Digital Asset Fraud from Breach to Recovery

Action Plan Checklist

WeirFoulds LLP

BDO

STEVENS & BOLTON

1. Detection of Digital Assets-Based Fraud and Securing Remaining Assets

✓ Determine the nature of the breach, loss, data compromised, amounts at stake and obtain urgent expert input on the technical cause.

- Evaluate potential internal breaches (e.g., employees or service providers) as a possible source of compromise.
- Review external services (e.g., cloud wallets, custodians) for any vulnerabilities that may have contributed to the breach.

✓ Identify risks of ongoing loss that needs to be remediated and steps to halt ongoing dissipation (i.e., unresolved cybersecurity breach; unresolved access to digital wallets; or compromised accounts/wallet addresses).

- Specify the use of multi-signature wallets or more advanced cryptographic tools to secure remaining assets.

✓ Secure and preserve remaining assets (i.e., transfer digital assets to secure off-chain wallet or insured custodian).

- Initiate real-time system monitoring to promptly detect any unauthorized access or suspicious transactions.

2. Immediate Assessment of the Client's Loss, Possible Routes for Recovery and Confidential Notifications to Third Parties

✓ Assess and map the flow of funds to identify potential target accounts or wallets, including the transaction network and associated wallet addresses, where available.

✓ Consider immediate risk of dissipation and urgent notice to intermediaries (i,e., confidential soft notices, draft orders, or subpoenas to banks, exchanges and other affected parties).

✓ Consider flagging and actively monitor transactions and wallet addresses on blockchain, where applicable.

3. Initiate Internal Investigation to Protect Interests and Support Recovery Efforts

✓ Evaluate internal systems, protocols and procedures of client for immediate risks, vulnerabilities and consider urgent stop-gap measures.

✓ Consider notices to customers or other affected parties, where appropriate.

✓ Implement Litigation Hold and preserve client data and records for future use.

✓ Initiate an internal investigation and fact finding with the legal team.

4. Evaluation of Tracing Options and Available Court Remedies

✓ Liaise with team of international lawyers to determine the most appropriate jurisdiction for court recovery, based on available information on bad actor(s) residency and intermediary offices and asset holdings as well as jurisdiction enforcement options.

✓ Assess urgent, without notice injunctive relief options against bad actor(s) and third party intermediaries, including asset freezing and third party disclosure orders.

✓ Assess urgent, without notice injunctive options to seize evidence (i.e., Anton Pillers seizing hardware and data relevant to the attack and loss).

5. Engagement of Consultants and Experts to Reduce Risk, Build Case and Help in Tracing and Recovery of Digital Assets

✓ Consider engagement of asset tracing and business intelligence investigators to follow any available leads (i.e., background checks, Open Source Intelligence (OSINT), dark web searches; confidential sources; surveillance).

✓ Consider engagement of digital asset forensic consultants to assist in the following:

- Acquiring, processing, analysing, and reporting on data stored electronically.
- Tracing transactions on the blockchain and utilize multiple blockchain analytics tools (e.g., TRM, Chainalysis, Elliptic, Arkham, and others) including OSINT platforms to assess involved parties or intermediaries.
    - Following the path of cryptocurrency transactions from one address to another.
    - Identifying the origin and destination of funds.
    - Mapping out the transaction network and relevant wallet addresses.
- Determine the bad actor(s) wallet attribution.
    - Group related wallet addresses that are likely controlled by the same entity.
    - Attempt to link wallet addresses to an entity or individual.
    - Obtain leads that are essential for legal proceedings and asset recovery.
- Engage financial transaction specialists in digital asset to assess money laundering activities.

6. Consider Engagement of Law Enforcement/Government and Whether it Can Help Support the Client's Interests

✓ Determine if a crime or regulatory breach has been committed and reporting obligations (and in which jurisdiction).

✓ Consider cross-border issues and questions of government/agency jurisdiction/local counsel.

✓ Assess with client how their interests and goals align or conflict with law enforcement/government agency interests.

✓ Collaborate with Virtual Asset Service Providers (VASPs) if stolen funds are traced to their platforms.

7. Consider Regulator Interests and How that Impacts Risk Assessments and Action Plans

✓ Consider regulatory environment of client, bad actor and intermediaries and applicable regulatory rules and guidelines, and reporting obligations.

✓ Consider applicable reputational considerations for all possibly involved parties.

8. Consider Other Routes to Recovery if Claims Against Bad Actors Fail and Recovery Proves Impossible – Are There Viable Claims Against Third Parties and in Which Jurisdiction?

Presenters

Javier Alvarez
Managing Director
Forensics Digital Assets Leader at BDO

Benjamin Bathgate
Partner, Chair
Commercial Litigation and Digital Asset Investigations, WeirFoulds LLP (Canada)

Sarah Murray
Head of Commercial Litigation
Stevens & Bolton LLP (UK)

Scan the QR codes to follow us on LinkedIn