Romance Scam Research Center

SOCIAL TECHNOLOGY AND SAFETY FOUNDATION

LIVING EVIDENCE SYNTHESIS

Platform and Law-Enforcement Responses

Platform and Law-Enforcement Responses to Romance-Initiated and Hybrid (Pig-Butchering/Cryptorom) Scams

Reviewed evidence characterizes romance-initiated and pig-butchering/hybrid scams as transnational and operationally complex. Investigations are hindered by anonymity and fake profiles, invalid usernames or IPs, and cases occurring outside investigators’ jurisdictions; traced cryptocurrency flows are difficult to attribute to individuals. On-chain and documentary tracing studies identify exchanges and intermediaries in laundering chains, and report large aggregate exchange deposits (one study reports US$635 million in identified exchange deposits; another estimates at least US$5.6 billion per year from Western exchanges in transactions below $500,000), while explicitly cautioning that these totals cannot all be attributed to scams. Empirical methods in the corpus include DOJ/PACER document searches, court and sentencing analyses, case datasets of victim–scammer conversations, platform report time-series analysis, and combined on-chain and documentary research. Authors note research imbalances and data limitations: sentencing analyses are primarily shaped by legal factors and plea decisions, research is disproportionately focused on victims rather than offender or laundering structures, classification practices can obscure romance-baiting contributions to investment-fraud statistics, and anonymity and cross-border factors make geographic attribution difficult. Recommended priorities supported in the reviewed material include strengthened international police collaboration and joint investigations, development of unified online-fraud legislation with clear offense definitions and sentencing guidance, implementation or testing of platform warning banners when conversations indicate money requests, ongoing revision of fraud taxonomies as hybrid methods evolve, and substantial international cooperation to address cryptocurrency-enabled cross-border scams.

Published Aug 29, 2026 Updated Aug 29, 2026 Synthesis version 33

PUBLICATIONS	EVIDENCE STATEMENTS	CITED SOURCES	SYNTHESIS VERSION
39	246	39	33

Reviewed evidence characterizes romance-initiated and pig-butchering/hybrid scams as transnational and operationally complex. Investigations are hindered by anonymity and fake profiles, invalid usernames or IPs, and cases occurring outside investigators' jurisdictions; traced cryptocurrency flows are difficult to attribute to individuals. On-chain and documentary tracing studies identify exchanges and intermediaries in laundering chains, and report large aggregate exchange deposits (one study reports US$635 million in identified exchange deposits; another estimates at least US$5.6 billion per year from Western exchanges in transactions below $500,000), while explicitly cautioning that these totals cannot all be attributed to scams. Empirical methods in the corpus include DOJ/PACER document searches, court and sentencing analyses, case datasets of victim–scammer conversations, platform report time-series analysis, and combined on-chain and documentary research. Authors note research imbalances and data limitations: sentencing analyses are primarily shaped by legal factors and plea decisions, research is disproportionately focused on victims rather than offender or laundering structures, classification practices can obscure romance-baiting contributions to investment-fraud statistics, and anonymity and cross-border factors make geographic attribution difficult. Recommended priorities supported in the reviewed material include strengthened international police collaboration and joint investigations, development of unified online-fraud legislation with clear offense definitions and sentencing guidance, implementation or testing of platform warning banners when conversations indicate money requests, ongoing revision of fraud taxonomies as hybrid methods evolve, and substantial international cooperation to address cryptocurrency-enabled cross-border scams. [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13]

Scale, modality, and operational features relevant to platforms and policing

Multiple studies and forensic reports describe romance-initiated scams and hybrid romance–investment (pig-butchering/cryptorom) schemes as frequently transnational and organized, using layered roles and overseas infrastructure that complicate detection and enforcement. Case and court-judgment analyses report organized roles, repeated extraction sequences, and continued offending after initial contact in many adjudicated matters. [10] [14] [3] [15] [16] [17]

Fraudsters commonly shift early contacts from dating-site profiles into less-moderated private channels (direct messaging or email) and then rely on local third parties (bank accounts, phone numbers, and accomplices) and cross-border payment rails (overseas remittance services, MoneyGram, and cryptocurrencies) to frustrate tracing and prolong victim extraction sequences. [18] [7] [19] [20]

Qualitative and court-judgment analyses additionally report distributed operational roles (scammers, money-mule and laundering intermediaries, and local agents), persistence of offending despite enforcement contact in some adjudicated cases, and the use of organization-level compartmentalization that limits investigators’ ability to identify leadership from low-level arrests. [15] [21] [22]

Blockchain, financial forensics, and investigative constraints

On-chain forensic methods (address clustering, flow tracing) have produced large aggregate estimates of likely scam-linked crypto inflows and can reveal intermediary exchanges and service providers; authors emphasize that such analyses produce investigative leads but carry attribution uncertainty because seed addresses are incomplete and traced flows may include non-scam activity. [10] [6]

Case-level forensic work combining on-chain tracing with documentary research can identify common intermediaries across geographically distinct flows and produce plausible linkages between cases, but authors repeatedly caution that (a) not all exchange deposits traced can be attributed to scams, (b) incomplete seed-address sets limit exhaustive attribution, and (c) additional off-chain subpoena evidence is frequently needed to confirm account ownership and support prosecutions. [6] [20]

Operational case reports show practical investigative frictions: subpoenas to exchanges may be required but delayed or unanswered, victims may be unable to provide email headers or other sender metadata, and investigators often must coordinate cross-border legal requests to obtain identity and transaction records—requirements that slow attribution and asset-recovery actions. [20]

Law-enforcement practice, capacity, and training

Authors recommend prosecutor and judicial engagement with crypto evidence (for example, prompt subpoenas to exchanges and coordinated on-chain/off-chain analysis) and specialized law-enforcement training and tools to trace and preserve digital evidence, while acknowledging that international legal fragmentation and restricted data access hinder consistent implementation. [20] [23] [14] [4]

Multiple practical recommendations focus on building investigator capacity: specialist training in blockchain and digital forensics, access to forensic tools and link-analysis platforms, and closer operational relationships with financial institutions and platforms to expedite preservation and disclosure of transactional records when legal channels permit. [23] [20] [6]

At the same time, police-practice studies document systemic obstacles that limit enforcement reach: under-resourced central fraud teams, limited mutual-legal-assistance outcomes, corruption and collusion in some contexts, and jurisdictional mismatches that impede timely extradition, subpoena execution, and asset seizure. [24] [11] [25] [26]

Platform governance, detection, and prevention measures

Several platform-focused studies and practice reviews recommend concrete measures that platforms can implement or trial: more prominent in-app warnings when conversations indicate requests for money, stronger identity and address verification, and refinements to automated fake-profile detection combined with human review. [27] [12] [28] [29]

Technical tools could be used by dating and social-media platforms—platforms could use reliable deepfake-detection tools alongside current profile-validation techniques—but operational limits remain: IP- and proxy-based signals can be obscured (e.g., via unregistered proxies or compromised residential hosts), and platform adoption of such detection tools would likely depend on voluntary organizational discretion and goodwill. [30] [28]

Authors repeatedly call for evaluative field trials and transparency: testing warning banners triggered by money-request indicators, assessing the usability and prominence of reporting flows, and publishing intervention evaluations so policymakers and platforms can compare candidate mitigations and scale up approaches that demonstrably reduce victim loss or support investigations. [27] [12] [29] [31]

Legal classification, prosecution, and sentencing evidence

A recurring policy recommendation across reviews and empirical studies is sustained international cooperation: information sharing, harmonized investigative procedures, rapid joint operations, and coordinated legal tools are repeatedly identified as necessary to disrupt cross-border scam rings and facilitate asset recovery. [2] [32] [6] [14] [11]

Reviewed doctrinal and case-record analyses document wide jurisdictional variation in legal classification: many countries lack a specific offence for ‘romance scam’ or catfishing, so prosecutions use general fraud, false-identity, or electronic-information statutes—producing inconsistent classification, investigation pathways, and statistical visibility. [16] [33] [34] [35]

Fraud reporting facilities appear to classify pig-butchering inconsistently as either romance or investment fraud. The ACCC’s practice of classifying romance baiting as investment fraud because losses arise from a false investment likely hides romance-related losses within broader investment-fraud totals and can distort trend interpretation. In Indonesia, existing provisions (commonly Article 378) can be used to prosecute fraud but do not specifically address the offender’s methods or repeat offending, which reduces visibility into those aspects of love-scam cases. [36] [8] [35]

Empirical sentencing research in the United States and judicial-file analyses in several jurisdictions provide limited but concrete findings: a U.S. sentencing memorandum study found formal legal factors strongly influence sentencing and that pleading guilty was associated with reduced imprisonment likelihood in its sample; other country-level convicted-case studies report mostly short median custodial sentences and frequent use of intelligence-driven arrests. [2] [37]

Authors who analyse sentencing consistently note evidence limitations: many studies rely on partial legal records or selective convicted samples, legal documents lack detailed court-level and defendant-background variables, and observed relationships may be correlational—constraints that the authors identify as reasons for cautious interpretation and for further work using richer datasets. [2] [38]

Cross-border coordination, operational practice, and evaluations of coordinated action

A recurring policy recommendation across reviews and empirical studies is sustained international cooperation: information sharing, harmonized investigative procedures, rapid joint operations, and coordinated legal tools are repeatedly identified as necessary to disrupt cross-border scam rings and facilitate asset recovery. [2] [32] [6] [14] [11]

Operational evidence shows both the potential and the limits of coordinated action: multinational police operations can yield arrests, raids, account freezes, and intercepted funds, but overall cross-border investigative activity appears small relative to problem scale because of mutual-legal-assistance frictions, uneven resources, and limited global sanctions tailored to transnational fraud. [11] [6]

Regionally focused research documents offender mobility and practical enforcement barriers: West African studies report migration driven by enforcement pressure and local conditions and call for comparative regional research and strengthened intelligence sharing to improve extradition and joint investigations. [1] [26]

Methodological patterns, limitations, and priority evidence gaps

Reviewed studies used several methods: a dataset of 60 victim–scammer online conversations (50 volunteered via a Facebook research page and 10 via the Royal Malaysia Police CCID); application of the 11P profiling method and Maltego link analysis to map relationships among victims, suspects, transactions, domains, and online entities; analysis of monthly romance-fraud reports known to UK Action Fraud from April 2014 through December 2020; and blockchain/exchange transaction analysis. One paper reports total exchange deposits of US$635 million but cautions that this total cannot all be attributed to scams; another estimates US$5.6 billion per year from Western exchanges in transactions under $500,000 and interprets that figure as a lower bound on funds defrauded from victims using Western exchanges. Authors also note evidence gaps: research is disproportionately focused on victims rather than offender structures, laundering systems, or regulatory effectiveness; available information is insufficient to document all scams or produce a reliable exhaustive list; and three barriers—few arrests of senior leaders, relocation of networks after disruption, and limited mutual legal assistance—constrain accurate evidence about scam-enterprise structures. [5] [6] [7] [20] [9] [10] [21]

Key evidence gaps and recommended future work identified by the authors include: rigorous evaluation of platform interventions (for example, testing warning banners, address-verification methods, algorithmic transparency, algorithmic de-amplification, and real-time scam-detection tools); ongoing revision of fraud taxonomies to capture evolving and hybrid schemes; targeted specialist training and legal education for law-enforcement, prosecutors, and judges in cryptocurrency, digital forensics, and tracing techniques; and documentation of a gap in international legal instruments specifically addressing organised, transnational pig-butchering crypto-investment scams. The literature also documents methodological advances combining on-chain analysis with documentary research to identify exchanges and service providers and demonstrates linked flows through common intermediaries in traced cases. [23] [29] [31] [4] [6] [8] [12]

Authors also call for comparative and multi-jurisdictional empirical work to map offender structures, migration, organized-network roles, and sentencing outcomes; several studies recommend integrating platform data, geographic hot-spot analysis, and court records to improve targeting of prevention and enforcement resources. [39] [11] [38] [15]

References

1. Button, Mark; Lazarus, Suleman; Hock, Branislav; Bugbilla Sabia, James; Pandey, Durgesh; Gilmour, Paul (2025). Factors Influencing Involvement in Cyber-Frauds in West Africa and the Implications for Policy DOI
2. Wang, Fangzhou (2024). A Quantitative Analysis on the Sentencing Disparity in Online Romance Scam Cases in United States: A Focal Concern Theory Perspective DOI
3. Cross, C.; Holt, TJ. (2022). The Use of Military Profiles in Romance Fraud Schemes DOI
4. Ashibly, Ashibly (2025). Paradoks Hukum Rekayasa Sosial Pig Butchering Scam Dalam Investasi Digital Aset Kripto DOI
5. Gujarathi, Palak; Verma, Shankey; Nair, Vipin Vijay (2026). Pig Butchering Scams as Cyber-Enabled Financial Crime: A Scoping Review of Dimensions, Modus Operandi, and Victim-Offender Dynamics DOI
6. Reiter, Jonathan; Team, Bitrace (2024). Connecting Chinese and American Scam Victims DOI
7. Shaari, AH.; Kamaluddin, MR.; Paizi@Fauzi, WF.; Mohd, M. (2019). Online-Dating Romance Scam in Malaysia: An Analysis of Online Conversations between Scammers and Victims DOI
8. Cross, C. (2023). Romance baiting, cryptorom and ‘pig butchering’: an evolutionary step in romance fraud DOI
9. Buil-Gil, D.; Zeng, Y. (2021). Meeting you was a fake: investigating the increase in romance fraud during COVID-19 DOI
10. Griffin, John M.; Mei, Kevin (2024). How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering DOI
11. Button, Mark; Hock, Branislav; Suh, Joon Bae; Koh, Chol Soo (2025). Policing cross-border fraud ‘Above and below the surface’: mapping actions and developing a more effective global response

DOI

12. Wang, Fangzhou; Dickinson, Timothy (2024). Hyperpersonal feedback and online romance fraud: an empirical examination DOI
13. Shapiro, LR. (2022). Online Romance Scammers DOI
14. Krause, David (2025). The Deceptive Allure: Understanding and Combating Cryptocurrency Pig Butchering Scams DOI
15. Lee, Hyejin; Boo, Minseo (2025). Analyzing the Evolving Modus Operandi of Romance Scams via Court Judgments: Crime Script and Policy Implications DOI
16. Grace Carvalho Fernandes, S.; BASTOS DO NASCIMENTO, V.; Castelo Branco Do Nascimento, V. (2023). Romance Scam: Victim Manipulation and Human Trafficking DOI
17. Fu, Zhenglang (2024). Analysis of "Pig-Butchering Scam" Type of Network Fraud from the Legal Perspective DOI
18. Thiel, C. (2020). Love scam in cyberspace DOI
19. Kim, Hyo-shin; Seo, Jun-bae (2019). A Study on Romance Scam : The Current Situation and Effective Countermeasures DOI
20. Botha, Johannes George; Singh, Kreaan; Leenen, Louise (2025). Analysis of a Cryptocurrency Investment Scam: Pig Butchering DOI
21. Luong, Hai Thanh; Ngo, Hieu Minh (2024). Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam’s Perspective DOI
22. Luo, Qiaoyu; Zhao, Yun (2025). Butcher or be butchered: understanding the unwitting recruitment by cybercrime groups in China DOI
23. Lim, A.; Choi, KS. (2025). Modus Operandi and Blockchain Analysis of Romance Scams: Cryptocurrency-Driven Victimization DOI
24. Gillespie, AA. (2017). The Electronic Spanish Prisoner DOI
25. Barnor, J. (2024). The charade of discreetness: Exploring the paradoxical lifestyles of romance fraudsters DOI
26. Lazarus, S.; Button, M.; Garba, KH.; Soares, AB.; Hughes, M. (2025). Strategic business movements? The migration of online romance fraudsters from Nigeria to Ghana DOI
27. Sorell, T.; Whitty, M. (2019). Online romance scams and victimhood DOI

28. Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging DOI
29. Wang, C. (2022). Online Dating Scam Victims Psychological Impact Analysis DOI
30. Suarez-Tangil, Guillermo; Edwards, Matthew; Peersman, Claudia; Stringhini, Gianluca; Rashid, Awais; Whitty, Monica (2019). Automatically Dismantling Online Dating Fraud DOI
31. Ohu, Francis; Jones, Laura (2025). An Examination of Digital Validation-Seeking Behaviors in Adolescents as Precursors to Romance Scamming DOI
32. Sarkar, Gargi; Shukla, Sandeep K. (2024). Bi-Directional Exploitation of Human Trafficking Victims: Both Targets and Perpetrators in Cybercrime DOI
33. Almeida, Paulo Henrique Carvalho; Costa, Sebastião Patrício Mendes da (2025). Catfishing: a conduta de assumir uma identidade falsa nas plataformas de mídia social e suas consequências jurídico-penais DOI
34. Shaqilla, Nikita; Reda, Yahia (2024). Catfishing, Is it Unregulated Crime in Indonesia? DOI
35. Soleha Liliani Malik; Fakhris Lutfianto Hapsoro (2025). Love Scamming in the Digital Era: Legal Protection and Challenges in Handling Love Scam Cases on Dating Applications in Indonesia DOI
36. Whittaker, Jack M.; Lazarus, Suleman; Corcoran, Taidgh (2024). Are fraud victims nothing more than animals? Critiquing the propagation of “pig butchering” (Sha Zhu Pan, □□□) DOI
37. Soares, Adebayo Benedict; Lazarus, Suleman; Button, Mark (2025). Love, Lies, and Larceny: One Hundred Convicted Case Files of Cybercriminals with Eighty Involving Online Romance Fraud DOI
38. Soares, Adebayo Benedict; Lazarus, Suleman (2024). Examining fifty cases of convicted online romance fraud offenders DOI
39. Sinclair, R.; Bland, M.; Savage, B. (2023). Dating hot spot to fraud hot spot: Targeting the social characteristics of romance fraud victims in England and Wales DOI

This AI-assisted synthesis is based on reviewed evidence records. It may contain errors or omissions. Follow the publication and DOI links, consult the original works, and make your own judgment about the evidence.

About this document

This living evidence synthesis was produced through AI-assisted analysis of approved RSRC publications. Claims are linked to supporting evidence and checked for source consistency. It may change as the corpus is updated. Readers should consult the cited publications when making research, policy, or practice decisions.

Current web version: https://romancescamresearch.org/research-insights/platform-and-law-enforcement-responses-to-platform-enabled-romance-scams-an-evidence-synthesis