



**FRAUD
SHIELD** TM

Confidential Redacted Report

ENHANCED INVESTMENT OPPORTUNITY INVESTIGATION REPORT

This sample report has been prepared to demonstrate the type of intelligence-led insight IYE Fraud Shield can provide to organisations operating in high-risk financial, transactional, and counterparty environments.

It is intended to show how Fraud Shield looks beyond standard compliance checks by assessing behavioural risk, corporate exposure, associated networks, adverse indicators, and potential red flags that may not be identified through conventional KYC, due diligence, or investigative processes.



**FRAUD
SHIELD**™

CONFIDENTIAL – REDACTED SAMPLE REPORT

IYE GLOBAL Ltd

ENHANCED INVESTMENT OPPORTUNITY INVESTIGATION REPORT

Reference: IYE/INV/REDACTED/0005348/26

CLIENT: [REDACTED]
DATE: 22 May 2026
SUBJECT: Investigation into a proposed international investment and private banking opportunity
CLASSIFICATION: Strictly Confidential - Client Use Only

1. EXECUTIVE SUMMARY

IYE IS instructed by the Client to conduct a comprehensive enhanced due diligence (EDD) and forensic intelligence investigation into an investment opportunity presented by several individuals claiming to represent an international private investment consortium. Allegedly operating within the field of structured finance, private banking instruments, cryptocurrency liquidity management, and commodity-backed investment products IYE was commissioned to assess the veracity of the opportunity.

The proposed transaction involved an alleged low-risk investment programme offering unusually high returns generated through private banking facilities, offshore investment structures, and institutional-grade monetisation arrangements. The Client was advised that participation in the programme required an initial capital contribution together with substantial “compliance”, “insurance”, and “banking release” payments prior to activation of the investment.

The investigation conducted by IYE included extensive review of the individuals involved, their associated companies, the banking institutions referenced, transactional documentation, corporate structures, financial routing arrangements, adverse intelligence indicators, litigation exposure, money laundering risk, sanctions exposure, travel patterns, digital infrastructure, and comparative analysis against known international fraud typologies. The review incorporated enhanced screening parameters ordinarily reserved for high-risk financial crime investigations,



**FRAUD
SHIELD**™

including criminality indicators, financial regulator warnings, reputational review, corporate verification, intelligence risk assessment, sanctions screening, money laundering exposure analysis, and wider network association checks.

The findings of this investigation are conclusive and highly concerning.

IYE assesses with a high degree of confidence that the investment opportunity presented to the Client forms part of a sophisticated international fraud operation utilising fabricated investment structures, cloned corporate identities, false banking representations, and layered financial-routing arrangements intended to unlawfully obtain funds from investors under false pretences.

The investigation identified extensive indicators of organised criminality, including links to previously reported investment scams. The use of recycled criminally used contractual documentation and suspicious offshore corporate networks, including laundering pathways involving cryptocurrency conversion, and transactional structures consistent with international advance-fee and investment fraud methodologies caused significant further concern.

IYE firmly recommends that the Client should not proceed with the proposed investment under any circumstances.

2. BACKGROUND

The Client was approached through an intermediary identifying himself as [REDACTED], purportedly operating on behalf of an international investment facilitation group connected to:

- Helvetic Strategic Capital
- Crown International Monetisation Partners
- Blackwater Asset Recovery & Finance

The opportunity was presented as an exclusive institutional programme involving private banking instruments, over-the-counter cryptocurrency liquidity management, and commodity-backed trade financing.



The Client was informed that:

- guaranteed monthly returns of between 12% and 18% were achievable;
- the investment was secured by “Tier 1 banking protection”;
- and a European banking institution had already approved the transaction;
- investor funds would remain “fully protected”;
- the opportunity was only available to a small number of selected investors;
- substantial profits could be generated within 90 days.

The Client was further advised that advance payments were required to cover compliance clearance, anti-money laundering certification, legalisation costs, transaction insurance, and “bank instrument activation fees”.

3. INVESTIGATION METHODOLOGY

IYE undertook a multi-layered forensic and intelligence investigation into the transaction and associated parties.

The review included:

- Identity and corporate verification
- Enhanced adverse media analysis
- Financial crime intelligence review
- International regulatory and sanctions screening
- Review of litigation and insolvency exposure
- Analysis of travel patterns and offshore affiliations
- Verification of banking institutions and account structures
- Digital footprint and infrastructure analysis
- Cryptocurrency wallet tracing
- Contractual comparison against known scam documentation
- Social media and communication profiling
- Corporate beneficial ownership analysis
- Money laundering risk assessment
- Open-source intelligence collection
- Comparative fraud typology assessment.



**FRAUD
SHIELD**™

The companies involved in presenting the opportunity displayed numerous indicators associated with fraudulent or deceptive trading structures.

Although the entities maintained professional websites and produced apparently sophisticated documentation, forensic examination revealed that the majority of the corporate infrastructure had been created within a relatively short period prior to approaching investors.

The investigation identified:

- Virtual office facilities used as registered addresses
- Hidden domain registration data
- Fabricated trading histories
- Unverifiable licensing claims
- Cloned regulatory wording copied from legitimate financial institutions
- Inconsistencies in incorporation records
- Absence of legitimate audited financial information.

One of the principal entities claimed to operate banking relationships with:

- HSBC Holdings plc
- UBS Group AG
- JPMorgan Chase & Co.

However, IYE identified no evidence that any formal institutional relationship existed with the entities presenting the opportunity.

Documentation purporting to show banking support contained numerous inconsistencies including invalid formatting, incorrect institutional terminology, manipulated signatures, and non-verifiable SWIFT references. All documents were missing hidden bank security protocols and indicators.



**FRAUD
SHIELD**™

Individuals Presenting the Opportunity

The principal individuals involved in the transaction appear to have used carefully constructed professional identities designed to create legitimacy and trust.

The investigation established that several of the biographies supplied to investors contained false or exaggerated employment histories, including fabricated claims of prior association with major international banks and investment houses.

Multiple profile photographs used in presentations and digital communications were identified as either stock images or previously used in unrelated online profiles.

One individual operating under the name [REDACTED] was linked through digital intelligence analysis to prior investment propositions involving:

- Cryptocurrency arbitrage schemes
- Fake gold-backed investment programmes
- False bank guarantee transactions
- Advance-fee trade finance frauds

IYE additionally identified communication overlaps, shared document templates, and identical contractual clauses previously observed in separate investment scam investigations involving entities operating from:

- Cyprus
- Turkey
- United Arab Emirates
- Hong Kong
- Georgia



**FRAUD
SHIELD**™

Contractual and Documentation Analysis

A detailed forensic comparison of the contractual documentation identified significant evidence that the paperwork had been adapted from templates previously associated with unrelated fraudulent investment schemes. Several clauses, formatting styles, indemnity provisions, and confidentiality wording matched documentation previously reviewed by IYE in investigations involving fraudulent cryptocurrency investment operations and private-placement frauds.

The agreements contained provisions specifically designed to:

- Discourage independent verification
- Prevent direct bank-to-bank communication
- Create artificial urgency
- Shield organisers from liability and/or identification
- Justify repeated advance-fee requests

The legal opinions supplied to investors appeared to have been fabricated. The law firms referenced either did not exist or denied involvement when independently approached.

Money Laundering and Financial Routing Assessment

The investigation identified serious concerns regarding the proposed movement of investor funds. Rather than directing funds into regulated investment structures, investors were instructed to transfer monies through layered intermediary accounts located in multiple jurisdictions, including:

- Lithuania
- Estonia
- Singapore
- United Arab Emirates



The transactional structure displayed characteristics strongly associated with laundering methodologies, including:

- Rapid onward transfers
- Use of payment processors
- Conversion into cryptocurrency assets
- Use of decentralised exchanges
- Splitting of funds across multiple jurisdictions
- Layering through shell companies

IYE's cryptocurrency tracing review identified wallet interactions connected to addresses previously referenced within intelligence reports relating to investment fraud and cyber-enabled financial crime. The overall routing structure appears deliberately engineered to frustrate recovery efforts and obscure beneficial recipients.

Links to Previous Scam Activity

The investigation established substantial overlap between the present opportunity and previously identified fraud operations.

IYE identified intelligence suggesting that certain individuals connected to the transaction may have participated in prior schemes targeting investors in the United Kingdom, Germany, the Netherlands, Singapore, and the United Arab Emirates.

Several associated entities were also found to have appeared in adverse media and regulatory intelligence relating to high-yield investment frauds and false banking instrument schemes.

Intelligence Risk Assessment

The intelligence risk associated with this investment opportunity is assessed as **EXTREME**.



The transaction structure, behaviour of the participants, banking inconsistencies, contractual manipulation, and financial-routing arrangements collectively demonstrate a pattern fully consistent with organised international investment fraud.

No credible evidence was identified to support the legitimacy of the opportunity.

Conversely, the investigation identified overwhelming evidence of deception, concealment, financial crime exposure, and deliberate misrepresentation.

4. CONCLUSION

Following extensive investigation, IYE concludes that the investment opportunity presented to the Client is fraudulent.

The opportunity displays all key indicators associated with sophisticated international advance-fee investment fraud and private banking scam activity. The evidence strongly suggests that the individuals involved are operating within a coordinated network utilising false corporate legitimacy, fabricated banking support, manipulated legal documentation, and layered money laundering structures to obtain investor funds unlawfully.

The proposed investment should be regarded as a serious financial and reputational threat to the Client.

5. RECOMMENDATION

IYE makes the following firm recommendation:

The Client should not proceed with the proposed investment under any circumstances. No funds should be transferred, no additional documentation should be signed, and all communications and evidential material should be preserved.



**FRAUD
SHIELD**™

Consideration should additionally be given to:

- Notifying relevant banking institutions
- Preparing necessary reports for law-enforcement and intelligence agencies
- Preserving digital evidence

Prepared by:

IYE Investigation Team 1

IYE Global Ltd

20-22 Wenlock Road, London N1 7GU United Kingdom | +44 (0)20 7112 8807