GLOBAL ANTI-SCAM CENTRE

GASC INTELLIGENCE REPORT · NO. 1

International Investment Fraud Networks

Financial Flows and Investigative Challenges in 2026

GASC Intelligence Team · November 2026 · Data cut-off: 21 November 2026

globalantiscam.com

GLOBAL ANTI-SCAM CENTRE

ABOUT THIS REPORT

GASC Intelligence Reports bring together official statistics and public enforcement records on cross-border fraud. This first edition examines how international investment-fraud networks acquire victims, move money and respond to enforcement. It is written for journalists, lawyers, compliance teams and policymakers, and for victims and families seeking context.

DATA CUT-OFF

21 November 2026. Every official figure was checked against its primary source on that date. Field observations are labelled as approximate.

SUGGESTED CITATION

Global Anti-Scam Centre (2026). *International Investment Fraud Networks: Financial Flows and Investigative Challenges in 2026*. GASC Intelligence Report No. 1, data cut-off 21 November 2026. Sydney: Global Anti-Scam Centre. https://globalantiscam.com/research/international-investment-fraud-networks-2026/

IMPORTANT INFORMATION

This report is general information. It draws on public sources and on generalised, approximate GASC investigator field observations, which are clearly labelled and are not official statistics. It is not legal, financial or investment advice. References to charges, indictments and forfeiture complaints describe allegations; defendants are presumed innocent unless proven guilty. Figures are as published by the cited agencies at the data cut-off and may later be revised. The report contains no client information and no case identifiers.

© 2026 Global Anti-Scam Centre. Level 35, Tower One, 100 Barangaroo Avenue, Barangaroo NSW 2000, Australia · info@globalantiscam.com · +61 2 7257 0211 · globalantiscam.com

Contents

At a glance 4

Key findings 5

1. Scale of the problem 6

2. How networks are organised 8

3. Cross-border money flows 12

4. The 2026 enforcement response 14

5. Investigative and legal challenges 16

6. Implications for victims, lawyers and institutions 18

7. Outlook for 2027 19

8. Methodology and sources 20

9. How to cite this report 22

Figures and tables

Figure 1. Investment fraud within total reported scam losses, US and Australia, 2024–2025

Figure 2. Inside an investment-fraud syndicate (GASC investigator field observations)

Figure 3. Reported scam losses by payment method, Australia, 2025

Figure 4. ASIC online scam takedowns, FY25 and FY26

Table 1. Selected public enforcement actions, October 2025 to November 2026

Table 2. Principal datasets used in this report

At a glance

This report brings together official data and public enforcement records from Australia, the United States, the United Kingdom, the European Union and Singapore to show how international investment-fraud networks acquire victims, move money and respond to enforcement, alongside clearly labelled and approximate GASC investigator field observations. Every official figure is footnoted to a primary source and was checked against that source on 21 November 2026.

KEY STATISTICS AT A GLANCE

US$8.65bn
Investment-fraud losses reported to the FBI IC3 in 2025
FBI IC3

A$837.7m
Australian investment-scam losses in 2025, the largest category
NASC

19,400+
Online scams removed by ASIC in FY26, up 182%
ASIC

5,811
Arrests in INTERPOL Operation First Light 2026, 97 countries and territories
INTERPOL

~127,271 BTC
Subject of a US civil forfeiture complaint, about US$15bn at filing
US DOJ

2,329
FCA warnings about unauthorised or potentially fraudulent firms in 2025
FCA

All figures are sourced in the notes. Losses are as reported to each agency.

Key findings

- **Investment fraud is the costliest form of reported scam in both the United States and Australia.** The FBI's Internet Crime Complaint Center (IC3) recorded US$8.65 billion in reported investment-fraud losses in 2025, from 72,984 complaints.[1] Australia's National Anti-Scam Centre (NASC) recorded A$837.7 million in combined investment-scam losses in 2025, the largest single category.[2]

- **The trends are diverging.** US reported investment-fraud losses rose from US$6.57 billion in 2024 to US$8.65 billion in 2025.[3] Australian investment-scam losses fell 11.4%, from A$945.0 million to A$837.7 million, even as total combined scam losses rose 7.8% to A$2.18 billion.[4] On GASC's calculation from the published totals, investment fraud's share of reported losses rose from about 40% to 41% in the US and fell from about 47% to 38% in Australia.

- **The front end has been industrialised.** ASIC removed more than 19,400 online scams in FY26, up 182% on the previous year, including 7,051 fake investment platforms.[5] Europol describes a "crime-as-a-service" supplier of fraudulent trading websites serving call-centre operators in Albania, Kosovo and North Macedonia.[6]

- **The money moves through layers built to look legitimate.** Public cases describe shell-company networks, payment intermediaries, cryptocurrency platforms, casinos and prime property. The US Treasury found that Cambodia-based Huione Group laundered at least US$4 billion in illicit proceeds between August 2021 and January 2025.[7]

- **Enforcement in 2025–26 has reached record scale but remains largely disruptive.** In October 2025 the US Department of Justice filed a civil forfeiture complaint against approximately 127,271 bitcoin, then worth about US$15 billion.[8] INTERPOL's Operation First Light 2026 produced 5,811 arrests across 97 countries and territories.[9] Restraining assets is not the same as returning them to victims, and many networks operate from jurisdictions beyond the direct reach of victims' home authorities.

- **Syndicates operate as a supply chain of specialist providers.** In GASC investigator field observations, separate providers supply ready-made fraud platforms, lead lists and laundering services to syndicate owners, with each component placed in a different country. These are approximate observations, not published data; public cases corroborate several elements.[10]

1. Federal Bureau of Investigation, Internet Crime Complaint Center, *2025 Internet Crime Report* (2026), PDF pp. 8 and 26. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
2. National Anti-Scam Centre (ACCC), *Targeting Scams: Report of the National Anti-Scam Centre on scams data and activity 2025* (March 2026), PDF p. 8. https://www.accc.gov.au/system/files/targeting-scams-report-2025.pdf
3. FBI IC3, *2025 Internet Crime Report*, PDF p. 26 (three-year loss table).
4. NASC, *Targeting Scams 2025*, PDF pp. 4, 7 and 8 (Table 3).
5. ASIC, media release 26-195MR, "ASIC warns scammers are using AI to spin vast webs of deception" (17 August 2026). https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-195mr-asic-warns-scammers-are-using-ai-to-spin-vast-webs-of-deception
6. Europol, "Investment scams with potential victims in at least 50 countries: over 100 servers seized" (3 November 2026). https://www.europol.europa.eu/media-press/newsroom/news/investment-scams-potential-victims-in-least-50-countries-over-100-servers-seized
7. US Department of the Treasury, press release sb0278, "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia" (14 October 2025). https://home.treasury.gov/news/press-releases/sb0278
8. US Department of Justice, Office of Public Affairs, "Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes" (14 October 2025). https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged
9. INTERPOL, "Over 5,800 arrests, USD 293 million intercepted in global fraud bust" (9 July 2026). https://www.interpol.int/en/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust
10. GASC investigator field observations (approximate; see Section 2.4 and Methodology). Corroborating public sources are cited in Sections 2.4 and 3.4.

- **Victims face a second wave of harm.** Europol reports that one network re-contacted people who had already lost money, offering to recover their funds for an initial deposit of €500.[11] Recovery fraud is now a recognised feature of the investment-scam lifecycle.

1. Scale of the problem

1.1 United States

The IC3 received 1,008,597 complaints in 2025, reporting losses of US$20.877 billion, a 26% increase on 2024.[12] Investment fraud was again the largest single loss category, at US$8,648,617,756, up from US$6,570,639,864 in 2024 and US$4,570,275,683 in 2023.[13] Investment complaints also rose sharply, from 47,919 in 2024 to 72,984 in 2025.[14]

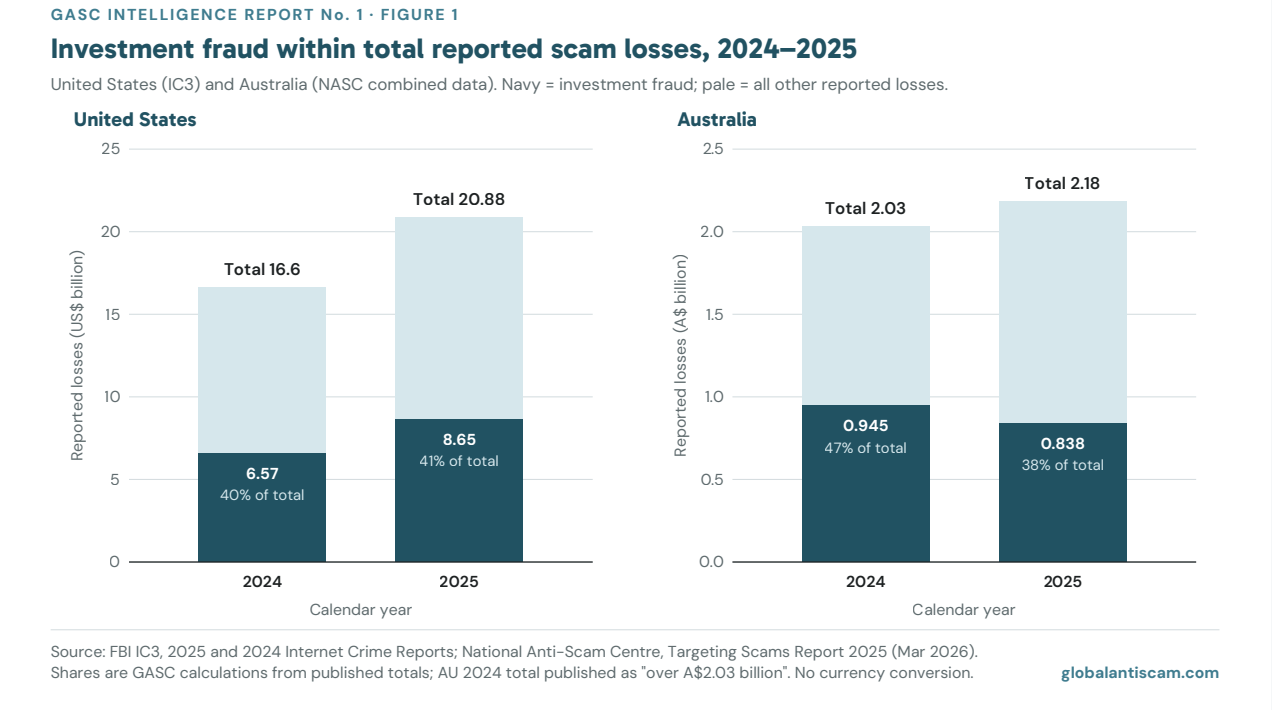
Cryptocurrency is central to the US picture. The IC3 reports that cryptocurrency investment fraud was "the highest source of financial losses to Americans in 2025 with $7.2 billion reported in losses", and attributes these schemes largely to "organized criminal enterprises based in Southeast Asia using victims of human trafficking as forced labor".[15] The IC3 also notes that investment complaints with a reported artificial-intelligence nexus exceeded US$632 million in losses, and it cautions that many victims may not realise AI was involved.[16]

1.2 Australia

The NASC's combined dataset, which draws on Scamwatch, ReportCyber, the Australian Financial Crimes Exchange (AFCX), IDCARE and ASIC, recorded A$2.18 billion in reported scam losses in 2025, up 7.8% from over A$2.03 billion in 2024. Report volumes were broadly stable, at 481,523 compared with 494,732.[17] Investment scams remained the largest category by loss, at A$837.7 million, but fell 11.4% from A$945.0 million in 2024.[18] The NASC also reports that the median loss fell from A$500 to A$400, which it reads as more people being successfully targeted while losing smaller amounts on average.[19]

11. Europol, "Call centres dismantled and ten arrested in EUR 50 million online fraud case" (29 April 2026). https://www.europol.europa.eu/media-press/newsroom/news/call-centres-dismantled-and-ten-arrested-in-eur-50-million-online-fraud-case
12. FBI IC3, *2025 Internet Crime Report*, PDF p. 6.
13. FBI IC3, *2025 Internet Crime Report*, PDF p. 26.
14. FBI IC3, *2025 Internet Crime Report*, PDF p. 25 (three-year complaint table).
15. FBI IC3, *2025 Internet Crime Report*, PDF p. 11.
16. FBI IC3, *2025 Internet Crime Report*, PDF p. 40.
17. NASC, *Targeting Scams 2025*, PDF pp. 4 and 7.
18. NASC, *Targeting Scams 2025*, PDF p. 8 (Table 3).
19. NASC, *Targeting Scams 2025*, PDF p. 4.

Figure 1. Investment fraud within total reported scam losses, United States and Australia, 2024–2025



Investment fraud's share of reported losses rose slightly in the US and fell in Australia, even as total reported losses rose in both. *Sources: FBI IC3, 2025 and 2024 Internet Crime Reports; NASC, Targeting Scams Report 2025. Shares calculated by GASC.*

1.3 United Kingdom and Singapore

The UK Financial Conduct Authority (FCA) does not publish an equivalent national loss series in the sources reviewed for this report. Its Warning List is nevertheless a useful indicator of activity. The FCA issued 2,329 warnings about unauthorised or potentially fraudulent firms and individuals in 2025, compared with 2,240 in 2024.[20] Of the 2025 alerts, 1,528 related to unauthorised crypto entities and promotions.[21] By 20 August 2026 the FCA had issued more than 1,200 warnings for the year.[22]

In Singapore, the Monetary Authority of Singapore (MAS) maintains an Investor Alert List of persons who may be wrongly perceived as licensed or authorised by MAS. At the data cut-off, the list carried a notice that MAS will no longer publish the names and online identifiers of entities impersonating MAS-regulated financial institutions, and it directs the public to verify institutions through official channels.[23] This is a useful reminder that alert lists are designed as consumer-protection tools, not as complete measures of the threat.

20. Financial Conduct Authority, "FCA cracks down on illegal promotions and market abuse in first year of new strategy" (9 July 2026). https://www.fca.org.uk/news/press-releases/fca-cracks-down-illegal-promotions-and-market-abuse-first-year-new-strategy
21. FCA, freedom-of-information release FOI2026/00006, "Information on crypto-related alerts – February 2026" (20 February 2026). https://www.fca.org.uk/freedom-information/information-crypto-related-alerts-february-2026
22. FCA, "Consumers warned to beware of risky mini-bonds and loan notes" (20 August 2026). https://www.fca.org.uk/news/press-releases/consumers-warned-beware-risky-mini-bonds-and-loan-notes
23. Monetary Authority of Singapore, Investor Alert List (accessed 21 November 2026). https://www.mas.gov.sg/investor-alert-list/

1.4 Reading the numbers with care

None of these series is directly comparable. The IC3 counts complaints filed by the public. The NASC combines several reporting channels and adjusts for duplication. FCA figures count regulatory alerts, not losses. All are affected by under-reporting, and none captures losses that victims do not recognise as fraud. GASC therefore compares shares and directions of travel within each jurisdiction rather than converting currencies or adding national totals together.

> **"AI is making investment scams more convincing and harder to detect. A simple online search is not enough to verify whether an opportunity is legitimate."**
>
> **Sarah Court, Chair, Australian Securities and Investments Commission**
> ASIC media release 26-195MR, 17 August 2026

2. How networks are organised

Sections 2.1 to 2.3 draw only on findings published by courts, prosecutors, regulators and international policing bodies. Section 2.4 adds GASC investigator field observations, which are clearly marked and kept separate from the official record. Neither describes any individual GASC matter.

2.1 The front end: advertising, endorsements and fake platforms

Contact usually begins with an advertisement or an unsolicited message. ASIC reports that potential investors "may be taken from an ad on a well-known platform to a fake news article featuring celebrity endorsements and fabricated public comments", followed by "scripted phone calls, fake investment platforms and even small profit payments to build trust".[24] In FY26 the most impersonated public figures in Australian online scams were associated with A$7.4 million in reported losses.[25]

Europol's November 2026 operation shows how this front end is supplied as a service. A company allegedly operating from Cyprus and Israel supplied fraudulent trading websites to criminal groups. Deceptive affiliate-marketing advertisements directed people to the platforms, and the personal data collected was "sold to criminal groups operating call centres".[26] The UK FCA's April 2026 week of action against illegal "finfluencers", involving 17 regulators, identified 1,267 illegal financial adverts on Meta platforms, 66% of them from firms or individuals already on the FCA Warning List.[27]

2.2 The engine room: call centres and scam compounds

Two organisational models recur in the public record.

24. ASIC, 26-195MR (17 August 2026).
25. ASIC, 26-195MR (17 August 2026), citing Scamwatch data.
26. Europol (3 November 2026).
27. FCA, "FCA spearheads global action to stop illegal finfluencers" (24 April 2026). https://www.fca.org.uk/news/press-releases/fca-spearheads-global-action-stop-illegal-finfluencers

The first is the corporate-style call centre. In the Tirana case dismantled in April 2026, Europol describes a network of up to 450 employees, with "conversion agents" handling acquisition and "retention agents" managing victims over long periods, supported by finance, IT, human-resources and back-office teams. Operators worked in language teams of six to eight people covering German, English, Italian, Greek and Spanish, and were paid a monthly salary of about €800 plus commission.[28]

The second is the forced-labour scam compound. US and UK authorities describe compounds in Cambodia and Burma where trafficked workers are held against their will and made to defraud victims overseas under threat of violence.[29] OFAC states that the Prince Group operated at least ten scam compounds in Cambodia.[30] The US Department of Justice reports that two managers of the Shunda compound in Burma relocated to a compound in Cambodia after Shunda was seized, which illustrates how these operations displace rather than disappear.[31]

2.3 The conversion of trust into payments

Across jurisdictions the sequence is similar. Victims make a small initial deposit, are shown fictitious profits, are pressed to invest larger sums, and then face delays, "taxes" or fees when they try to withdraw.[32] The IC3 reports that victims are often offered loans to encourage larger investments.[33]

2.4 GASC investigator field observations: the syndicate as an ecosystem

The official record describes individual call centres and compounds. Across their investigations, GASC investigators observe that these sit within a wider commercial ecosystem, in which syndicate owners buy specialist services from third parties rather than running every function themselves. The observations below are generalised from multiple matters, contain no client or case identifiers, and are presented separately from the cited official statistics.

GASC INVESTIGATOR FIELD OBSERVATIONS

Approximate figures observed across GASC investigations. Not published or officially verified data.

Set-up providers. Third-party providers research a company name suited to the fraud, often borrowing the name or licensing details of a genuine company that has no website of its own. They register the domain, design the website, set up email accounts and a VoIP telephone number, and arrange an office address. A single provider may hold up to around 20 ready-made websites waiting for syndicates to use. ASIC separately warns that scammers misuse licence details by "using another entity's licence number", and Europol's November 2026 operation targeted a suspected supplier of fraudulent trading platforms to call-centre operators.[34]

28. Europol (29 April 2026).
29. US Department of Justice, Office of Public Affairs, "Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting Americans" (23 April 2026). https://www.justice.gov/opa/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers-targeting ; UK Government, "UK and US take joint action to disrupt major online fraud network" (14 October 2025). https://www.gov.uk/government/news/uk-and-us-take-joint-action-to-disrupt-major-online-fraud-network
30. US Treasury, sb0278 (14 October 2025).
31. US DOJ (23 April 2026).
32. Europol (3 November 2026); ASIC, 26-195MR (17 August 2026).
33. FBI IC3, *2025 Internet Crime Report*, PDF p. 11.
34. ASIC, 26-195MR (17 August 2026); Europol (3 November 2026). See also US DOJ (23 April 2026) on the seizure of 503 fake investment domains.

Lead brokers. Separate brokers sell spreadsheets of names, addresses, telephone numbers, email addresses, employment details and approximate wages, typically at around US$1 per lead in sheets of around 10,000. Lists include former fraud victims, and the same leads are recycled across different platforms. Europol reports that personal data collected through deceptive advertising was "sold to criminal groups operating call centres".[35]

The boiler room (front room). A front room typically employs 20 to 100 staff, mostly foreign nationals in the host country. "Trade qualifier" (TQ) operators each make around 400 calls a day on a low base wage plus commission on first deposits. An administrator sends lure emails and a room manager oversees the floor.

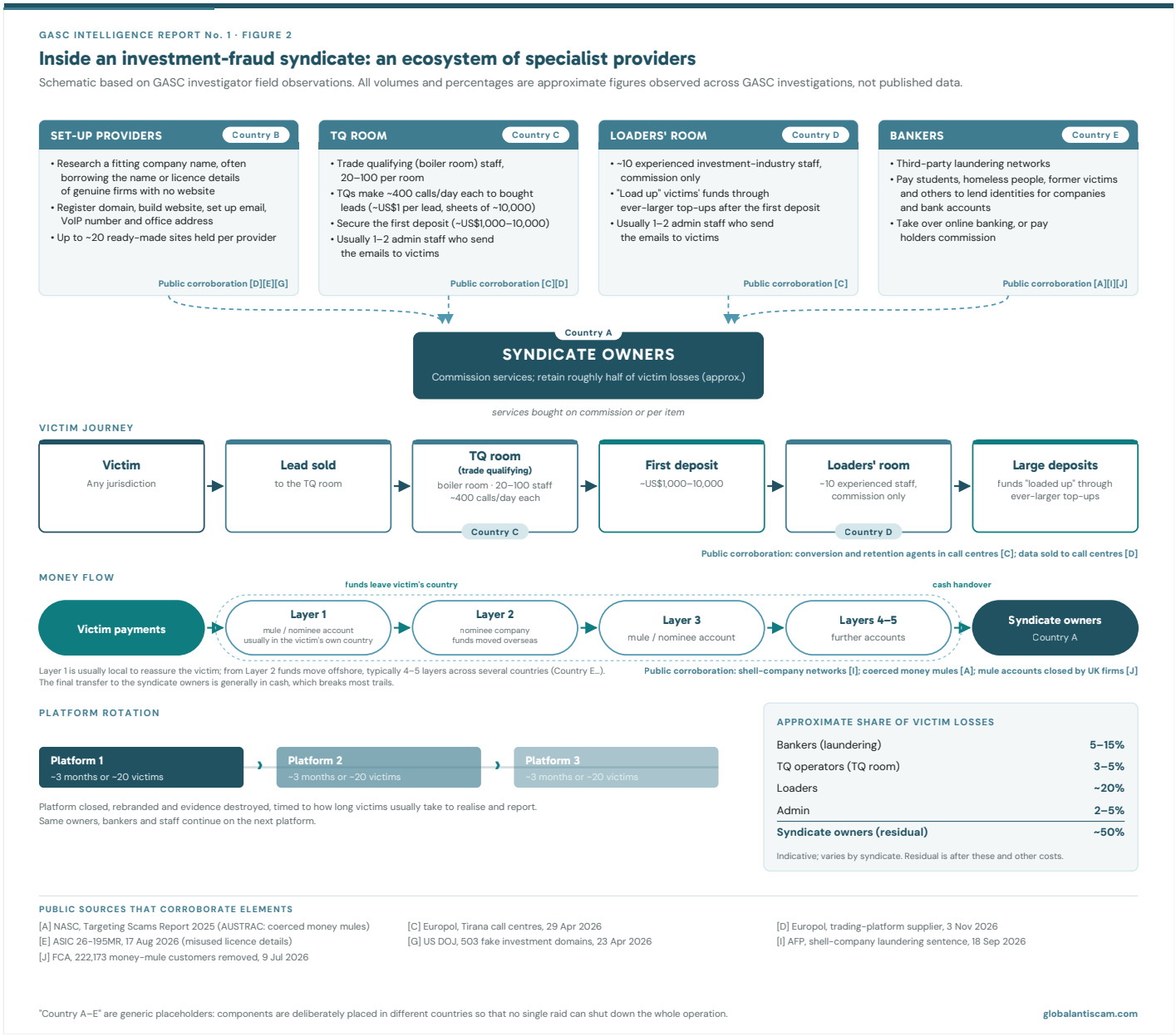
The loaders' room. Once a victim makes an initial deposit, typically around US$1,000 to US$10,000, their details pass to a separate room of around ten foreign staff with investment-industry experience. "Loaders" are so called because they "load up" the victim's funds: after the first deposit they press the victim into ever-larger top-ups. Loaders work on commission only and can earn around US$25,000 a week. Europol's description of "conversion agents" handling acquisition and "retention agents" managing victims over long periods reflects the same two-stage division of labour.[36]

Jurisdictional dispersal. Each component typically sits in a different country, both to frustrate law enforcement and so that no single raid can shut down the whole operation. The Europol case announced in November 2026, with a platform supplier allegedly operating from Cyprus and Israel and call centres in Albania, Kosovo and North Macedonia, illustrates the pattern.[37]

All figures in this box are approximate and reflect what GASC investigators have observed across investigations. They are not published or officially verified data.

35. Europol (3 November 2026).
36. Europol (29 April 2026).
37. Europol (3 November 2026).

Figure 2. Inside an investment-fraud syndicate: an ecosystem of specialist providers (GASC investigator field observations)



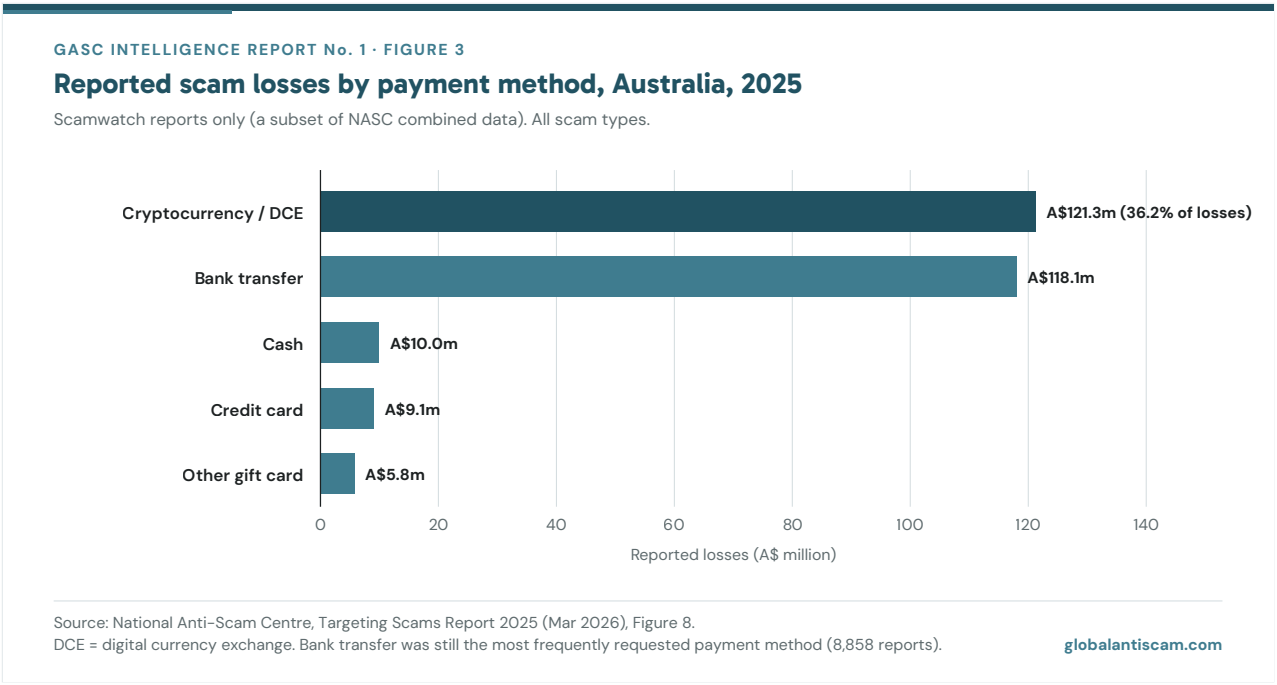
Syndicate owners at the centre buy services from set-up providers, a trade qualifying (TQ) room (the boiler room, where trade qualifiers make about 400 calls a day to bought leads, with usually 1–2 admin staff per room who send emails to victims), a loaders' room (loaders "load up" the victim's funds, pressing for ever-larger top-ups after the first deposit, also usually with 1–2 admin staff per room) and bankers. The victim journey runs from a purchased lead to the TQ room, to a first deposit, then to the loaders' room, while money passes through four to five layers of mule and nominee accounts: the first-layer account is usually in the victim's own country, from the second layer funds are moved overseas, and the final transfer to the syndicate owners is generally made in cash, which breaks most of the money trail. All volumes and percentages are approximate figures observed across GASC investigations, not published data. *Source: GASC investigator field observations (approximate). Corroborating public sources keyed in the figure: NASC/AUSTRAC; Europol (29 April and 3 November 2026); ASIC 26-195MR; US DOJ; AFP; FCA.*

3. Cross-border money flows

3.1 Payment rails

The public record shows victim funds moving through both the banking system and cryptocurrency channels. In Australian Scamwatch data, cryptocurrency and digital currency exchanges (DCEs) accounted for 36.2% of reported losses in 2025, A$121.3 million, overtaking bank transfers (A$118.1 million), although bank transfer remained the payment method most often requested by scammers.[38] The NASC notes that the cryptocurrency/DCE category captures money "moving outside of traditional banks".[39]

Figure 3. Reported scam losses by payment method, Australia, 2025 (Scamwatch data)



Cryptocurrency and digital currency exchanges overtook bank transfers as the largest loss channel in Scamwatch data in 2025. *Source: NASC, Targeting Scams Report 2025, Figure 8. Scamwatch reports only; all scam types.*

3.2 Layering: shell companies and payment intermediaries

Sentencing and sanctions material consistently describe corporate layering. In the Australian case sentenced in September 2026, the offender "used a network of shell companies to conceal and transfer funds generated through fraudulent online investment schemes" between June and November 2023.[40] OFAC designated

38. NASC, *Targeting Scams 2025*, PDF p. 39 (Scamwatch data only).
39. NASC, *Targeting Scams 2025*, PDF p. 39, note 88.
40. Australian Federal Police, "Man jailed for role in $50 million scam which swindled more than 1000 victims" (18 September 2026). https://afp.gov.au/news-centre/media-release/man-jailed-role-50-million-scam-which-swindled-more-1000-victims

117 Prince Group-affiliated businesses, "the vast majority of which are offshore shell companies that engage in no apparent real commercial or business activity", and states that Chen Zhi laundered proceeds "through a complicated network of over 100 shell and holding companies all around the world".[41]

Payment intermediaries sit between the scam and the wider financial system. FinCEN's final rule under section 311 of the USA PATRIOT Act severed Huione Group from the US financial system. Treasury reports FinCEN's finding that, of the at least US$4 billion Huione laundered, at least US$36 million came from virtual-currency investment scams, at least US$37 million from DPRK cyber heists and US$300 million from other cyber scams.[42]

3.3 Integration: property, hospitality and digital assets

The final stage places proceeds into assets that look legitimate. The UK government reports that Chen Zhi's network incorporated businesses in the British Virgin Islands and invested in London property, including a £12 million mansion, a £100 million office building in the City of London and seventeen flats, all frozen by UK sanctions.[43] OFAC describes Prince Group compounds run under the umbrella of a hotel and casino business.[44] The US forfeiture complaint concerns bitcoin "previously stored in unhosted cryptocurrency wallets whose private keys the defendant had in his possession".[45]

3.4 GASC investigator field observations: bankers, layering and rotation

GASC INVESTIGATOR FIELD OBSERVATIONS

Approximate figures observed across GASC investigations. Not published or officially verified data.

"Bankers". Laundering is commonly outsourced to third-party networks that GASC investigators refer to as bankers. They pay university students, homeless people, former victims and others to lend their identities to open companies and bank accounts, then either take over the online-banking logins or pay the account holder a commission to move money through the account. Bankers typically use four to five layers of bank accounts before funds reach the syndicate owners. In GASC investigators' experience, the first-layer account is usually in the victim's own country, which reassures the victim that their money is not leaving the country; from the second layer, funds are moved overseas, away from the victim's jurisdiction; and the final transfer to the syndicate owners is generally made in cash, which breaks most of the money trail. This is consistent with the shell-company network described in the September 2026 Australian sentence, with AUSTRAC's finding that most high-volume crypto ATM users it examined were scam victims or coerced money mules, and with UK firms removing 222,173 customers as money mules.[46]

Approximate division of proceeds. As observed by GASC investigators, bankers take around 5 to 15% of victim losses, TQ operators 3 to 5%, loaders around 20% and administrators 2 to 5%. After these and other operating costs, syndicate owners retain roughly half. Shares vary between syndicates and do not sum exactly.

41. US Treasury, sb0278 (14 October 2025).
42. US Treasury, sb0278 (14 October 2025); FinCEN, "FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System" (14 October 2025). https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system
43. UK Government (FCDO), "UK and US take joint action to disrupt major online fraud network" (14 October 2025).
44. US Treasury, sb0278 (14 October 2025).
45. US DOJ (14 October 2025).
46. AFP (18 September 2026); NASC, *Targeting Scams 2025*, PDF p. 14 (AUSTRAC Crypto Taskforce); FCA (9 July 2026).

Platform rotation. Some syndicates run a platform for around 20 victims, or about three months, before switching to a new one. The timing reflects how long victims usually take to realise they have been defrauded and to report it, which allows the operation to continue and evidence to be destroyed before police become involved.

All figures in this box are approximate and reflect what GASC investigators have observed across investigations. They are not published or officially verified data.

> **"The scammers behind these crimes often believe layers of companies, financial transactions and international money movements will shield them from detection. This is not the case."**
>
> **Detective Superintendent Marie Andersson, Australian Federal Police**
> AFP media release, 18 September 2026

4. The 2026 enforcement response

Enforcement in 2026 built on the coordinated US–UK action of 14 October 2025, when OFAC designated 146 targets in the Prince Group transnational criminal organisation, the UK sanctioned Chen Zhi and associated entities, and the US unsealed an indictment in the Eastern District of New York.[47] Table 1 summarises the principal public actions in the period covered by this report.

Table 1. Selected public enforcement actions against investment-fraud networks, October 2025 to November 2026

Date	Jurisdiction	Action (as described by the source)	Source
14 Oct 2025	United States, United Kingdom	OFAC designates 146 Prince Group targets; FinCEN section 311 final rule against Huione Group; UK sanctions on Chen Zhi and associates, freezing London property; US indictment and civil forfeiture complaint over approx. 127,271 BTC	US Treasury; FinCEN; FCDO; US DOJ
12 Nov 2025	United States	OFAC designates a Burmese armed group and seven companies and individuals linked to scam centres, including the Tai Chang compound	US Treasury
15 Jan – 30 Apr 2026	97 countries and territories	INTERPOL Operation First Light 2026: 5,811 arrests, US$293m intercepted, 31,014 bank accounts blocked, over 142,000 victims identified	INTERPOL
6 Mar 2026	United States	Executive Order 14390, "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens"	US Treasury
17 Apr 2026	Austria, Albania	Action day against Tirana call centres: ten arrests; €891,735 cash, 443 computers and 238 mobile phones seized; losses of at least €50m	Europol

47. US Treasury, sb0278; UK Government (FCDO); US DOJ (all 14 October 2025).

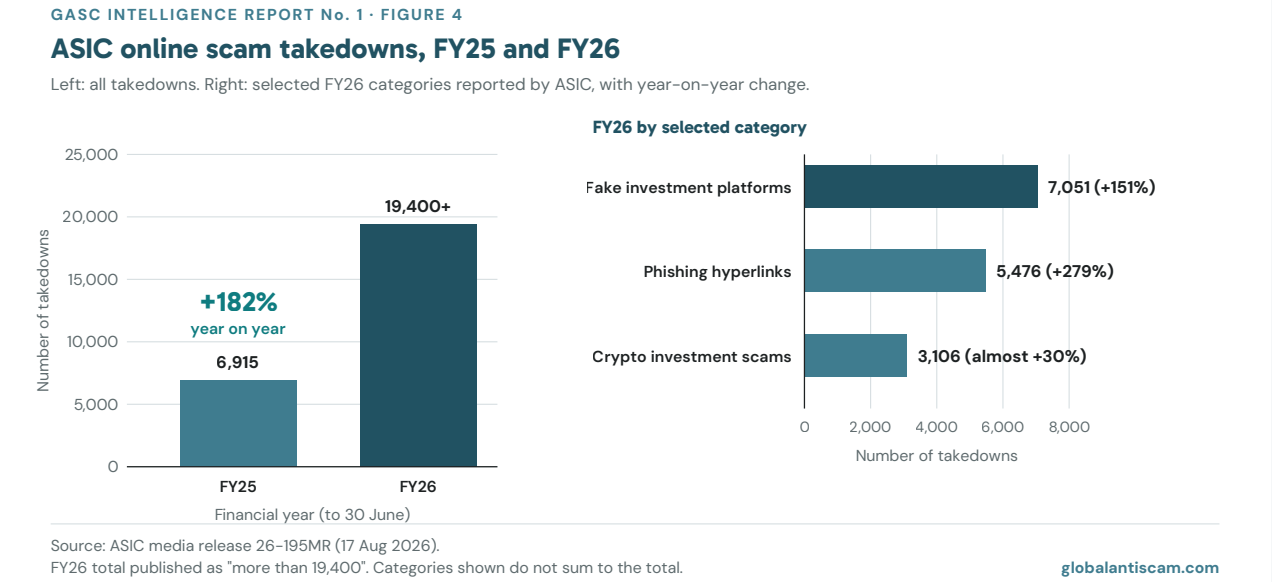
Date	Jurisdiction	Action (as described by the source)	Source
20 Apr 2026 (week)	17 regulators, led by the FCA	Action against illegal finfluencers: FCA issued 34 new alerts and made 120 account takedown requests	FCA
23 Apr 2026	United States	Charges against two Shunda compound managers; 503 fake investment domains seized; more than US$700m in crypto restrained; OFAC designates Cambodian senator Kok An and 28 others	US DOJ; US Treasury
18–21 May 2026	United States, industry partners	"Disruption Week": activity disrupted across more than 1.4 million accounts; over US$3.8m in crypto frozen; seven arrests in Thailand	US DOJ
17 Sep 2026	Australia	NSW District Court sentences a Sydney man to 14 years (non-parole period nine years) for dealing with more than A$50m in investment-scam proceeds	AFP
3 Nov 2026	Seven jurisdictions, with Europol and Eurojust	Action against a suspected crime-as-a-service platform supplier: 100+ servers seized, seven arrests, 17 searches; estimated losses over €4m	Europol

Sources for Table 1 are given in the accompanying notes.[48]

Three features stand out. First, operations are increasingly multinational by design: the Europol case announced in November 2026 involved seven jurisdictions, two joint investigation teams and European Investigation Orders, European Arrest Warrants and freezing orders coordinated through Eurojust.[49] Second, governments are enlisting the private sector. During the US "Disruption Week" in May 2026, industry voluntarily disrupted criminal activity across more than 1.4 million social media and email accounts and froze over US$3.8 million in cryptocurrency.[50] Third, Australia is testing its newer money-laundering laws: the AFP describes the September 2026 sentence as one of the first significant prosecutions under the proceeds-of-general-crime provisions introduced through the 2021 Economic Disruption Act reforms.[51]

48. Table 1 draws on the sources in notes 6, 7, 8, 9, 11, 27, 29, 40 and 50, and on US Department of the Treasury, press release sb0469, "Treasury Sanctions Cambodian Senator Kok An and Scam Center Network Defrauding Americans" (23 April 2026), for the 12 November 2025 designation, Executive Order 14390 and the 23 April 2026 designations. https://home.treasury.gov/news/press-releases/sb0469
49. Europol (3 November 2026).
50. US Department of Justice, Office of Public Affairs, "Scam Center Strike Force Announces Results of U.S. & Private Industry 'Disruption Week'" (3 June 2026). https://www.justice.gov/opa/pr/scam-center-strike-force-announces-results-us-private-industry-disruption-week
51. AFP (18 September 2026).

Figure 4. ASIC online scam takedowns, FY25 and FY26



Takedowns of fake investment platforms rose 151% in FY26; total takedowns rose 182%. *Source: ASIC media release 26-195MR, 17 August 2026.*

5. Investigative and legal challenges

5.1 Jurisdiction and time

Public cases show how long cross-border investigations take. Europol's November 2026 operation followed four years of investigation and earlier action days in 2022 and 2025.[52] The Tirana case began with Austrian victims identified around June 2023 and reached its action day in April 2026.[53] Victim funds, by contrast, are moved quickly. In the Tirana case Europol states that the money "was never invested but was instead channelled into an intricate international money-laundering scheme".[54]

> **"Criminal syndicates exploit human psychology to manipulate their targets, and no nation can stay safe unless all countries are equipped and committed to jointly fighting back."**
>
> **Tomonobu Kaya, Director, INTERPOL Financial Crime and Anti-Corruption Centre**
> INTERPOL news release, 9 July 2026

52. Europol (3 November 2026).
53. Europol (29 April 2026).
54. Europol (29 April 2026).

5.2 Corporate opacity and offshore structures

Shell companies, nominee directors and offshore incorporation slow attribution and asset identification. The UK and US actions against the Prince Group both emphasise offshore vehicles, including British Virgin Islands incorporations.[55] For victims and their advisers, this means identifying who controls an entity can take far longer than establishing that a loss occurred.

5.3 From tracing to recovery

Restraint, forfeiture and return are separate legal stages. The US Scam Center Strike Force reported that more than US$700 million in cryptocurrency had been restrained by April 2026, and stated that it is "working tirelessly to forfeit funds" so that money can be returned "whenever possible".[56] INTERPOL reports US$293 million in illicit assets intercepted during Operation First Light 2026.[57] These are significant outcomes, but the figures are not the same as amounts returned to victims, and they are small relative to the reported losses described in Section 1.

5.4 Secondary victimisation

Recovery fraud targets people who have already lost money. Beyond the Europol case noted above, the NASC links a 170% rise in reported losses to rebate scams in 2025 to "several reports of high value cryptocurrency recovery scams".[58] Any credible response has to warn victims about this risk and avoid creating expectations that cannot be met.

55. UK Government (FCDO) (14 October 2025); US Treasury, sb0278 (14 October 2025).
56. US DOJ (23 April 2026).
57. INTERPOL (9 July 2026).
58. NASC, *Targeting Scams 2025*, PDF p. 38.

6. Implications for victims, lawyers and institutions

Warning signs for victims and institutions

FOR INVESTORS AND FAMILIES

- A new platform trading under the name or licence details of a genuine company that has no website of its own, or whose details do not match the regulator's register.
- Contact through a VoIP or forwarded telephone number, a generic email address or a serviced-office address.
- An unsolicited call after you have filled in an online form, or after you have previously lost money to a scam.
- A sudden handover from a friendly "account manager" to a more senior "trader" or "analyst" after the first deposit, followed by pressure to invest much larger sums.
- Instructions to pay personal accounts or unrelated companies, with account details that change between payments.
- A platform that blocks withdrawals with fees or "taxes", or disappears or rebrands within a few months.

FOR BANKS, PAYMENT FIRMS AND PLATFORMS

- Newly opened personal or business accounts receiving payments from many unrelated individuals, followed by rapid onward transfers.
- Account holders, such as students or people with no business profile, whose activity does not match their circumstances.
- Payments to newly incorporated companies whose names resemble those of established, regulated firms.
- Customers who report a change of "account manager" or who are being urged to top up an investment quickly.

Drawn from the public record and GASC investigator field observations in Sections 2 and 3. No single sign proves fraud.

For victims and families. Older people bear a disproportionate share of reported losses. In the US, complainants aged 60 and over reported US$7.7 billion in losses across all crime types in 2025; in Australia, older Australians make up about 17.1% of the population but account for 26.5% of losses reported to Scamwatch.[59] Early, accurate documentation of payments and communications preserves options. Unsolicited offers to recover money, particularly those requiring an upfront fee, should be treated with extreme caution.

For lawyers and insolvency practitioners. Sanctions designations, section 311 findings, forfeiture complaints and sentencing outcomes are public, citable records that can support pleadings, tracing applications and risk assessments. Advisers should assume that assets have crossed borders, may sit in corporate or digital-asset structures, and may already be subject to competing claims or government restraint.

59. FBI IC3, *2025 Internet Crime Report*, PDF p. 6 (complaint highlights by age group); NASC, *Targeting Scams 2025*, PDF p. 4.

For financial institutions and platforms. Australia's Scams Prevention Framework Act 2025, assented to on 20 February 2025, establishes a framework requiring designated sectors to prevent, detect, disrupt and respond to scams.[60] The FCA's annual results report 222,173 customers removed as money mules across 35 firms, up 4.4%.[61] Both point to growing expectations that intermediaries identify scam flows earlier, not only after a victim reports a loss.

7. Outlook for 2027

The following are GASC's analytic judgements, based on the public record summarised above. They are not forecasts of specific figures.

- **Displacement rather than decline.** Enforcement against compounds in one country is likely to push operators towards other locations, as the Shunda relocation shows.[62]
- **More AI-enabled front ends.** ASIC and the IC3 already report AI-generated endorsements and AI-assisted conversations (Sections 1.1 and 2.1). GASC expects deepfake promotion and AI-assisted scripting to become standard features of investment-fraud marketing.
- **Infrastructure-level disruption.** Takedowns of domains, advertisements and accounts are scaling quickly, as ASIC's FY26 figures and US domain seizures show. GASC expects more public–private disruption exercises, and with them more data on the infrastructure that networks rely on.
- **Sanctions as a financial-crime tool.** The use of sanctions and section 311 measures against scam networks and their facilitators is likely to continue, increasing compliance exposure for institutions that deal, even indirectly, with designated parties.
- **Persistent recovery-fraud risk.** As public awareness of large seizures grows, fraudsters are likely to exploit it, impersonating authorities or "recovery" services to target past victims.

60. *Scams Prevention Framework Act 2025* (Cth), No. 15, 2025, Federal Register of Legislation. https://www.legislation.gov.au/C2025A00015/asmade/2025-02-20/text/original/pdf
61. FCA (9 July 2026).
62. US DOJ (23 April 2026).

8. Methodology and sources

Scope. This report covers international investment fraud: schemes that solicit money for fictitious or misrepresented investment opportunities, including cryptocurrency, foreign-exchange and share-trading schemes, where the offenders, infrastructure or proceeds cross borders.

Sources. We used only primary official publications: annual reports, media releases, sanctions notices, court-related press material and freedom-of-information disclosures from the FBI IC3, the National Anti-Scam Centre (ACCC), ASIC, the AFP, Europol, INTERPOL, the US Department of the Treasury (OFAC and FinCEN), the UK Foreign, Commonwealth & Development Office, the US Department of Justice, the FCA, MAS and the Federal Register of Legislation. Each figure is footnoted to its source.

Table 2. Principal datasets used in this report and what they measure

Source	Coverage	What it measures	Period
FBI IC3, Internet Crime Report	United States	Complaints and losses reported by the public	Calendar years 2023–2025
NASC, Targeting Scams Report	Australia	Combined reports and losses from Scamwatch, ReportCyber, AFCX, IDCARE and ASIC, adjusted for duplication	Calendar years 2024–2025
ASIC media releases	Australia	Takedowns of scam websites, adverts and phishing links	Financial years FY25–FY26
FCA releases and FOI disclosures	United Kingdom	Warning List alerts (not losses)	2024 to August 2026
MAS Investor Alert List	Singapore	Entities possibly perceived as MAS-authorised (qualitative only)	At cut-off
Enforcement releases	International	Case facts and allegations: Europol, INTERPOL, US DOJ, US Treasury, UK FCDO, AFP	Oct 2025 – Nov 2026

Field observations. Sections 2.4 and 3.4 and Figure 2 draw on generalised observations by GASC investigators across multiple investigations. They describe criminal structures only. They contain no client information, no case identifiers and no description of how GASC investigates. Volumes, prices and percentages in these sections are approximate, have not been independently verified and should not be cited as official statistics. Where public cases corroborate an element, the source is footnoted.

Verification. Every official figure and link was checked against the live source on 21 November 2026, which is the data cut-off for this edition. Figures that could not be confirmed against a primary source on that date were excluded. The approximate figures in the field-observation boxes are the only exception, and are labelled as such.

Calculations. Percentage shares in Figure 1 are GASC calculations from the published category and total figures; Australian totals are published to two decimal places, so the shares are approximate. No currency conversion has been applied.

Limitations. Reported losses understate true losses. Datasets use different definitions and collection methods, may double-count, and are revised. Indictments and complaints contain allegations only; defendants are presumed innocent unless proven guilty. Figure 2 is a generalised schematic, not a depiction of any single network or of any GASC matter. The field observations are approximate and are not official statistics. This report contains no client information and no case identifiers.

Glossary

- **Boiler room (front room):** a call centre that cold-calls leads to secure a first deposit.
- **Trade qualifier (TQ):** a front-room caller paid a low base wage plus commission on first deposits.
- **Loader:** a commission-only closer who "loads up" the victim's funds, pressing the victim into ever-larger top-ups after the first deposit.
- **Banker:** a third-party laundering network that moves victim funds through accounts and companies opened in borrowed identities.
- **Lead broker:** a seller of personal-data lists used to target potential victims.
- **Set-up provider:** a supplier of ready-made fraud infrastructure, including company names, domains, websites, email, VoIP numbers and office addresses.
- **Money mule or nominee:** a person whose identity or account is used to receive and pass on illicit funds.

Source list

1. Australian Federal Police, "Man jailed for role in $50 million scam which swindled more than 1000 victims", 18 September 2026. https://afp.gov.au/news-centre/media-release/man-jailed-role-50-million-scam-which-swindled-more-1000-victims
2. Australian Securities and Investments Commission, Media release 26-195MR, "ASIC warns scammers are using AI to spin vast webs of deception", 17 August 2026. https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-195mr-asic-warns-scammers-are-using-ai-to-spin-vast-webs-of-deception
3. Europol, "Call centres dismantled and ten arrested in EUR 50 million online fraud case", 29 April 2026. https://www.europol.europa.eu/media-press/newsroom/news/call-centres-dismantled-and-ten-arrested-in-eur-50-million-online-fraud-case
4. Europol, "Investment scams with potential victims in at least 50 countries: over 100 servers seized", 3 November 2026. https://www.europol.europa.eu/media-press/newsroom/news/investment-scams-potential-victims-in-least-50-countries-over-100-servers-seized
5. Federal Bureau of Investigation, IC3, 2024 Internet Crime Report (2025). https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
6. Federal Bureau of Investigation, IC3, 2025 Internet Crime Report (2026). https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
7. Federal Register of Legislation (Australia), Scams Prevention Framework Act 2025, No. 15, 2025. https://www.legislation.gov.au/C2025A00015/asmade/2025-02-20/text/original/pdf
8. Financial Conduct Authority, "FCA spearheads global action to stop illegal finfluencers", 24 April 2026. https://www.fca.org.uk/news/press-releases/fca-spearheads-global-action-stop-illegal-finfluencers
9. Financial Conduct Authority, "FCA cracks down on illegal promotions and market abuse in first year of new strategy", 9 July 2026. https://www.fca.org.uk/news/press-releases/fca-cracks-down-illegal-promotions-and-market-abuse-first-year-new-strategy
10. Financial Conduct Authority, "Consumers warned to beware of risky mini-bonds and loan notes", 20 August 2026. https://www.fca.org.uk/news/press-releases/consumers-warned-beware-risky-mini-bonds-and-loan-notes
11. Financial Conduct Authority, FOI2026/00006, "Information on crypto-related alerts – February 2026", 20 February 2026. https://www.fca.org.uk/freedom-information/information-crypto-related-alerts-february-2026
12. FinCEN (US Treasury), "FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System", 14 October 2025. https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system

13. INTERPOL, "Over 5,800 arrests, USD 293 million intercepted in global fraud bust", 9 July 2026. https://www.interpol.int/en/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust
14. Monetary Authority of Singapore, Investor Alert List (accessed 21 November 2026). https://www.mas.gov.sg/investor-alert-list/
15. National Anti-Scam Centre (ACCC), Targeting Scams: Report of the National Anti-Scam Centre on scams data and activity 2025, March 2026. https://www.accc.gov.au/system/files/targeting-scams-report-2025.pdf
16. UK Government (FCDO and Home Office), "UK and US take joint action to disrupt major online fraud network", 14 October 2025. https://www.gov.uk/government/news/uk-and-us-take-joint-action-to-disrupt-major-online-fraud-network
17. US Department of Justice, "Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes", 14 October 2025. https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged
18. US Department of Justice, "Scam Center Strike Force Takes Major Actions Against Southeast Asian Scam Centers Targeting Americans", 23 April 2026. https://www.justice.gov/opa/pr/scam-center-strike-force-takes-major-actions-against-southeast-asian-scam-centers-targeting
19. US Department of Justice, "Scam Center Strike Force Announces Results of U.S. & Private Industry 'Disruption Week'", 3 June 2026. https://www.justice.gov/opa/pr/scam-center-strike-force-announces-results-us-private-industry-disruption-week
20. US Department of the Treasury, Press release sb0278, "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia", 14 October 2025. https://home.treasury.gov/news/press-releases/sb0278
21. US Department of the Treasury, Press release sb0469, "Treasury Sanctions Cambodian Senator Kok An and Scam Center Network Defrauding Americans", 23 April 2026. https://home.treasury.gov/news/press-releases/sb0469

9. How to cite this report

Global Anti-Scam Centre (2026). *International Investment Fraud Networks: Financial Flows and Investigative Challenges in 2026*. GASC Intelligence Report No. 1, data cut-off 21 November 2026. Sydney: Global Anti-Scam Centre. https://globalantiscam.com/research/international-investment-fraud-networks-2026/

Media enquiries: info@globalantiscam.com, +61 2 7257 0211.

About GASC. Global Anti-Scam Centre is a private Australian organisation of experienced investigators specialising in investment fraud, digital-asset fraud and cross-border asset tracing. It is based at Level 35, Tower One, 100 Barangaroo Avenue, Barangaroo NSW 2000.

Need an independent view of a suspected investment fraud?

Our experienced investigators provide confidential, evidence-led case assessments. You can **contact our team**, or check a platform before you invest with **GASC Verify**.