FRAUD SHIELD™

# Confidential Redacted Report

## FORENSIC SBLC VERIFICATION & FRAUD ANALYSIS 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.

## CONFIDENTIAL – REDACTED SAMPLE REPORT

IYE GLOBAL Ltd
FORENSIC SBLC VERIFICATION & FRAUD ANALYSIS REPORT
Reference: IYE/SBLC/005237 /2025 /REDACTED

**CLIENT NAME:** REDACTED
**DATE:** 22 February 2025
**SUBJECT:** Verification and Intelligence Assessment relating to a purported Standby Letter of Credit ("SBLC") valued at USD 75,000,000.00
CLASSIFICATION: STRICTLY CONFIDENTIAL – CLIENT USE ONLY

# 1. EXECUTIVE SUMMARY

IYE Global is instructed to conduct a forensic verification and intelligence-led due diligence investigation concerning a purported Standby Letter of Credit ("SBLC") presented to the Client as part of an international investment and trade finance opportunity.

The Client had been approached by individuals claiming to represent a private investment consortium offering access to "high-yield structured banking instruments" backed by a major European banking institution. The investment proposal required the Client to provide an advance "compliance and monetisation facilitation fee" totalling approximately USD 2.8 million prior to release of the purported banking instrument. Certain funds have been released prior to IYE being commissioned.

Following detailed analysis, IYE concludes that the SBLC provided to the Client was fraudulent and formed part of a wider organised advance-fee fraud operation commonly associated with international trade finance scams targeting high-net-worth investors and corporate entities.

The investigation identified multiple indicators of criminal deception, including forged banking identifiers, falsified SWIFT references, fabricated legal opinions, cloned corporate identities, and the use of offshore shell entities linked to known financial crime typologies.

The evidence strongly supports the conclusion that the parties involved intended to unlawfully obtain funds from the Client under false pretences without any legitimate banking instrument existing.

## 2. BACKGROUND

The Client was introduced to the transaction through an intermediary identifying himself as:
“Michael DeLuca”
(assessed to be an alias)

The individual claimed to represent an international financial facilitation group operating from Deluca Strategic Holdings / European Capital Monetisation Group.

The proposal outlined an opportunity to participate in a “bank instrument monetisation programme” allegedly supported by a top-25 global bank.

The Client was informed that:

The SBLC had already been issued and that instrument was “cash-backed” offering immediate returns of between 300%–500% through “private placement monetisation”. Funds were urgently required to release the instrument from compliance restriction.

Some funds were transferred, however the Client subsequently instructed IYE to independently verify the legitimacy of the transaction and associated parties before transferring additional funds.

# 3. DOCUMENTS REVIEWED

IYE reviewed the following material:

- Purported SBLC documentation
- SWIFT MT799 and MT760 copies
- Legal opinion letters
- Corporate registration certificates
- Passport and identification material
- Banking correspondence
- WhatsApp and encrypted messaging communications
- Wire transfer instructions
- Compliance invoices
- Broker agreements
- Non-disclosure agreements
- Video conference recordings
- Digital metadata associated with supplied PDF files

# 4. KEY FINDINGS

## 4.1 The SBLC presented was a Fraudulent Banking Instrument.

The SBLC presented to the Client contained numerous errors inconsistent with legitimate banking practice, including:

- Incorrect SWIFT formatting
- Invalid authentication references
- Non-compliant ICC wording
- Inconsistent issuing bank terminology
- Formatting errors inconsistent with genuine bank-generated instruments
- Electronic signatures incapable of validation
- Incorrect Officer designations
- Fabricated instrument registration references
- Lack of embedded security indicators

Independent verification established that the alleged issuing bank had no record of the instrument and the purported “bank officer” named within the documentation could not be identified as an employee of the institution.

## 4.2 Use of Typical Advance Fee Fraud Methodology

The investigation identified a classic organised SBLC advance-fee fraud structure involving:

- Initial presentation of high-value banking instruments
- Use of urgency and confidentiality
- Claims of elite banking access
- Requests for repeated “compliance” and “release” fees
- Escalating demands for additional payments
- Use of offshore accounts and cryptocurrency wallets
- Attempts to avoid direct bank-to-bank verification
- This methodology closely mirrors known international trade finance fraud typologies investigated by multiple law enforcement agencies worldwide.

## 4.3 False Corporate Identities

The entities used in the transaction demonstrated characteristics consistent with cloned or fabricated corporate structures.

- Indicators included:
- Virtual office addresses
- Recently incorporated entities
- Nominee directors
- Lack of verifiable trading activity
- No regulatory permissions
- Contradictory corporate histories
- Websites created within the preceding 12 months
- Generic AI-generated marketing content
- Hidden domain ownership

The investigation further identified links between associated email infrastructure and prior fraud complaints involving purported cryptocurrency investment platforms and commodity trading schemes.

### 4.4 Intelligence & Adverse Findings

IYE conducted a broader intelligence-led assessment which included:

- adverse media checks
- sanctions screening
- politically exposed person screening
- corporate structure analysis
- litigation searches
- financial crime intelligence review
- social media and digital footprint analysis
- offshore financial profiling
- travel pattern assessment
- international regulatory warning searches

The assessment identified links between persons associated with the transaction and entities previously referenced in:

- financial regulator warning notices
- boiler room investment operations
- cryptocurrency fraud intelligence packages
- prior failed trade finance schemes

One associated intermediary was identified as having historical links to criminal entities operating from:

- United Arab Emirates
- Turkey
- Cyprus
- Hong Kong

These jurisdictions are commonly observed within layered international financial fraud structures involving shell entities and rapid movement of funds.

## 5. FINANCIAL ANALYSIS

The banking instructions supplied to the Client directed funds through a series of intermediary accounts held in:

- Lithuania
- Georgia
- Singapore

The account structures displayed characteristics commonly associated with laundering typologies, including:

- rapid pass-through transactions
- unrelated beneficiary entities
- layered transfers
- use of payment processors
- conversion into cryptocurrency assets
- onward transfers to decentralised exchanges

The transaction trail indicates that the fraud network was likely operating internationally using compartmentalised actors fulfilling separate roles including:

- introducers
- document fabricators
- compliance impersonators
- account facilitators
- crypto off-ramp operators

## 6. ASSESSMENT OF CRIMINALITY

Based upon the totality of evidence reviewed, IYE assesses with a high degree of confidence that:

The SBLC instrument was fraudulent and that the transaction was part of an organised advance-fee fraud conspiracy with multiple individuals involved knowingly participating in deceptive conduct. The objective of the scheme was the unlawful extraction of funds from the Client and there is substantial evidence suggesting wider international criminal involvement.
The transaction presents a substantial financial and reputational risk to the Client.

## 8. RECOMMENDED ACTIONS

IYE recommended the following immediate actions:

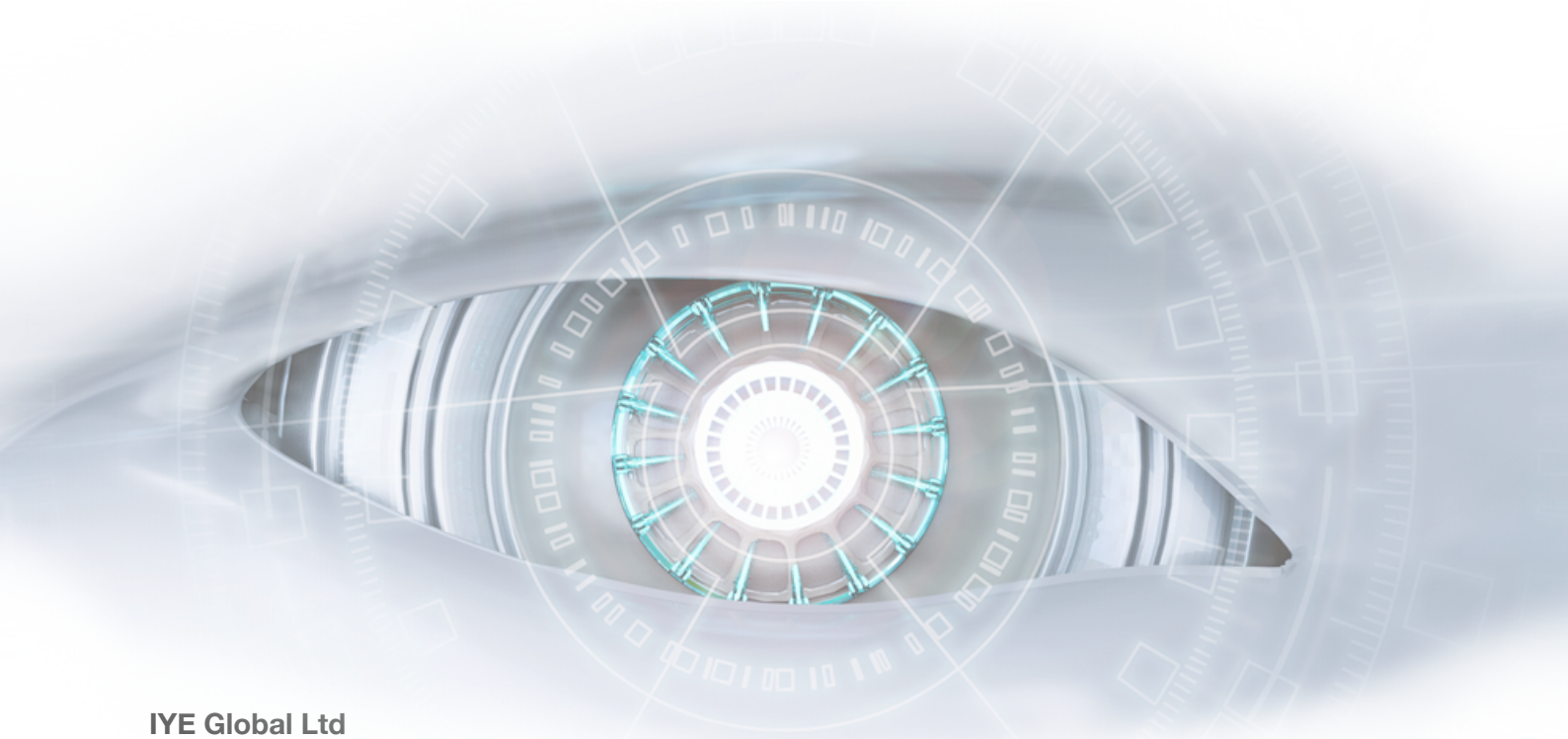
- Immediate suspension of all payments
- Preservation of communications and digital evidence
- Banking intervention requests
- Asset tracing procedures
- Cryptocurrency wallet analysis
- Regulatory intelligence submissions
- Law enforcement referral preparation
- Civil recovery assessment
- Identification of additional victims
- Multi-jurisdictional intelligence coordination

## 9. CONCLUSION

The investigation identified overwhelming evidence that the purported SBLC transaction was fraudulent and formed part of a sophisticated organised financial crime operation designed to exploit investor confidence through fabricated trade finance instruments. The structure, methodology, documentation, and participant behaviour observed throughout the investigation are fully consistent with known international SBLC and bank instrument fraud typologies. Certain individuals and associates identified during the course of the investigation have been evidenced as having involvement in various criminal activities in the past, some of which are presently under investigation.

The matter should be treated as a serious cross-border financial crime investigation requiring immediate containment and coordinated recovery efforts.

Prepared by:
**IYE Investigation Team 1**



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