The Block Audit LLC
info@theblockaudit.com
(954) 698-2700
1931 Cordova Rd #2053
Fort Lauderdale, FL 33316

August 23, 2026

TRIAGE LETTER

SAMPLE FOR ILLUSTRATION

This is a sample of The Block Audit's triage letter deliverable. Every name, address, wallet, transaction, amount, and service provider in it is fictional and appears for illustration only. An actual triage letter is prepared from the transactions reported in your matter and is delivered confidentially.

RE: Sample Customer Request (Fictional)

1. Scope of Engagement

The Block Audit, LLC is a cryptocurrency forensic analysis firm specializing in blockchain investigations, asset tracing, and expert witness services for law enforcement, financial institutions, and professional services clients.

The Block Audit was engaged by First Bank of Sample, a fictional institution, on behalf of an affected customer to conduct a triage assessment of virtual asset transactions reported as fraud or theft resulting from a Business Email Compromise scam. The information detailed in Section 2 below was provided as the starting point of the analysis.

This triage letter is an exposure assessment intended to identify off-ramps where the victim's assets may have arrived at Virtual Asset Service Providers (VASPs) so that immediate action can be taken to prevent further loss and identified VASPs can apply voluntary risk mitigation measures based on their own internal policies. Unless designated below as a Direct Attribution finding, the tracing reflected in this letter identifies general asset flows and exposure points, not the level of precision required for forensic attribution of specific funds to victim losses; detailed forensic-grade tracing for those destinations will be performed at the request of law enforcement to support legal process.

2. Information Provided

T1	Date	03/12/26	Amount	1.8402	Asset	BTC
	Receiving Address	bc1qsm2v7e4x9wq3t8u6r5n0hczv4dfk2m9waeud7c				
	Transaction Hash	facade01a6c34d9e0b7f24c81d5a9e36f0c2b48d17e5a03c96b1d84f27e60a53				

T2	Date	03/13/26	Amount	0.9617	Asset	BTC
	Receiving Address	bc1qsm2v7e4x9wq3t8u6r5n0hczv4dfk2m9waeud7c				
	Transaction Hash	facade02d94e17b60c3f85a2e9d40b7c16f38a5d02e9c74b81f5d36a90e21c47				

3. Findings

The Block Audit's preliminary analysis produced the following outcomes for the transactions described in Section 2:

☐ **Direct Attribution**
Specific assets traced to identified VASP destinations at a forensic-level standard.

☐ **Effectively Obfuscated**
Advanced techniques or services obscured the flow of funds; recovery is not feasible.

☐ **Basic Trace**
Asset flow identified to known VASPs; standard-complexity follow-on analysis required to support legal action.

☒ **Advanced Trace**
Asset flow identified to known VASPs; advanced-complexity follow-on analysis required to support legal action.

☐ **Wallet Monitoring**
Assets remain on chain in identified wallets; ongoing monitoring required to resume the trace.

Outcome 1: Advanced Trace

ANALYST NOTES

Our initial assessment followed the target assets through numerous hops with intentional obfuscation techniques employed by the bad actor, including the use of a cross-chain bridging service to move BTC assets to USDT on the Tron network. The contents of this triage are for exposure analysis only. A tracing of specific assets would require the application of accounting methods and detailed documentation to support these findings.

4. Next Steps

While Virtual Asset Service Providers may, at their discretion, take action to guard against the laundering of criminal proceeds or the dispensation of victim assets based on the contents of this letter, law enforcement is the only entity with the legal authority to request records, freeze accounts, and seize funds from virtual asset service providers and associated entities. Any law enforcement agency taking action on the matters covered in this triage is entitled to a complimentary thirty-minute consultation with The Block Audit to review the findings and discuss appropriate next steps. Timely coordination is critical, as digital assets can move rapidly or become further obfuscated.

The exposure points identified below under Advanced Trace are sufficient to support voluntary VASP action based on each provider's risk policies. To support legal process against these destinations, contact The Block Audit to engage an Advanced Trace follow-on for forensic-grade documentation.

5. Follow-Up Actions

Advanced Trace Exposure Points

Each exposure point below identifies a Virtual Asset Service Provider with potential exposure to victim funds. May support voluntary VASP action; legal process requires follow-on forensic engagement.

VASP: Northgate Digital Ltd (fictional)

Legal address: 14 Harbourfront Way, Road Town, Tortola, British Virgin Islands

Process type required: LETTERHEAD REQUEST

Preferred service: Email (compliance@northgate-digital.example)

Exposure point 1

Receiving address: TSampFic7Kd2mQ9xW4vR8nB5cE3aG6hJ1pZ

Sending transaction: facade05b83c19e46d072f5a1c8e94b30d67a2f51e09c84d73b6a15f28e90c46

Amount: 61,250 / USDT

VASP: Harborline Exchange Pte. Ltd. (fictional)

Legal address: 8 Marina View #21-03, Singapore 018960

Process type required: LETTERHEAD REQUEST

Preferred service: Service Portal (https://legal.harborline.example)

Exposure point 2

Receiving address: TSampFicWq83LdN5vK2xR7mB9cA4eF6gH1jT

Sending transaction: facade06c74d28f51e093a6b2d9f85c41e07b3a62f19d05c83e74b26a91f30d5

Amount: 27,940 / USDT

Signature omitted from sample.

Jesse Gossman, Managing Partner
The Block Audit LLC
1931 Cordova Rd #2053
Fort Lauderdale, FL 33316
info@theblockaudit.com
(954) 698-2700