series focusing on investment scams targeting victims in the United States and Australia.

Please visit Group-IB's Research Hub for part 1 of this series, focusing on a social media-driven pump-and-dump scheme that uses deepfake impersonation to manipulate real stock prices on legitimate exchanges.

04 Key findings

01	All fake investment platforms identified by Group-IB exclusively accept cryptocurrency for deposits, bypassing traditional banking controls and complicating fund recovery.
02	Group-IB's Graph analysis of one confirmed fake investment platform (tetherglobalItd[.]com) reveals it shares contact information with 23 other fake platforms and shares the same IP address with 208 additional fraudulent domains.
03	Multiple fake investment platforms share remarkably similar design templates and contact information, confirming shared development resources and a common operator behind the network.
04	The estimated total revenue across the 208 connected platforms exceeds US$187 million across Australia and the United States, and this represents only one identified cluster.
05	On-chain analysis reveals that threat actors transfer stolen funds directly to KYC-compliant centralised exchanges without obfuscation, creating potential investigative leverage for law enforcement.
06	USDT-TRC20 address cluster analysis identified two addresses sharing three common downstream recipients, supporting single-actor attribution across the platform network.
07	Victims are subjected to secondary victimisation through "recovery scams" — fraudulent firms, often operated by the same threat actors, that offer to retrieve lost funds for an upfront fee.

05 Attribution

Threat Actors

Group-IB customers can access our Threat Intelligence portal for more information about the following threat actors below.



CoinLure

First seen
November 2022

About

CoinLure is a financially motivated threat actor that develops and operates fake investment platforms at an industrialized scale.

Skillset

- Web and user interface development
- Search Engine Optimization (SEO) manipulation
- Social engineering
- Cryptocurrency operations
- Operation resilience (208-platform network)

Toolset

- Shared platform templates
- Multi cryptocurrency address BTC/ETH/USDT wallets
- Cryptocurrency exchange accounts
- Fake KYC systems
- Referral programme infrastructure

Targeted Industries

- Financial services
- Retail investment and trading services
- Cryptocurrency

Motivation

- Financial gain

Modus Operandi

CoinLure’s modus operandi combines SEO manipulation, social media outreach, and romance-based social engineering to identify and engage victims, who are then migrated to WhatsApp for direct communication. Operators introduce victims to fraudulent crypto investment platforms that feature simulated “trial” funds and tiered investment plans designed to build confidence. Once trust is established, victims are encouraged to make cryptocurrency deposits, after which withdrawals are systematically obstructed through fabricated fees or compliance checks. In later stages, victims may be re-targeted with “recovery” scams. Funds are ultimately cashed out directly via KYC-compliant exchanges, with little to no use of obfuscation techniques.

Scam Profile

Group-IB customers can access our Fraud Intelligence portal for more information about the following threat actors below.

Fake/Unlicensed Investment Platform

Threat Actors
CoinLure

First Discovered
November 2022

About

Victims are directed to fraudulent investment platforms displaying fabricated returns to encourage deposits. Platforms operate exclusively via cryptocurrency. Withdrawal attempts are systematically obstructed through escalating fee demands. On-chain analysis reveals direct fund transfers to KYC-compliant exchanges.

Techniques

SEO manipulation | Impersonation of legitimate investment platforms /services UI/UX | Fake KYC processes | Trial fund psychological traps | Tiered investment plans with unsustainable returns | Cryptocurrency-only transactions | Crypto address rotation | Multi-level referral programmes | Trust escalation model | Withdrawal obstruction | Recovery scam (secondary victimisation)

Targeted Jurisdictions

Australia | United States

Victim Path

01 Organic search / Social media advertisement / Romance scam

02 WhatsApp contact

03 Fake investment platform registration

04 Cryptocurrency deposit

05 Withdrawal obstruction

06 Potential recovery scam

Victimology

The following data is sourced from the ACCC Targeting Scams Report (2025), the U.S. Federal Trade Commission (FTC) Consumer Sentinel Network (2025), and Scamwatch. Investment scams represent the highest-loss fraud category in both jurisdictions.

By Jurisdiction

Jurisdiction	Industries / Entities Targeted	Reported Losses (2025)
Australia	Individuals (retail investors) · Banking clients · Trading platform users	US$837.7 million (investment scams) US$2.18 billion (all scam types)
United States	Individuals (retail investors) · Banking clients · Trading platform users	US$7.9 billion (investment scams) US$15.9 billion (all fraud types)

By Sector

Sector	Industries / Entities Targeted	Reported Losses (2025)
Trading Platforms	Centralised exchanges used as both deposit sources (by victims) and cash-out destinations (by threat actors)	Regulatory and compliance exposure

In Australia, 481,523 scam reports were filed across all agencies in 2025, with 274,577 involving financial losses. Australians aged 65 and over accounted for 26.5% of total losses reported to Scamwatch. Online-based scams with a financial loss increased by 31.8% in 2025. In the United States, 3 million fraud reports were filed in 2025, with investment scams alone accounting for approximately half of all reported fraud losses.

06 Fake or unlicensed investment platform scheme

Overview

This scheme involves directing victims to fraudulent investment platforms that are either entirely fabricated or impersonate legitimate, licensed Australian or US financial services providers. The platforms display fabricated returns to encourage progressively larger deposits, then obstruct all withdrawal attempts through escalating fee demands and manufactured obstacles.

Jurisdictional Relevance

These platforms frequently impersonate Australian Securities and Investment Commission (ASIC)-regulated entities in Australia, or Securities and Exchange Commission (SEC)/Financial Industry Regulatory Authority (FINRA)-registered firms in the US. They may display fake Australian financial services license (AFSL) numbers or fictitious registration details. The operations are typically run from offshore jurisdictions, making law enforcement and fund recovery extremely challenging.

Investment Scams
Scheme 2

Fake Investment Platform Attack Chain & Operational Flow

Step 0

Reconnaissance & Resource Development

- Develop sophisticated fake investment platform websites
- Build SEO-optimised content and landing pages to capture organic search traffic for investment-related queries.
- Create and maintain multiple social media accounts and pages with professional branding for ad distribution.
- Prepare cryptocurrency wallets, mule bank accounts, and potentially shell companies for fund collection and laundering.

Step 1

Initial Lure & Social Engineering

- Social media advertisements
- Romance / relationship scams (pig butchering)
- Organic search / SEO
- Email phishing & forum posts
- Referral schemes
- Messaging app outreach

Step 2

Onboarding & Initial Investment on Fake Platform

- Victims register on the fraudulent platform and make initial deposits. The platform is designed to appear fully functional and may allow small early withdrawals to establish trust.

Step 3

Withdrawal Obstruction & Escalation Tactics

- When victims attempt to withdraw larger sums, the platform deploys a systematic series of obstruction tactics designed to extract additional funds while preventing any actual payout.

Step 4

Cash-Out & Money Laundering

- Threat actors move stolen funds through layered channels to obscure the origin and make recovery extremely difficult.

Step 5

Recovery Scam (Secondary Victimisation)

- After the fake platform was taken down, victims may be subsequently contacted by a “recovery firm” — often operated by the same or affiliated threat actors — offering to recover lost funds for an upfront fee.

Stage 0 Reconnaissance & Resource Development

Setting Up a Convincing Fake Investment Platform

Threat actors that perpetuate fake or unlicensed investment platforms would register domains that closely resemble the look and user interface of legitimate Australian or US financial services providers, and invest significant effort in building convincing fake investment platform websites.

These platforms typically feature a professional homepage layout to create an immediate impression of legitimacy; an investment plan overview presenting structured "products" that mimic legitimate offerings; user statistics (e.g., "50,000+ registered users") to suggest popularity and trustworthiness; investor satisfaction ratings to provide social proof; and live transaction feeds to create an impression of an active, successful platform.

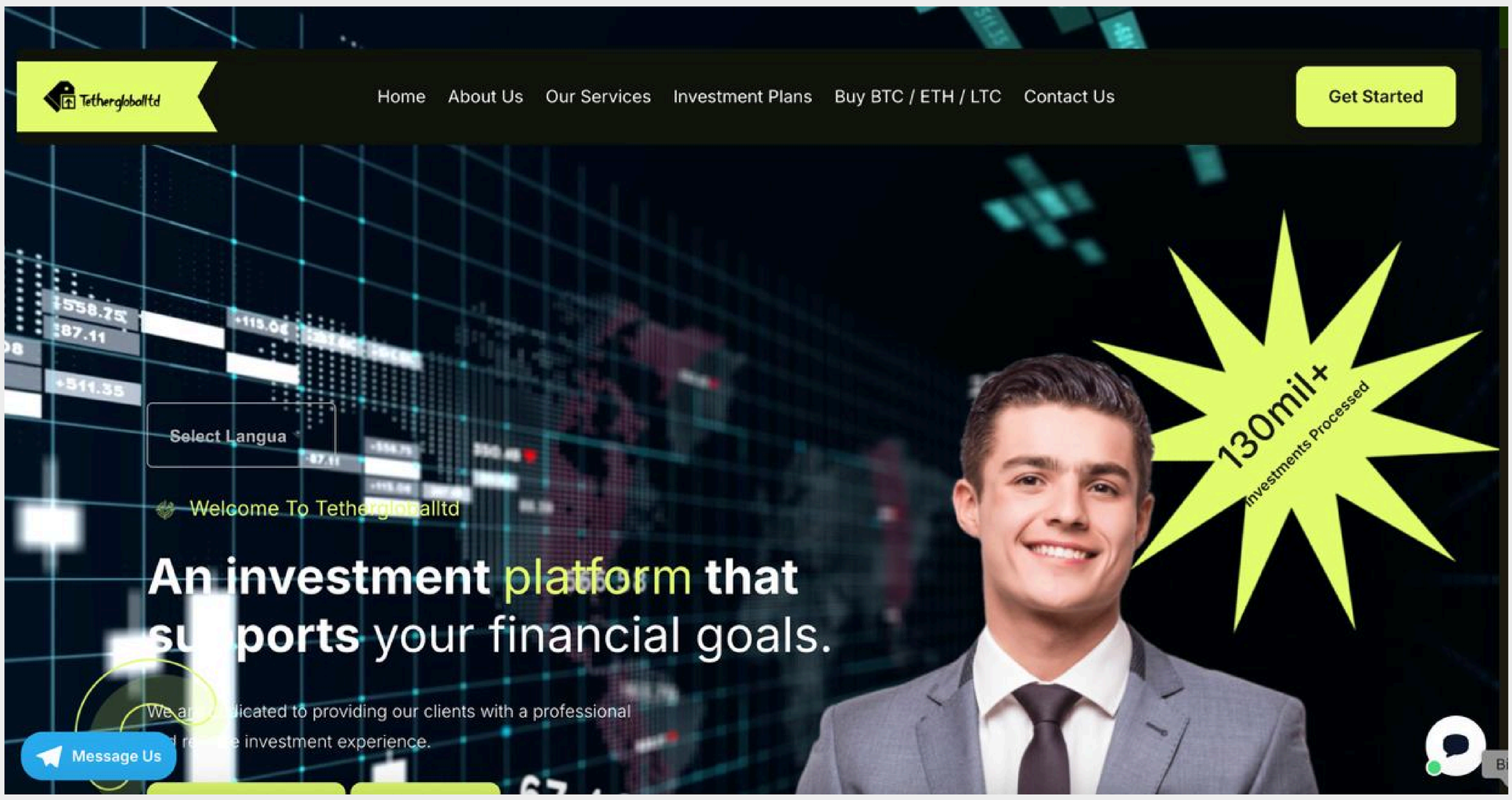


Figure 2. A screenshot of a fake investment platform (https://tethergloballtd[.]com/).

However, these elements are typically fabricated and cannot be independently verified. Notably, multiple fake investment platforms observed by Group-IB shared remarkably similar design characteristics, suggesting the use of common templates, or the involvement of shared development resources. This assessment is further supported by the shared contact information identified across multiple fake investment platforms.

Establishing Multiple Fake Investment Platforms for Resilience and Revenue Maximisation

Analysis of one confirmed fake investment platform (tetherglobalItd[.]com) using Group-IB's patented Graph solution reveals that the website (as shown in Figure 8) shares identical contact information, including name, email, phone number, and physical address, with 23 other fake investment platforms.

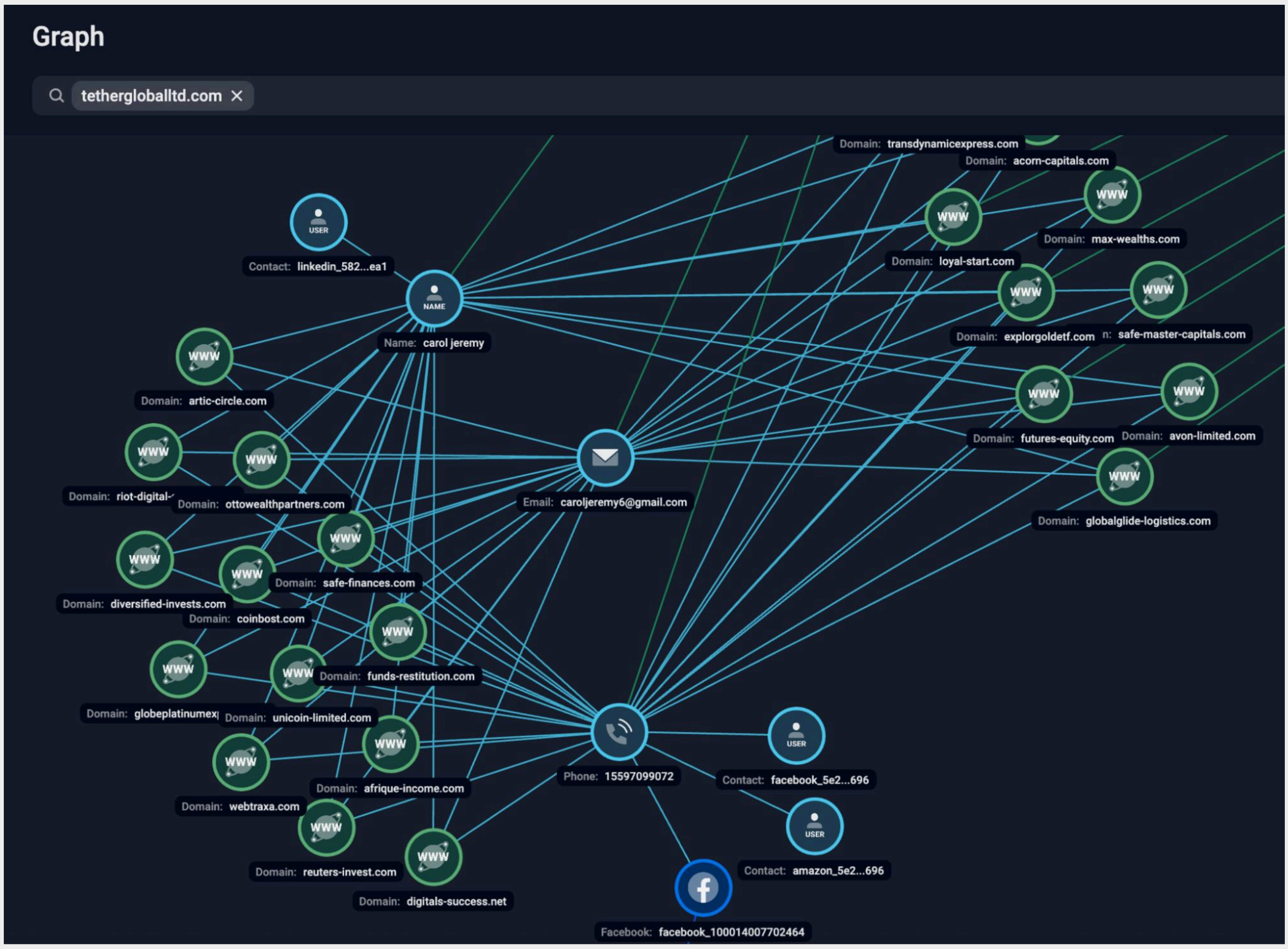


Figure 3. Group-IB's Graph analysis of the contact information of the fake investment platform (https://tetherglobalItd[.]com/).

Furthermore, the same platform shares its hosting IP address with 208 additional fraudulent investment domains. These connections strongly indicate that the same threat actor or organised cybercriminal group operates the entire network of platforms, which also explains the remarkably similar design characteristics observed across them.

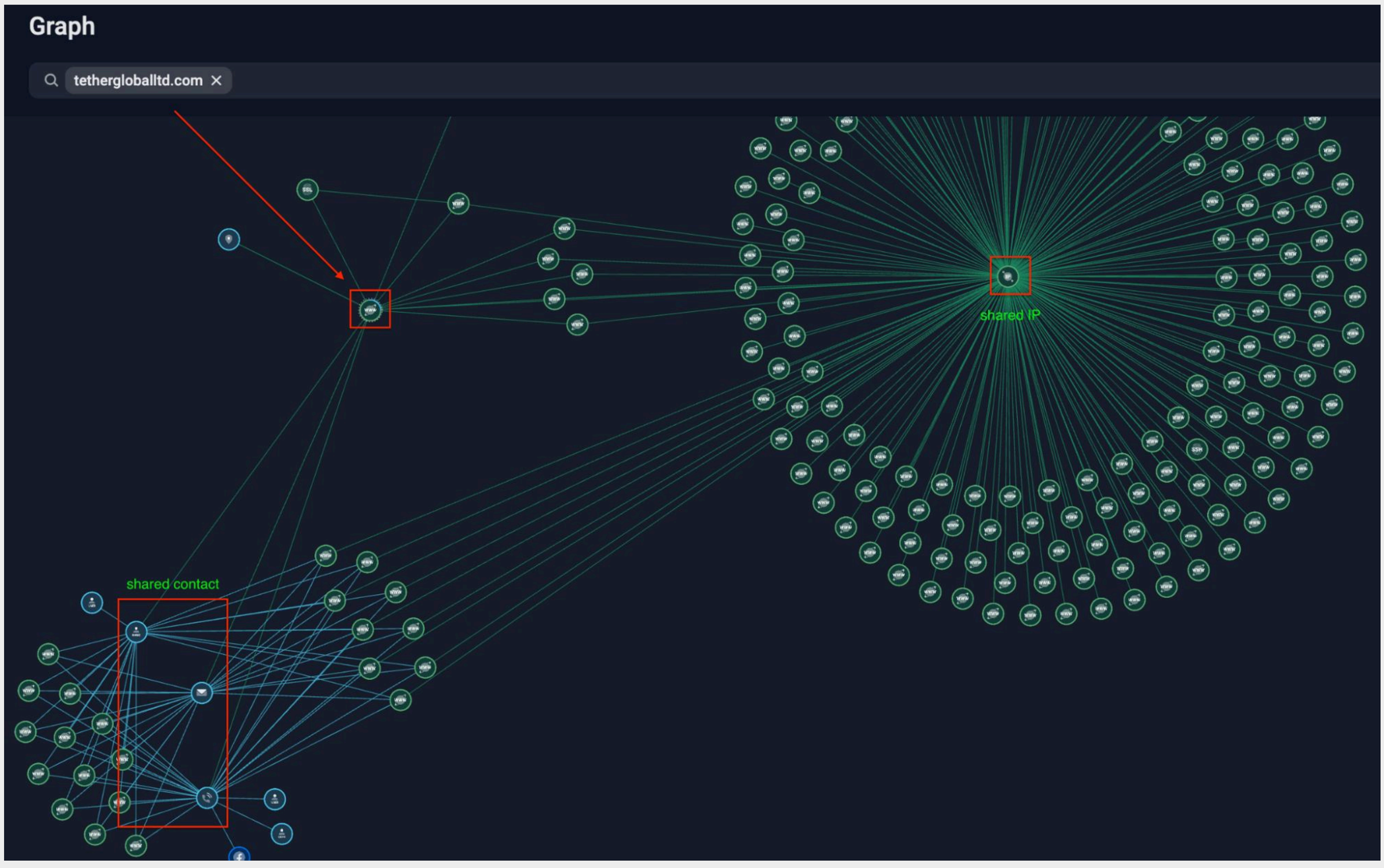


Figure 4. 208 more fake investment platforms share the same IP address with https://tetherglobalItd[.]com/

The strategic rationale behind operating such an extensive network is twofold: first, it ensures operational resilience so that even if one or several platforms are identified and taken down, the remaining platforms continue to operate and generate revenue; and second, it maximises victim reach by presenting multiple seemingly independent platforms across different domains and brand identities, thereby expanding the total addressable victim pool.

Building SEO-Optimised Content and Creating Social Media and Messenger Accounts

Based on multiple victim testimonies provided by Group-IB's clients in Australia, Group-IB's Fraud Intelligence analysts have identified the following victim's journey in such scams:

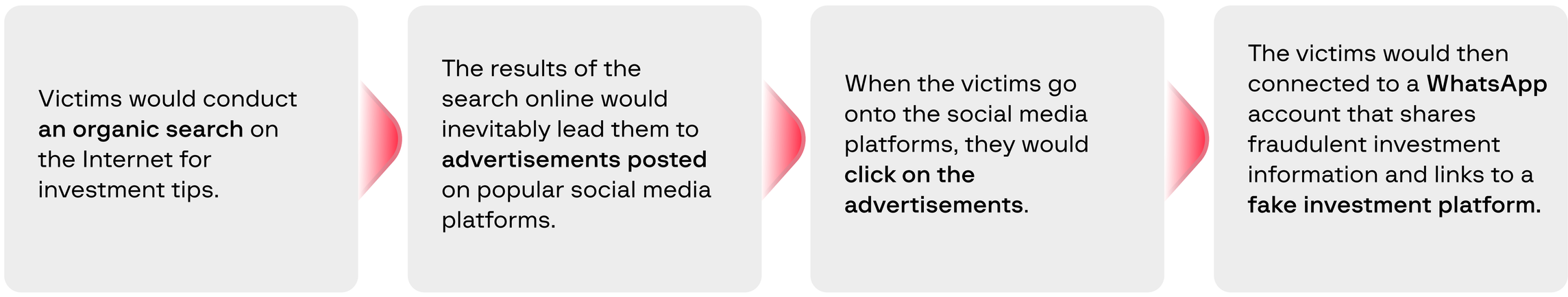


Figure 5. A flowchart depicting a victim's journey in a fake or unlicensed investment platform scheme.

This indicates that threat actors are knowledgeable in building SEO-optimised content and landing pages, as well as their potential victims' profiles and psychology, to capture organic search traffic for investment-related queries. They also create and maintain multiple social media accounts with fake or impersonated professional branding for advertisement distribution. This step adds credibility and serves the additional function of redirecting users from public platforms to more private messenger platforms such as WhatsApp or Telegram, where the fake investment websites are promoted.

Money Laundering through Cryptocurrency Wallets and Mule Accounts

A defining characteristic of all identified fake investment platforms is the exclusive use of cryptocurrency for deposits and withdrawals. Users are typically prompted to link cryptocurrency wallets directly to the platform, transfer funds to a wallet address controlled by the threat actor, and purchase cryptocurrency specifically for deposit. The following is a list of crypto wallet addresses identified by Group-IB that were used in this scheme:

TA's crypto wallet address:
bc1qeu024wyhev6c3mv66ea8u0
0xCF8Fc675A89Bb22e1e4588cE7
TMUJXvCHYkrTLCtyb8URQRZtnnv
0xa366508EA08880e8d8Ca0e629
bc1qks40mcz7x02a3p5x2qasme9
TPt2JUCnYf3JcCStJioDo9SYgbrd6X
DTxHoe3kZtaEhEg61vY4aqr4mT7
0xf32198bC176aEfc9a6819Bd593
1PKAdFXfwFNC2jwQnh8DZ9Q2CZ
LMXMJz7K7uLNqPBHPs5WUCozK
TDb3coJu5ExZmoWgyyzYAGCmW
1JZZX98JjhwnBXJzTT89LdBDt6PN
TSBwDUvMnmHcuHgNEHtiztWzo
0x05c83071C2A73Cfc2260B126d
bc1pcsyzr8qrs87250a6gh0x023yl
TYonySKqCuUaqeUUNio5J7DMTz
0x6Af1DFb684Dba55c6761a610B
TRSdvdhf6iVR9g5pb5cD8S4Up5H
DQATAzHMp3gziCF3JvPsvxE9oQy

Figure 6. A list of cryptocurrency wallet addresses used in the money laundering scheme.

It is worth noting that legitimate Australian investment platforms typically accept bank transfers, BPAY, and debit/credit card payments. Platforms that exclusively accept cryptocurrency deposits should be treated with caution, as they are generally attempting to evade regulatory oversight, prevent transaction reversal or dispute, obscure the destination of funds, and/or complicate law enforcement tracing.

Stage 1 Initial Lure & Social Engineering

Multiple Acquisition Channels	Victims are directed to the fake investment platform through multiple acquisition channels, often combining tactics such as emotional manipulation, with professional-looking marketing. Apart from the primary victim journey described above (Figure 11), several other common channels have been observed directing victims to fake investment platforms:
Romance and relationship scams (pig butchering):	Fraudsters cultivate romantic or personal relationships via dating apps such as Tinder, Bumble or Hinge, or social media direct messages over weeks or months before introducing the investment "opportunity”.
Referral schemes	Existing victims are incentivised with small "bonuses" or "referral commissions" to recruit friends and family, adding a layer of social proof. Many fake investment platforms incorporate multi-level referral programmes where users receive commission based on investments made by their referrals. Multiple referral tiers may exist (e.g., 5% for direct referrals, 2% for second-tier). This structure incentivises victims to recruit additional victims and shares characteristics with pyramid schemes, enabling the victim pool to expand organically.
Messaging app outreach	Unsolicited messages via WhatsApp, Telegram, or SMS from unknown numbers promoting exclusive investment opportunities represent another channel.
Email phishing and forum posts	Spam emails or posts in investment forums including Reddit, Facebook groups or Whirlpool, promoting the platform with fabricated success stories.

Trust Escalation Model

A particularly insidious variant of victim acquisition involves a graduated trust escalation process that operates across both legitimate and fraudulent platforms.

In the initial phase, victims are encouraged to place small trades on legitimate, regulated platforms where they see real, verifiable gains. An assigned "account manager" maintains regular contact, building a relationship that creates emotional dependency and trust. Gradually, the stakes are raised: larger investment "opportunities" are introduced, and eventually, the victim is migrated to a fraudulent platform where they deposit significant funds.

Stage 2 Onboarding & Initial Investment on Fake Platform

Victims Register Accounts on Fake Investment Platforms

Once victims are redirected to a fake investment platform, they are asked to create an account and complete a fake KYC (Know Your Customer) process before commencing investment. Registration typically requires a username, email address, password, phone number (in some cases), and a referral or invitation code (optional but incentivised). This step lends credibility to the fake platform while simultaneously harvesting personal data that may be used for direct fraud execution, sale to other criminal actors, identity theft, or targeted phishing campaigns.

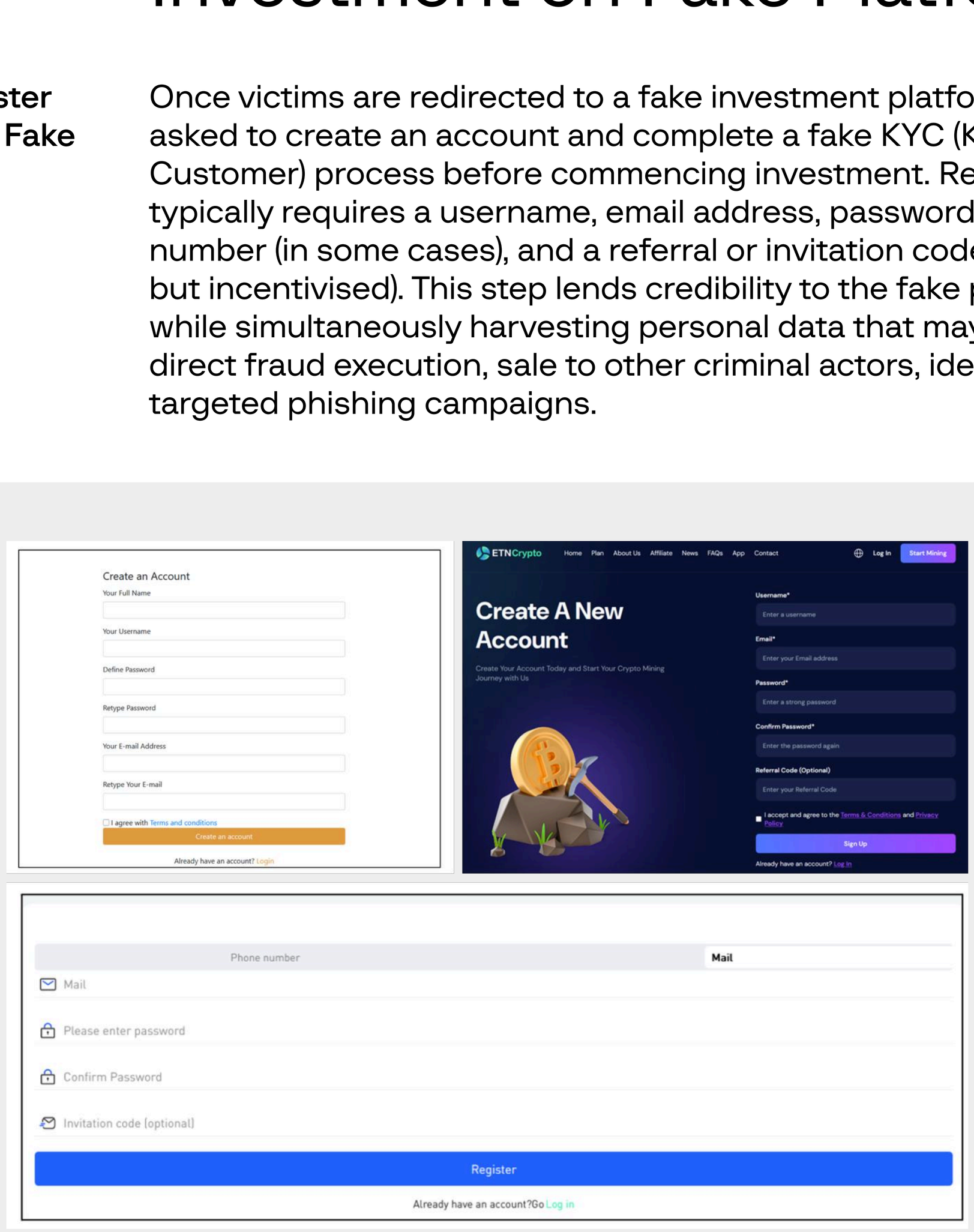


Figure 7. Screenshots of the sign-up form on fake or unlicensed investment platforms.

Some fake or unlicensed investment platforms operated by the fraudsters implement email verification procedures, which create an additional false sense of security. Confirmation emails upon successful registration further mimic legitimate onboarding experiences.

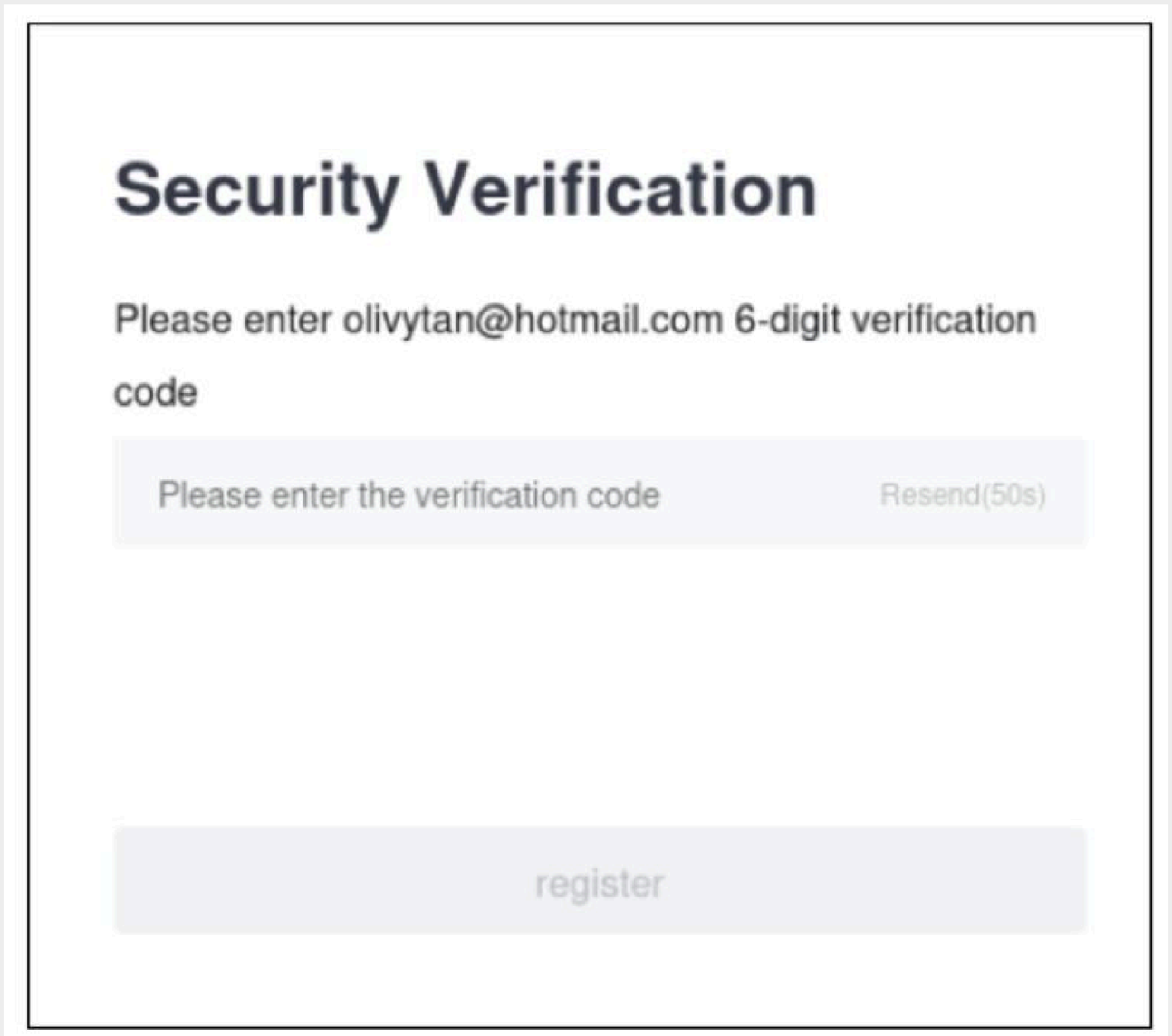


Figure 8. Screenshot of a “Security Verification” procedure from a fake or unlicensed investment platform.

Attracting Victims to Make Initial Deposits

These platforms offer tiered "investment plans" or "contracts" with increasing returns to lure victims into making initial deposits. The promised returns are mathematically unsustainable and characteristic of Ponzi scheme structures. Legitimate investment products cannot guarantee a return on investment or fixed daily returns of this magnitude.

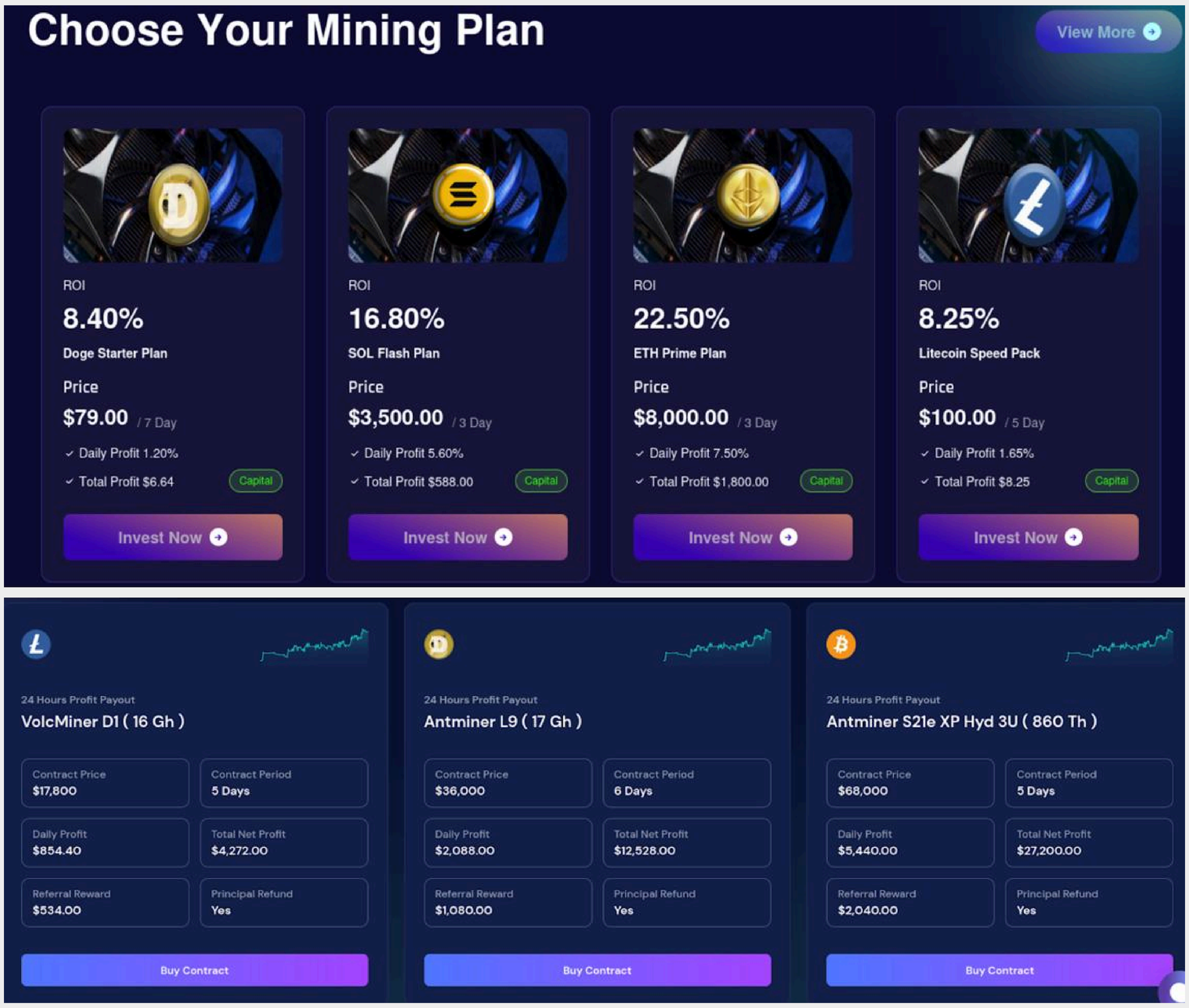


Figure 9. Screenshots of tiered “investment plans”from tradespotau[.]com (top) and etncrypto[.]com (bottom) that offer guaranteed “Daily Profits” and “Total Profits” in increasing amounts.

To further attract deposits, certain fake or unlicensed investment platforms (such as those observed at domains like etncrypto[.]com) provide "trial funds" or "welcome bonuses" upon registration, commonly in the range of US$50–US$100. However, these mechanisms are designed as psychological traps: the trial funds can typically only be applied to the lowest-tier investment plan, and returns from trial investments remain below the minimum withdrawal threshold. Users must deposit real funds to access their purported "earnings." This creates an incentive structure that appears compelling but is, in reality, entirely fraudulent.

Victim Deposits

As noted earlier, all identified fake investment platforms accept only cryptocurrency for deposits and withdrawals. Victims typically send funds directly from accounts held on mainstream centralised platforms, including:

- **Exchanges** such as Binance, Bybit, OKX, Coinbase, Crypto.com, Paxful, ChangeNow
- **Payment apps** such as Cash App, Luno

The average individual deposit identified during our investigation is approximately US$200, consistent with retail-level victims of investment fraud.



Figure 10. A scheme illustrating how the victims' monies are transferred to fraudsters from different platforms.

Stage 3 Withdrawal Obstruction & Escalation Tactics

When victims attempt to withdraw funds, the platform may deploy various obstruction tactics to extract additional payments from their victims, while preventing any actual payout. These techniques include but are not limited to:

Minimum balance requirements	Victims are informed that a minimum balance or trading volume must be reached before withdrawals are permitted, requiring further deposits.
Tax and fee demands	Victims are told they must pay "tax," "withdrawal fees," "insurance deposits," or "regulatory compliance charges", often 10–30% of the account balance, before funds can be released.
Upgrade requirements	Victims must "upgrade" their account tier at additional cost to unlock withdrawal functionality.
Technical issues	The platform claims system errors, maintenance periods, or processing delays to stall withdrawal requests indefinitely.
Account freezing	The platform "freezes" the account, citing alleged suspicious activity, anti-money laundering compliance, or identity verification issues, and demands additional documentation or payments.

Each time a victim meets one condition, a new requirement is introduced, creating an endless cycle of additional payments. While these platforms typically feature live chat functionality, the support mechanisms are designed to delay and deflect. Support agents are portrayed as being perpetually "busy," and any responses provided to the victims are generic and unhelpful. Users may be directed to submit email enquiries that will go unresponded, and there would be no further legitimate escalation pathways.

Stage 4 Cash-Out & Money Laundering

Since cryptocurrency is the only accept for deposits and withdrawals for all the fake investment platforms identified by Group-IB, money recovery is particularly difficult due to the inherent pseudonymity of cryptocurrency transactions. The deposits made by victims are generally moved quickly from initial deposit collection addresses to other cryptocurrency mule wallets.

Cryptocurrency Address Analysis & Money loss estimation

To better understand the threat actors' monetisation methods, an on-chain analysis was conducted on the fake investment platform **tetherglobalItd[.]com**. This platform collects victim funds across multiple cryptocurrencies, including BTC, ETH, and USDT-TRC20. Across all tracked addresses, this domain alone collected a combined total exceeding **US$90,000** in identifiable deposits, spanning hundreds of individual transactions over approximately three years.

An example of a threat actor’s addresses

Currency	Addresses
BTC	bc1qeu024[Redacted]
ETH	0xCF8Fc675[Redacted]
USDT-TRC20	TMUJXv[Redacted]

Financial Summary of Tracked Addresses

Currency	Addresses	Total Deposits	Approx. USD	Period
BTC	2+	~0.570 BTC	~US$38,000+	Nov 2022 – Feb 2026
ETH	1	10 txns, avg ~US$40	~US$400	Aug – Nov 2024
USDT-TRC20	2+	~53,691 USDT	~US$53,691+	Nov 2022 – Feb 2026

As noted in Stage 0, graph analysis reveals that the fake investment platform tetherglobalItd[.]com shares contact information with 23 other fake investment platforms, and shares the same hosting IP address with 208 additional fraudulent domains. Given that a single platform identified over US$90,000 in victim deposits, the 23 contact-linked platforms alone could be estimated to generate a combined revenue exceeding US$2 million for the threat actors. Extrapolating across all 208 IP-connected platforms yields an estimated total revenue of approximately US$187 million across both the Australian and US markets. It should be noted that this estimate is based only on one identified cluster of connected platforms. The actual scale of the operation is likely significantly larger, considering that many platforms remain undetected.

Money Movement Methods

Threat actors regularly rotate deposit addresses on the same website, a tactic typically employed to complicate tracking and reduce the risk of address-level blocking. Additionally, although the domain (tetherglobalItd[.]com) was registered in October 2025, the identified deposit addresses have been active since at least 2022–2023, indicating that these addresses may be reused across multiple fraudulent websites operated by the same actors.

Tracking the on-chain money movement reveals that the threat actors do not employ sophisticated obfuscation techniques. Outgoing funds are transferred directly to accounts on known centralised exchange services, without token swapping, mixing, or layering through intermediary wallets. This straightforward cash-out pattern is consistent across all three cryptocurrency types and suggests the actors seem to rely on the volume and speed of withdrawals rather than technical concealment.

Attribution Evidence: Connected Infrastructure

Further analysis of the USDT-TRC20 cluster uncovered evidence of connected infrastructure. Funds from the primary deposit address (TMUJXvCHY) flowed to a secondary address (TYKzWA18K) that exhibits an identical deposit pattern,with numerous small incoming transactions from retail exchange users, strongly suggesting it belongs to the same group.

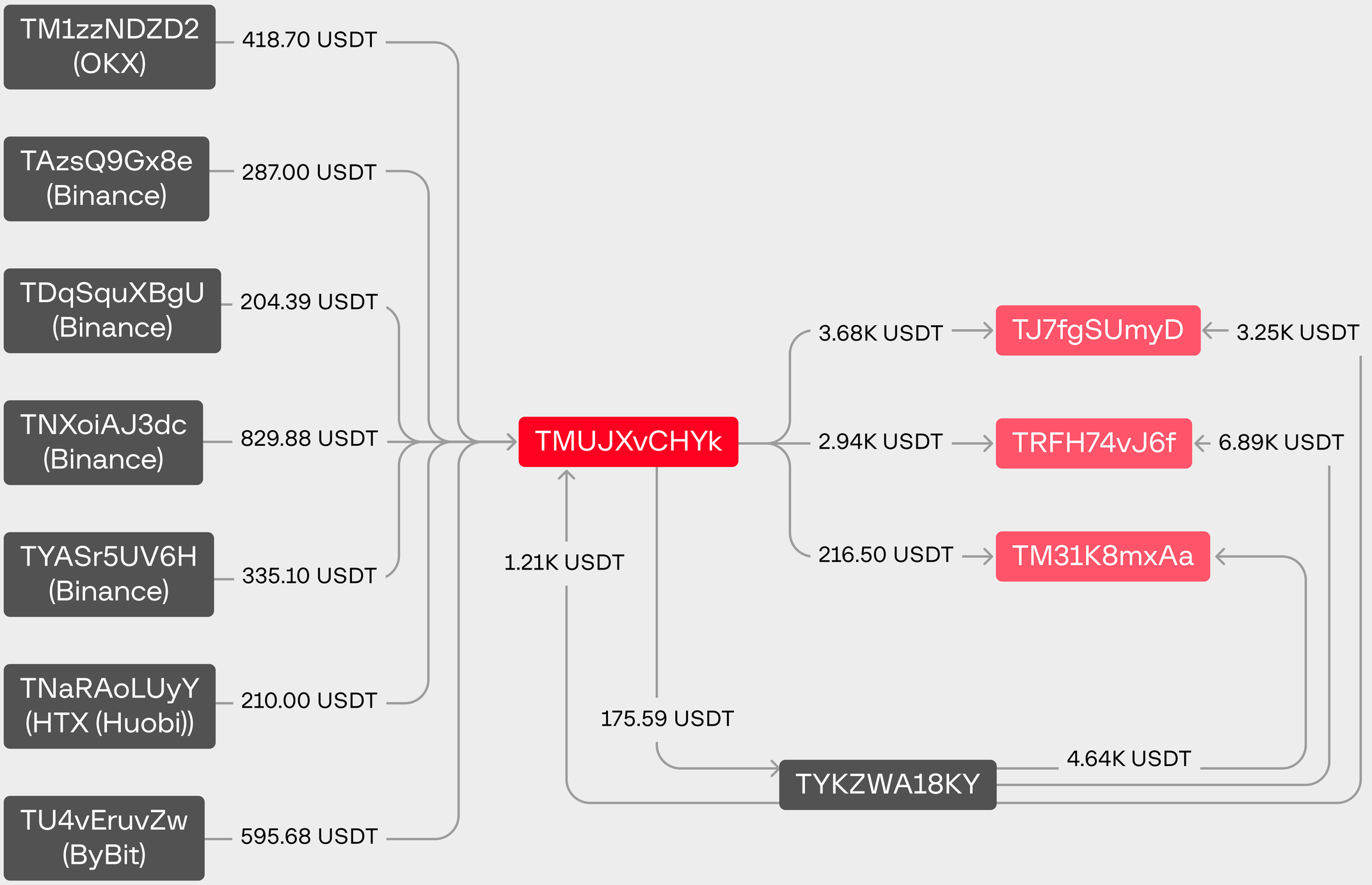


Figure 11. A scheme illustrating the connections of the USDT-TRC20 address TMUJXvCHYkrTLCtyb8URQRZtnnvjTwRoz4

Both addresses share three common downstream recipients, further supporting attribution to a single threat actor. This address recorded 831 transactions between November 2022 and June 2025, with 389 incoming transactions totalling 44,041 USDT from exchanges including Bybit, OKX, Binance, and Paxful.

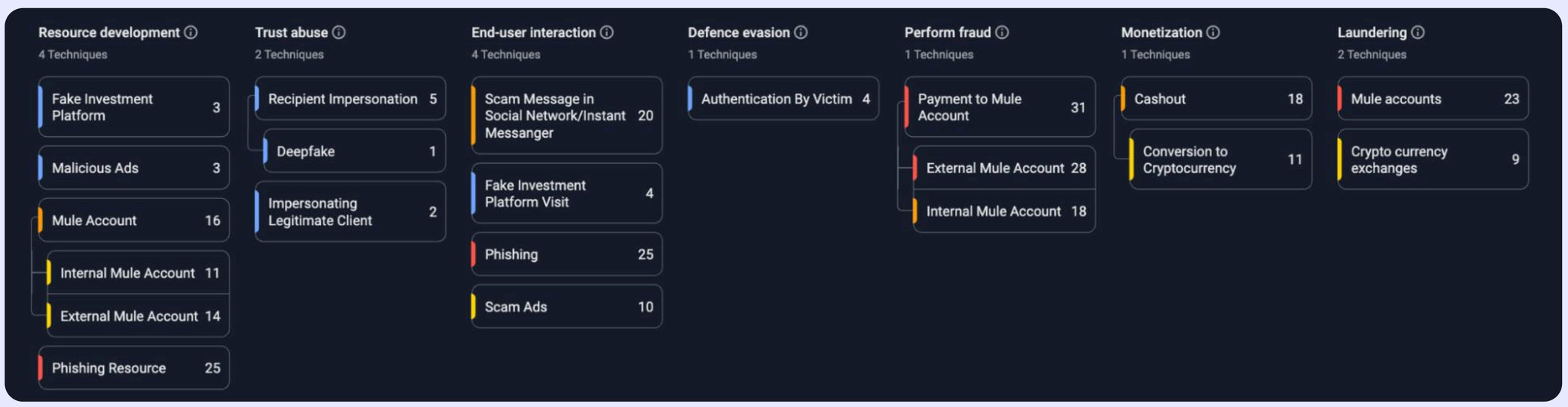
The implication is significant: threat actors behind this scheme earn tens of thousands of dollars on every cryptocurrency address they deploy, they rotate addresses regularly to prevent blocking, and they maintain a broader infrastructure of connected wallets that, taken together, represents a substantially larger operation than any single address would indicate.

Notably, the receiving exchange services are KYC-compliant platforms. This may provide **investigative leverage:** law enforcement or platform compliance teams could potentially identify the account holders receiving the funds.

Stage 5 Recovery Scam (Secondary Victimisation)

The fake platform may eventually be taken down or "disappear" once the operation reaches a certain scale or attracts regulatory attention. However, the victimisation does not necessarily end there.
Victims may subsequently be contacted by the same of affiliated threat actors, masquerading as a "recovery firm", offering to recover lost funds for an upfront fee. This constitutes a recovery scam, a form of secondary victimisation that exploits the victim's desperation and compounds their financial losses.

Fraud Matrix



07 Towards a predictive defence: Group-IB's Cyber Fraud Fusion Approach

The investment scam schemes examined in this fraud research report reveal a critical structural challenge: the attack chains span multiple platforms, jurisdictions, and industries, while the defensive capabilities of individual organisations remain siloed. Banks often have limited visibility into activity on social media. Cryptocurrency exchanges can find it difficult to distinguish victim deposits from legitimate transactions when viewed in isolation. While some institutions do monitor social media and messaging platforms, these efforts are typically fragmented and do not provide a complete, end-to-end view of a fraud or scam case.

Group-IB's Cyber Fraud Fusion approach addresses this gap by unifying cybersecurity capabilities including Threat Intelligence (TI), Digital Risk Protection (DRP), and Investigation services, with fraud prevention capabilities such as Fraud Protection and the Cyber Fraud Intelligence Platform (CFIP) into a single coordinated framework. Rather than responding to investment scams after victims have lost money, Cyber Fraud Fusion enables the ecosystem to predict and disrupt operations at the earliest stages of the attack chain, before they reach scale.

The following scenarios illustrate how Cyber Fraud Fusion would operate against the fraud scheme examined in this article, with specific reference to the findings of this research.

Scenario 2 Cyber Fraud Fusion Applied to Fake Investment Platforms

In a fake investment platform operation, the attack chain proceeds through SEO manipulation and social media advertising, platform onboarding, cryptocurrency deposit collection, withdrawal obstruction, and fund laundering. In this scenario, Group-IB's Cyber Fraud Fusion intervenes across this chain as follows:

Step 1

Detection & Network Exposure — Digital Risk Protection (DRP)

- DRP detects fraudulent investment platforms through domain monitoring, SEO keyword surveillance, and social media advertisement scanning.
- Upon confirming one fraudulent platform (e.g., tetherglobalItd[.]com), Group-IB's Graph analysis reveals the full connected infrastructure — 23 platforms sharing the same contact information and 208 platforms sharing the same IP address.
- DRP initiates mass takedown across the entire connected platform network, rather than addressing one domain at a time.

Step 2

Financial Flow Mapping — Threat Intelligence (TI) & Investigation Services

- The TI and Investigation teams analyse the cryptocurrency deposit addresses associated with the platforms and identifies the centralised exchanges used for cash-out.
- As this research has demonstrated, the threat actors transfer funds directly to KYC-compliant exchanges without obfuscation — no token swapping, mixing, or layering through intermediary wallets.
- The TI team maps the transaction patterns, identifies downstream recipient addresses, and profiles the USDT-TRC20 address clusters that support single-actor attribution.

Step 3

Fund Interception — Fraud Protection & CFIP

- The Fraud team shares the flagged cryptocurrency addresses and associated risk signals in real time through CFIP to member institutions — including cryptocurrency exchanges (Binance, Bybit, OKX, Coinbase), banks, and payment platforms.
- CFIP members flag transactions to the identified threat actor addresses, enabling exchanges to freeze or block transfers before funds are laundered.
- Given that this research identified over US$90,000 in deposits on a single platform and an estimated US$187 million across the connected network, the potential for loss prevention is substantial.

Step 4

Identification — Investigation Services

- The Investigation team leverages the KYC data held by the receiving exchanges to identify the real individuals behind the cryptocurrency wallets.
- The direct, unobfuscated transfer pattern identified in this research—from victim deposit addresses to exchange accounts without mixing or layering—provides a clear investigative path from stolen funds to identifiable persons.

Outcome

The platform network is taken down at scale (208 domains rather than just one), victim deposits are intercepted at the exchange level before laundering is completed, and the investigation team identifies the operators for law enforcement referral. The estimated US$187 million revenue potential of this network is significantly reduced or eliminated.

Why Cyber Fraud Fusion Matters

The critical insight of the Group-IB's Cyber Fraud Fusion approach is that investment scam operations have **multiple interdependent points of vulnerability** — fraudulent advertisements, cryptocurrency transactions, and platform infrastructure. No single product or team can address all of these simultaneously. However, when DRP detects the initial brand abuse, TI maps the infrastructure and financial flows, CFIP distributes alerts across the financial ecosystem, and Investigation traces funds to real identities, the combined effect is a defence that operates at the speed and scale of the attack itself.

Traditional approaches to investment fraud are reactive.They identify and report incidents after funds have been lost. Group-IB's Cyber Fraud Fusion reverses this dynamic by correlating risk signals across the entire attack chain in real time, enabling the ecosystem to act at the earliest stage of detection rather than the latest stage of loss.

08 Conclusion

The fake investment platform scheme examined in this article reveals a common and critical characteristic of modern investment fraud: fraudsters do not target technical security — they target and exploit trust. By constructing professional-looking platforms that are nearly indistinguishable from regulated financial services, fabricating returns to build investor confidence, and operating at industrial scale across a network of over 200 connected domains, these schemes succeed by positioning themselves precisely where trust already exists and redirecting it.

Australia is now one of the top global targets for investment fraud, with US$837.7 million lost to investment scams alone in 2025. In the United States, investment scam losses reached US$7.9 billion in the same period. Existing controls such as regulatory warnings, platform moderation, consumer education are crucial but demonstrably insufficient against an adversary that operates as an organised cyber-fraud ecosystem with sophisticated infrastructure, cross-jurisdictional reach, and a deep understanding of human psychology.

In the face of such evolving and overwhelming odds, Group-IB recommends that a new approach: one that matches the coordination of the attackers with equivalent coordination among defenders.

Group-IB's Cyber Fraud Fusion approach—unifying threat intelligence, digital risk protection, fraud prevention, and investigation under a single coordinated framework—offers a model for this new architecture of defence. By connecting the detection of fraudulent advertisements with real-time alerts to financial institutions, and linking cryptocurrency analysis to exchange-level fund interception, Group-IB's Cyber Fraud Fusion enables the ecosystem to predict and disrupt investment scam operations before they reach scale.

Cross-platform intelligence sharing through CFIP, proactive brand protection through DRP, threat actor profiling through TI, and fund tracing through investigation services together form a powerful, unified defense. The architecture of deception is sophisticated. The architecture of defence must be more so.

09 Recommendations

The industrial scale of fake investment platform networks demands responses tailored to each stakeholder group.

For Individuals

- Verify any investment platform's credentials through official regulatory registers: ASIC Connect for Australian entities, and SEC EDGAR / FINRA BrokerCheck for US firms — and confirm that the platform you are visiting matches the official domain of the registered entity.
- Be sceptical of any platform that exclusively accepts cryptocurrency deposits; legitimate Australian investment platforms typically accept bank transfers, BPAY, and debit/credit card payments.
- If a platform requires payment to process a withdrawal — whether labelled as tax, fees, insurance, or compliance charges — it is almost certainly fraudulent.
- Be aware that "recovery firms" contacting you after a loss may be operated by the same threat actors.
- Report suspected scams to Scamwatch (AU), ASIC (AU), the FTC (US), SEC (US), or local law enforcement.

For Cryptocurrency Exchanges

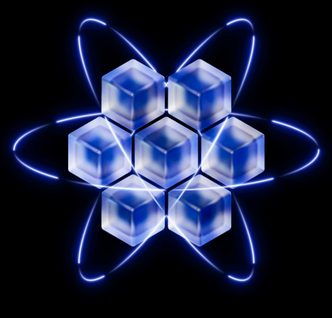
- Implement transaction monitoring rules to flag deposits to known or suspected fraudulent platform addresses.
- As this research demonstrates, threat actors transfer stolen funds directly to KYC-compliant exchanges without obfuscation — meaning that the receiving accounts can be identified and acted upon.
- Exchanges should consider participating in cross-institutional intelligence-sharing frameworks to receive flagged addresses in real time.
- Proactive monitoring for accounts exhibiting patterns consistent with investment scam cash-out — such as receiving numerous small deposits from diverse retail sources followed by rapid consolidation and withdrawal — can help detect threat actor accounts before they are flagged externally.

For Financial Institutions

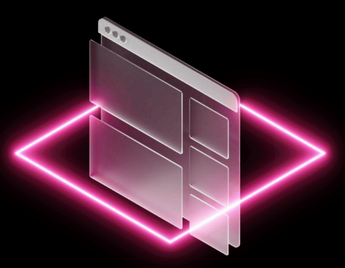
- Monitor for brand impersonation — particularly the cloning of institutional websites, branding, and AFSL numbers by fraudulent platforms.
- Implement alert mechanisms for clients making cryptocurrency purchases or transfers that may be destined for identified fraudulent platforms.
- Share threat intelligence on identified mule accounts, fraudulent domains, and associated cryptocurrency addresses with industry peers and regulators.
- Invest in customer education that specifically addresses the mechanics of fake investment platforms, including the "trial fund" psychological trap and the withdrawal obstruction cycle.

For the Ecosystem

Group-IB's Cyber Fraud Fusion approach, as detailed in this article, provides the operational framework for the cross-platform intelligence sharing that the current threat landscape demands. Specific capabilities that would strengthen the collective defence include:



Cyber Fraud Intelligence Platform (CFIP): Real-time, privacy-preserving exchange of anonymised risk signals between banks, cryptocurrency exchanges and payment providers. CFIP enables participating exchanges to freeze or block transactions to identified threat actor addresses before funds are laundered. Given the estimated $187 million revenue of the connected platform network, the potential for ecosystem-wide loss prevention is substantial. CFIP's patented Distributed Tokenisation technology ensures that all customer data remains anonymised, enabling collaboration without compromising privacy compliance.



Digital Risk Protection (DRP): Automated detection and takedown of impersonation sites, fake social media advertisements, phishing URLs, and fraudulent platform networks. As demonstrated in this research, graph analysis of a single confirmed platform can expose an entire network of 208 connected domains — enabling mass enforcement rather than reactive, one-at-a-time takedowns. DRP's continuous monitoring of social media, search engine results, domain registrations, and messenger platforms ensures that fraudulent infrastructure is identified at the earliest possible stage.



Threat Intelligence (TI) and Investigation Services: Dark web monitoring, threat actor infrastructure analysis, cryptocurrency address tracking, and investigation capabilities that trace funds from victim deposits to identifiable individuals. As this research has shown, threat actors transfer stolen funds directly to KYC-compliant exchanges without obfuscation — providing a clear investigative path that, when combined with TI-driven address mapping and USDT-TRC20 cluster analysis, can support law enforcement identification and prosecution of the individuals behind these operations.

10 Indicator of Compromise (IOCs)

Example of Fake Investment Platforms

https://etncrypto[.]com
https://tetherearnmining[.]com
https://tetherglobalItd[.]com
https://t[.]me/CEO_TETHERGLOBAL
https://www.cryptoglobalex[.]space
https://hashxcapital[.]com
https://nexmutual[.]com
https://t[.]me/Nexusmutual002
https://ts.tradespotau[.]com
https://vnbtc[.]com
filename[:]"/h5/"

GROUP-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,600+
Successful investigations of high-tech crime cases

500+
Employees

60
Countries

$1 bln+
Saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

*According to Cybersecurity Excellence Awards

11
Unique Digital Crime Resistance Centers

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- Forrester®
- datos INSIGHTS
- kuppingercole ANALYSTS
- Gartner®
- IDC
- FROST & SULLIVAN

Fight against cybercrime



GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785