

	Fraud Prevention Policy	RSC-POL-001-FIN
Publication Date: 10/15/2026	Risk Management	Public

Fraud Prevention Policy

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Contents

1. Purpose	2
2. Scope	2
3. Terms and Definitions	3
4. Principles	3
5. Fraud Typologies	4
6. Fraud Risk Assessment	4
7. Preventive Controls	5
7.1 Onboarding and registration	5
7.2 Access and authentication	5
7.3 Transactions and transfers	5
7.4 Employees and third parties	5
8. Precautionary Hold of Transfers	6
9. Detection, Investigation and Response	6
10. Interfaces with AML and Information Security	7
11. Sharing of Data on Indications of Fraud	7
12. Client Relationship and Remediation	8
13. Training and Awareness	8
14. Review	8
15. Reference Standards	8
16. Effectiveness	9
17. Version Control and History	9

	Fraud Prevention Policy	RSC-POL-001-FIN
Publication Date: 10/15/2026	Risk Management	Public

1. Purpose

This Policy sets out the principles, responsibilities and controls of Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda. ("Trace Finance") to prevent, detect, contain, investigate and remediate fraud and scams related to its products, services, channels and relationships.

It constitutes the fraud prevention policy required by article 43 of BCB Resolution No. 520/2025 and sets the guidelines for recording and sharing data and information on indications of fraud, in accordance with the applicable regulation.

2. Scope

This Policy applies to the officers, employees, interns, apprentices and service providers of Trace Finance and to all its products, services, channels, systems and relationships with clients, counterparties, partners and suppliers, in fiat currency and in virtual assets.

It covers external fraud, committed by clients, counterparties or third parties; internal fraud, committed by an employee or service provider, alone or in collusion; and scams against clients that involve Trace Finance's services.

The prevention of money laundering, information security and cybersecurity, and personal data protection are governed by specific regulations. This Policy addresses the interfaces with those topics.

	Fraud Prevention Policy	RSC-POL-001-FIN
Publication Date: 10/15/2026	Risk Management	Public

3. Terms and Definitions

Term	Definition
Fraud	Deceitful, misleading or bad-faith act, by action or omission, through untruth, abuse of power, breach of trust, circumvention of rules or other improper means, with the purpose of concealing facts or obtaining an undue advantage, for oneself or for third parties.
Scam	Fraud in which the client is induced, through social engineering, to authorize a transaction or transfer for the benefit of the fraudster.
Indication of fraud	Fact, pattern or information indicating the occurrence or attempt of fraud, not yet confirmed by investigation.
Internal fraud	Fraud committed by an officer, employee or service provider, alone or in collusion with third parties.
Account takeover	Improper access to the account, credential or channel of a legitimate client to carry out transactions without their authorization.
Mule account	Account or wallet of an intermediary used to receive and pass on funds or assets of fraudulent origin.
Precautionary hold	Temporary hold of a virtual asset transfer for risk analysis, in accordance with this Policy.
Fraud loss	Amount actually lost by Trace Finance or its clients as a result of fraud, net of recoveries.

4. Principles

a. Risk-based approach. Controls are proportionate to the exposure shown by the fraud risk assessment.

b. Prevention before execution. Preventive controls act before the activation of the relationship and the settlement of transactions whenever possible.

c. Immediate containment. In the face of a relevant indication, containment prevails over operational convenience, without prejudice to the client's rights.

d. Segregation of duties. Whoever executes a transaction does not release a held transaction or investigate their own actions.

e. Traceability. Events, decisions, losses, recoveries and data sharing produce verifiable records.

	Fraud Prevention Policy	RSC-POL-001-FIN
Publication Date: 10/15/2026	Risk Management	Public

f. Zero tolerance for internal fraud. Fraud committed by an employee or provider is investigated and sanctioned regardless of position or performance.

g. Data protection. The processing and sharing of data observe the purpose of fraud prevention, necessity and Law No. 13,709/2018.

5. Fraud Typologies

Trace Finance maintains a typology map that covers, at a minimum, the categories below:

Category	Examples
Identity and onboarding	Synthetic identity, false or stolen documents, use of a straw person, shell company and impersonation of a legal representative.
Account compromise	Account takeover, phishing, use of leaked credentials, session hijacking, device change and social engineering.
Payment and wallet instructions	Business e-mail compromise, improper change of bank details or wallet address, and false orders in the name of a client or counterparty.
Transfers and settlement	Unauthorized transfers, mule accounts and wallets, improper refunds and settlement against funds of fraudulent origin.
Scams against clients	Fake support, investment scams, false promises of returns and loss recovery scams.
Internal and third-party fraud	Collusion, abuse of privileged access, manipulation of parameters, improper alteration of records and supplier fraud.
Market fraud	Fictitious liquidity, wash trading and price manipulation of virtual assets. The prevention of market abuse and the reporting of spurious practices to the Central Bank of Brazil follow the Integrated Policy on Specific Activities and Custody, in accordance with article 70 of BCB Resolution No. 520/2025.

6. Fraud Risk Assessment

Fraud risk is assessed by product, channel, client segment and process, considering the mapped typologies, recorded events and losses, and the effectiveness of controls. The assessment uses the four-level scale (Low, Medium, High and Critical) adopted in Trace Finance's risk management and is updated annually and upon a new product, new channel, relevant event or change in typology.

The results feed the calibration of detection rules, the setting of limits and the prior assessment of new products and services, and are taken into account in the AML risk assessment where

	Fraud Prevention Policy	RSC-POL-001-FIN
Publication Date: 10/15/2026	Risk Management	Public

typologies overlap.

7. Preventive Controls

7.1 Onboarding and registration

- a.** validation of identity and documents through independent sources, including biometrics and device verification where applicable;
- b.** confirmation of the existence, activity and representatives of corporate clients;
- c.** checks against fraud indication databases and internal restriction lists before activation.

7.2 Access and authentication

- a.** strong, risk-based authentication for access to channels and for sensitive events;
- b.** enhanced controls for changes to registration data, bank details, wallet address, device and representatives;
- c.** confirmation, through a previously registered independent channel, of any change to a payment instruction or destination wallet.

7.3 Transactions and transfers

- a.** limits per client, per transaction and per period, and velocity controls;
- b.** lists of authorized withdrawal addresses and a waiting period for new addresses;
- c.** on-chain screening of the origin and destination of assets;
- d.** human review of transactions outside the client's pattern or showing signs of a scam.

7.4 Employees and third parties

- a.** segregation of duties and management of privileged access, with periodic review;
- b.** enhanced due diligence for roles and providers with access to systems, parameters or the movement of assets;
- c.** monitoring of access and of changes to sensitive records and parameters.

	Fraud Prevention Policy	RSC-POL-001-FIN
Publication Date: 10/15/2026	Risk Management	Public

8. Precautionary Hold of Transfers

As from January 1, 2027, transfers of virtual assets to a virtual asset service provider abroad or to a self-hosted wallet are held for up to 24 hours for risk analysis when the amount exceeds USD 10,000 or equivalent, considered individually or as the client's total for the day, and in the other situations defined by Trace Finance's risk assessment, in accordance with BCB Resolution No. 142/2021, as amended by BCB Resolution No. 584/2026.

The client is informed of the hold. The transfer may be released before the end of the period when the documented analysis concludes that the risk elements do not justify the hold, considering the risk profiles of the client, the transaction, the counterparty and the jurisdiction. The inclusion of the destination address in the list of wallets previously validated by Trace Finance (whitelist), with ownership verification, is a criterion for early release and does not exempt the transfer from the hold. The release decision is recorded per transaction, even if in a systematized manner, and early release is ruled out in the presence of signs of account takeover, recent changes to credentials, device or registration data, atypical client behavior or a high amount defined by Risk Management, in which case it requires dual approval. Transfers to virtual asset service providers authorized to operate in Brazil are not subject to the precautionary hold. The hold does not replace blocking arising from sanctions or the AML analysis.

9. Detection, Investigation and Response

Phase	Minimum actions
Detection	Detection rules and models, reports from clients, employees and partners, external intelligence, fraud indication databases and on-chain monitoring.
Classification	Severity, amount involved, clients affected, systemic risk and recording and reporting obligations.
Containment	Suspension of access, withdrawal restrictions, hold or blocking of transactions, blocking of beneficiary or address and notice to partners.
Investigation	Analysis of accounts, devices, wallets, counterparties, access trails and the transaction chain, with a case file.
Decision	Client remediation, recovery of funds, termination of the relationship, disciplinary measures and required communications.
Lessons learned	Root cause analysis and adjustment of rules, limits, product, communication and training.

	Fraud Prevention Policy	RSC-POL-001-FIN
Publication Date: 10/15/2026	Risk Management	Public

Events are classified on the four-level scale. High events are reported to the Chief Risk Officer, and Critical events also to the Board of Executive Officers and the Compliance Committee. The investigation of internal fraud is conducted by an area independent of the one involved, with preservation of evidence.

10. Interfaces with AML and Information Security

- a. AML:** every confirmed fraud event or event with a relevant indication is reported to Compliance within 24 hours of its identification, for assessment of reporting to Coaf. The flows are cumulative, and one may not replace the other; AML timeframes run from the date on which the indication was identified. The decision to report rests with the Officer responsible for AML.
- b. Relationship:** when the event involves an indication of ML/TF, the decision on the continuation of the relationship and the communication to the banking partner that carries out the transaction rest with Compliance, in accordance with the AML program.
- c. Prohibition of tipping off:** communications to the client about a hold, block or termination do not disclose the existence of an analysis or of a report to Coaf.
- d. Sanctions:** a match on a sanctions list identified during the investigation follows the asset freezing flow, which prevails over the measures of this Policy.
- e. Security incidents:** fraud arising from an information security incident is also handled in the incident response flow, including with regard to communications to authorities and data subjects.

11. Sharing of Data on Indications of Fraud

Trace Finance records and shares data and information on indications of fraud in accordance with Joint Resolution No. 6/2023 and BCB Resolution No. 343/2023, as extended to virtual asset service providers by BCB Resolution No. 552/2026, with implementation by October 30, 2026. The record includes, where applicable, the identification of whoever carried out or attempted the fraud, the description of the indications and the details of the destination account or wallet.

Sharing observes Law No. 13,709/2018 and the principles of purpose, necessity, quality and security. Each record identifies the origin, content, recipient, purpose, date and responsible person, with access control and a query trail.

Information received from third parties is a risk input and does not, on its own, produce an automatic adverse decision against the client without contextual analysis and handling of

	Fraud Prevention Policy	RSC-POL-001-FIN
Publication Date: 10/15/2026	Risk Management	Public

false positives.

Trace Finance maintains a contract with the provider of the electronic system for sharing data and information on indications of fraud and submits to the Central Bank of Brazil the monthly declaration of compliance, including when there are no records in the period, within the deadlines of BCB Resolution No. 343/2023.

12. Client Relationship and Remediation

The affected client is informed of the measures that affect them, through an official channel, without disclosure of information protected by secrecy. Complaints and fraud reports receive a protocol number, a response deadline and priority handling when there is a risk of further loss.

Client remediation, recovery of funds from partners and any reimbursement are decided based on the investigation, with the grounds recorded.

13. Training and Awareness

Employees receive annual training on fraud prevention, with specific content for the operations, client service and technology areas and for roles with access to the movement of assets or to sensitive parameters. Content is updated when new typologies are identified. Completion observes the deadline, minimum score and escalation applicable to Trace Finance's mandatory training, with recording of completion and results.

Trace Finance discloses to clients, users and suppliers information on good practices and on the risks of fraud and scams, in accordance with article 43, paragraph 2, III, of BCB Resolution No. 520/2025.

14. Review

This Policy is reviewed annually, with approval by the Board of Executive Officers, formalized in minutes, following prior deliberation by the Compliance Committee, and on an extraordinary basis upon a regulatory change, a Critical event, a new relevant typology or a change in products, channels or business model.

15. Reference Standards

Law No. 13,709/2018: General Personal Data Protection Law.

Law No. 14,478/2022: guidelines for the provision of virtual asset services.

	Fraud Prevention Policy	RSC-POL-001-FIN
Publication Date: 10/15/2026	Risk Management	Public

BCB Resolutions No. 519, 520 and 521/2025: authorization, operation and foreign exchange market transactions of virtual asset service providers.

Joint Resolution No. 6/2023 and BCB Resolution No. 343/2023: sharing of data and information on indications of fraud.

BCB Resolution No. 142/2021 (as amended by BCB Resolution No. 584/2026): fraud prevention procedures and controls, including the precautionary hold of virtual asset transfers, effective as from January 1, 2027.

BCB Resolution No. 85/2021, applicable by virtue of BCB Resolution No. 552/2026: cybersecurity policy.

BCB Circular No. 3,978/2020: prevention of money laundering and terrorist financing, with regard to the interfaces with anti-money laundering.

16. Effectiveness

This Policy enters into force on the date of its publication, after approval by Trace Finance's Board of Executive Officers, formalized in minutes, following prior deliberation by the Compliance Committee, and remains in force until its review or express revocation. The rules on the precautionary hold of transfers apply as from January 1, 2027.

17. Version Control and History

Version	Date	Change/Addition History	Approved by
1.0	10/15/2026	Initial issue.	Board of Executive Officers, following deliberation by the Compliance Committee