



THE FINANCIAL INTELLIGENCE UNIT

3rd Floor Norfolk House
P. O. Box SB-50086
Telephone: (242) 356-6327 or 356-9808
Email: director.fiu@fiubahamas.bs

Frederick Street
Nassau, The Bahamas
Fax: (242) 322-5551

FRAUD TYPOLOGY: POTENTIAL CYBER FRAUD AND MONEY LAUNDERING SCHEME

SUMMARY

On 15th May 2023, the Financial Intelligence Unit received a Suspicious Transaction Report (STR) from Brickell Law, a legal institution located in The Bahamas, informing that it was contacted via email by an individual and potential client named Sue Lang, who purported to represent Liberty Systems, a company based in the Philippines. Lang sought the firm's assistance in drafting a sales agreement between an entity in The Bahamas and Liberty Systems. However, numerous red flags emerged during the course of the interaction, including inconsistencies in documentation, questionable email addresses, and an unusual payment method.

KEY INDICATORS OF FRAUD

1. Use of Fraudulent or Misleading Identities:

- Sue Lang claimed to be a director of Liberty Systems, but external research on official sources contradicted this claim.
- Documents provided, such as the board of directors list, contained discrepancies when compared to open-source records.

2. Suspicious Communication Methods:

- Lang did not disclose how she discovered Brickell Law, which raises concerns about unsolicited phishing attempts.
- Multiple inconsistencies were identified in email addresses used by Lang and other associated parties, including slight variations in domain names (e.g., @libertygg.com vs. the legitimate @liberty.com).
- A domain search revealed that @libertygg.com was newly registered, suggesting a potential fraudulent setup.

3. Unusual Payment Method and Transaction Structuring:

- A bank draft worth USD \$200,000 was sent via courier instead of the industry-standard wire transfer or escrow agreement.
- The cover letter accompanying the bank draft was co-signed by Horace Johnson of Varrow View Brokerage, a party unrelated to the transaction.

- The cover letter contained inconsistencies in email addresses, further casting doubt on its authenticity.
 - The involvement of a large sum of money without clear transaction legitimacy suggests possible layering techniques in money laundering.
4. **Document Irregularities:**
- Typo's and formatting errors were present in official documents, which is unusual for a transaction of this scale.
 - The letter of instructions and board of directors list contained inaccuracies inconsistent with verified sources.
 - Open-source research revealed discrepancies between the provided board of directors list and official records.
5. **Potential Use of Fake or Counterfeit Financial Instruments:**
- The bank draft was sent by courier rather than through direct bank communication, which is a red flag for check fraud.
 - There was no verification of the draft's authenticity or whether the funds were backed by a legitimate financial institution.
-

POSSIBLE FRAUD TYPOLOGIES

1. **Business Email Compromise (BEC) or Phishing Scheme:**
- Fraudsters often create lookalike email addresses to deceive firms into facilitating fraudulent transactions.
 - The newly registered domain suggests an attempt to impersonate Liberty Systems.
2. **Advance Fee Fraud:**
- The fraudulent bank draft could have been an attempt to convince Brickell Law to release funds before discovering the check was invalid.
3. **Money Laundering via Legal Services:**
- Fraudsters may have attempted to use Brickell Law as an intermediary to legitimize illicit funds by integrating them into a legitimate transaction.
4. **Check Fraud:**
- The suspicious nature of the bank draft, combined with the lack of direct banking interaction, suggests possible counterfeit check activity.
-

OUTCOME AND RECOMMENDED ACTIONS FOR PREVENTION

All relevant intelligence and documents obtained by the FIU were forwarded to Law Enforcement Authorities. A Spontaneous Disclosure was also forwarded to the Jurisdiction associated with Sue Lang.

RECOMMENDATIONS FOR POTENTIAL FRAUD & MONEY LAUNDERING

- 1. Transaction Monitoring and Reporting:**
 - Flag and report suspicious activity or transactions to the Financial Intelligence Units (FIU) or other relevant regulatory bodies.
- 2. Enhanced Due Diligence (EDD):**
 - Verify all parties involved in transactions using open-source intelligence, official business registries, and third-party verification services.
 - Confirm client identities through direct communication with official company representatives.
- 3. Document Authentication and Verification:**
 - Cross-check board of directors lists with regulatory filings and company databases.
- 4. Cybersecurity Measures:**
 - Implement stricter email verification protocols to detect phishing attempts.
 - Train employees on common red flags associated with email spoofing and business email compromise.