TRM Products/Services Descriptions

Last Update: October 30, 2023

This page describes each of the TRM Products and/or Services, one or more of which may be indicated on the applicable Order Form. The purpose of this page is to inform the Customer on the scope of each product offering to which TRM's obligations for performance and provisioning of services is associated.

Product Descriptions:

TRM Forensics: Provides an integrated suite of tools to investigate the source and destination of crypto funds to accelerate cases. With Forensics, customers can rapidly explore and visualize TRM's enriched Blockchain Intelligence data. Major functionality includes:

- Graph Visualizer: allows users to represent and trace transaction flows visually across 25 different blockchains and 1 million+ assets, all viewed within the same graph. Graph Visualizer also provides users access to TRM's signatures, which automatically detect groups of blockchain transactions that may be indicative of money laundering or fraud.
- Block Explorer: A search engine for blockchains where users can perform due diligence on any given VASP or non-VASP entity. Block Explorer provides both off-chain and on-chain data. Off-chain data is sourced by TRM about an entity that is not found on blockchain which can add helpful context to an evaluation of a Virtual Asset Service Provider or other entity. On-chain data provides a holistic overview on an entity's activity, and TRM's next-generation attribution engine enriches on-chain data for risk scoring and insights.
- Detect: Setup alerts to watch for activity: incoming, outgoing, or all transfers. When activity is observed, based on a defined trigger, TRM will email a notification to your list of recipients so you can know immediately.
- Bulk Data Analysis: Enables investigators to enrich bulk sets of blockchain transactions with TRM data in order to attribute sending and receiving addresses as well as detect risk exposure. This means customers with a large set of transaction hashes can rapidly assess what addresses received or sent funds to what entities based on the transaction hashes and TRM's attribution in relation to those addresses and entities.

- Custom Entities: Customers can define a collection of addresses and pre-existing entities as a new custom entity and monitor the custom entity in TRM as they would others.
- Case Management: Customers can organize an investigation from first transaction to final report. They can track addresses, entities, and graphs material to an investigation, add notes and attachments to store references and keep track of your findings, and track the disposition of your cases (with custom properties), all within TRM Forensics.
- Demixing Request: Provides customers the means within TRM Forensics to submit a request to demix an identified deposit into a mixing service.

TRM Wallet Screening: Screen cryptocurrency wallets of the customer's choice and view entities associated with the wallet, the blockchain associated with the wallet address screened, and an associated risk score that indicates the level of risk the wallet has been exposed to. A given wallet can be assigned Severe, High, Medium, Low, or Unknown. The overall risk score of an address is representative of the highest risk indicator associated with that address.

TRM Transaction Monitoring: Enables organizations to continuously monitor on-chain transfers to meet their compliance obligations and detect suspicious activity that may be indicative of money laundering or financial crime. Doing so ensures that as an organization they are not facilitating transactions with illicit actors, or any known "Predicate Offenses". Provides visibility into the exposure that you have with your customer's on-chain crypto activity and take action and mitigate risk in real-time.

TRM Know-Your-VASP: Monitors the risk exposure of cryptocurrency businesses so customers can safely onboard VASPs as customers and partners, while meeting AML/CFT regulatory requirements. The VASP Watchlist allows for easy management of a list of Virtual Asset Service Providers.

TRM Tactical: Designed for frontline investigators, Tactical is a mobile blockchain forensics app that empowers law enforcement and tax authorities to extract wallet addresses or transaction hashes from photos taken on scene and convert them into actionable data and insights to expedite building their cases where cryptocurrency is used for criminal activity.

TRM API: TRM provides an API to facilitate workflow customization for customers to better enable safer financial transactions. Integration use cases include:

- Integrating TRM functionality into custom applications
- Understanding risk when facilitating transactions
- Understanding if a wallet address has exposure to OFAC sanctions.
- Explore and trace an API call back to TRM Forensics

TRM Academy: Provides an extensive library of self-serve digital courses including product guides, tutorials, case studies, drills and timely micro-learnings on recent events or new product features. TRM Academy access is included in the cost of a TRM license. For non-TRM users, access to the Academy can be purchased either as an individual or as a group of enterprise learners for a fee.

- TRM Academy separately offers certification courses on demand. These self-paced certification courses provide in-depth instruction on a range of crypto and blockchain subject matter. On demand certification courses require an additional fee and are not included with TRM Academy access. Upon successful completion of the final assessment, participants receive an accreditation digital certificate and badge for display on social media profiles.
- Students access TRM Academy certification courses online via a learning management platform. Live instructor-led certification courses can be arranged also on request for groups of at least 5 — additional fees apply.

Sanctions Plus: designed for DeFi and similar organizations to automate wallet screening via the TRM Wallet Screening API. Categories are limited to Sanctions Ownership, Terrorist Financing Ownership, CSAM, CSAM Vendor, CSAM Consumer and CSAM Scam. An additional limited list of categories may be provided for optional screening or monitoring. Access to the TRM user interface is not included. Instead, wallet screening results via API can be viewed on a Mode dashboard.