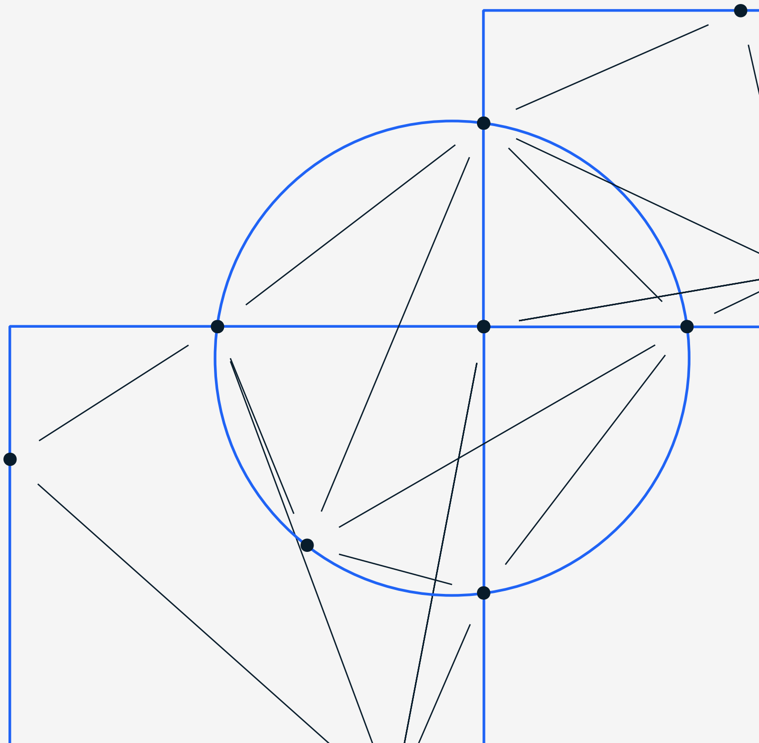
TRM WHITE PAPER

Four Ways TRM Improves Compliance in the Modern Sanctions Enforcement Era



TRMLABS.COM

In an increasingly digital and global financial ecosystem, digital assets have opened new avenues for innovation, efficiency, and inclusivity. However, this digital transformation has also introduced new risks, particularly in the realm of regulatory compliance and sanctions enforcement.

For global crypto exchanges, fintech companies, and financial institutions, maintaining compliance with international sanctions is more than just a regulatory requirement that protects organizations from reputational damage and monetary penalties – **it is essential for safeguarding the integrity of the financial system and guarding against illicit activities like money laundering, terrorist financing, and sanctions evasion.**

Moreover, where sanctions enforcement actions were historically dominated by the Office of Foreign Assets Control (OFAC) – which continues to focus on non-compliance in the digital asset space – global authorities are beginning to put increased efforts into enforcement and penalties for both sanctions evasion and lack of effective sanctions controls.

In this era of enforcement, blockchain intelligence solutions with robust sanctions programs have become indispensable to crypto, fintech, and financial institutions alike. **TRM Labs** provides the most expansive sanctions coverage and capabilities for identifying, assessing, and mitigating risks in real-time – empowering compliance teams to successfully navigate the complex and evolving landscape of global sanctions.

This paper is meant to highlight best practices, trends, and considerations for controls that institutions may wish to consider, depending on their own businesses and risks. Ultimately, institutions are responsible for all of their own sanctions and compliance-related decisions

The four pillars of effective sanctions compliance programs

TRM provides actionable sanctions intelligence and capabilities across four key pillars:

1. International list coverage
2. Comprehensive attribution
3. Speed of attribution
4. Dynamic alerts for facilitation and blocking

Let's take a closer look at each area in more detail.

1. International list coverage

One of the unique features of the crypto ecosystem is that it gravitates to multi-jurisdictional dynamics.

Exchanges often have a global customer base. Fintechs enabling crypto payments might facilitate transnational payment flows. Liquidity providers simultaneously service virtual asset service providers (VASPs) incorporated in crypto hubs like Hong Kong, the UAE, Singapore, or the United States. And even financial institutions building tokenized platforms may have cross-jurisdictional infrastructures — where the sub-custodian sits in one jurisdiction, the customer in another, a stablecoin asset issuer underpinning a trade in another, and so on.

With each border crossed, a new set of sanctions obligations is potentially unlocked. And as our modern sanctions regimes have grown increasingly more complex and adaptive to ever-changing national security issues, having international awareness and taking a global approach to your sanctions program (and the tools you use) has never been more critical.

When it comes to evaluating blockchain intelligence solutions, you need a platform that covers multiple national sanctions lists in order to ensure regulatory compliance and mitigate risk as your business scales.

TRM IN ACTION

TRM Labs enables crypto businesses and financial institutions to detect and prevent illicit transactions connected to sanctioned actors and jurisdictions by continuously monitoring global sanctions lists in real-time.

CASE STUDY
OFAC's sanctions against Dmitry Yuryevich Khoroshev

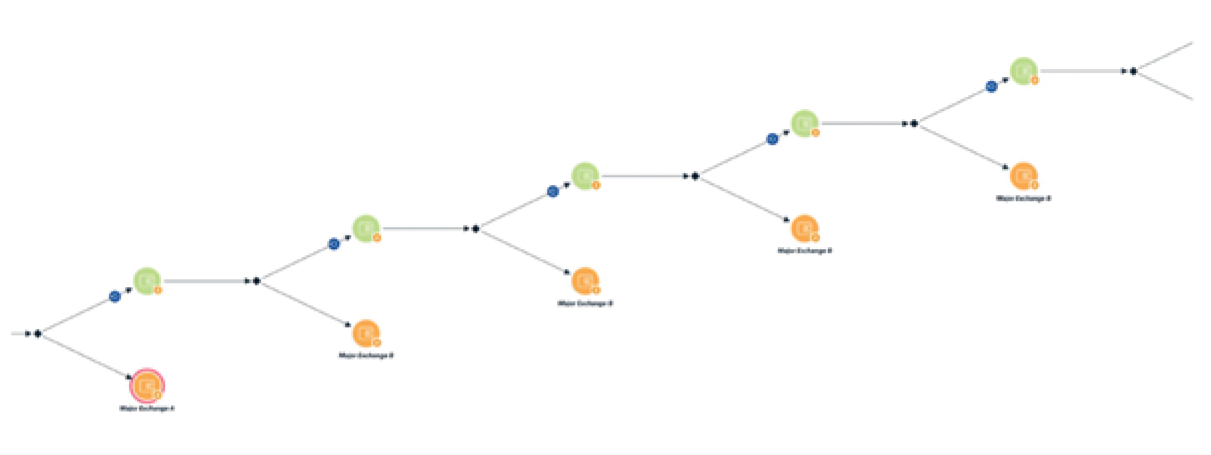
On May 7, 2024, Dmitry Yuryevich Khoroshev, a senior leader of the Lockbit ransomware group (one of the most active and prolific ransomware groups in the world), was sanctioned in a joint designation between the United States, United Kingdom, Australia, and other international partners. According to the designation, Khoroshev was responsible for a variety of Lockbit's activities – including upgrading the Lockbit infrastructure, recruiting new developers, and managing affiliates.

While each country added Khoroshev to its national sanctions list, OFAC also included a cryptocurrency address associated with Khoroshev in its designation. The addition of cryptocurrency addresses in any designation is a relatively new piece of intelligence, and a data point compliance programs must screen for. Yet it also creates the potential for designations in one country to have different information than another.

TRM IN ACTION

With the monitoring of multiple sanctions lists, TRM Labs was able to expand on the cryptocurrency address in OFAC's designation and identify hundreds of other addresses connected to Khoroshev.

TRM found that Khoroshev moved funds through a peeling chain, making multiple deposits to various global exchanges.



The Khoroshev designation is one of a number of examples of why it is crucial for crypto businesses to have blockchain intelligence tools that include real-time monitoring of major national sanctions lists.

At the same time, it's important to note that real-time monitoring of national lists cannot be the only proactive action taken. After a designation of crypto-related entities and individuals occurs, the best blockchain intelligence providers conduct additional post-designation investigations to ensure that the full scope of the sanctioned actor's on-chain footprint is uncovered. In the case of the Khoroshev sanctions, while OFAC only designated one address, TRM Labs was able to quickly conduct an investigation and attribute nearly 1,000 addresses to Khoroshev.

To that end, OFAC has explicitly placed an expectation on firms to screen and monitor entities' complete on-chain footprints, stating, "OFAC's digital currency address listings are not likely to be exhaustive. Parties who identify digital currency identifiers or wallets that they believe are owned by, or otherwise associated with, a specially designated national (SDN) and hold such property should take the necessary steps to block the relevant digital currency."[1]

[1] Source: https://ofac.treasury.gov/faqs/562

2. Comprehensive attribution

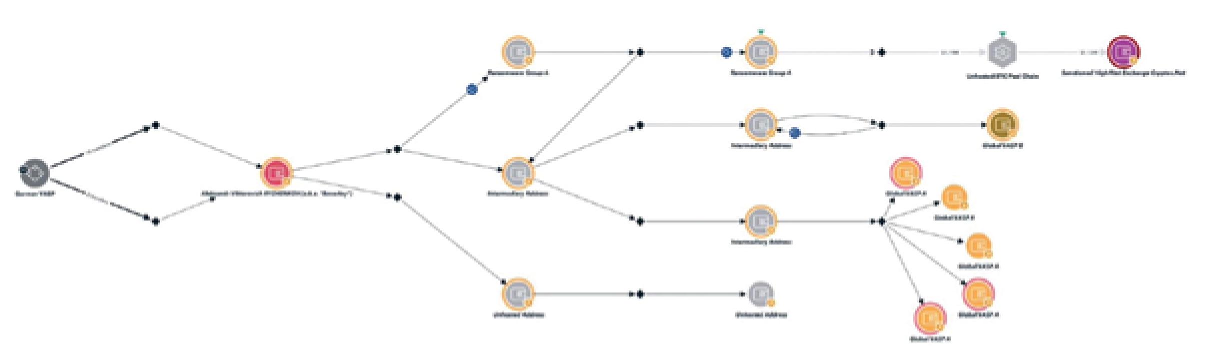
It's critical for blockchain intelligence solutions to have comprehensive attribution – not only for entities and individuals that appear on national sanctions lists, but also for entities and individuals in jurisdictions that are comprehensively sanctioned by OFAC, such as North Korea and Iran.

Identifying entities in comprehensively sanctioned or other hard-to-reach jurisdictions, and then mapping out their on-chain footprint, is an exceptionally complex challenge. Targeting and pinpointing these entities' transactional activities requires a deep understanding of blockchain data, geopolitical and legal contexts, and the ability to correlate on-chain data with off-chain intelligence. Additionally, these efforts must be supported by continuous monitoring and adaptation to evolving tactics used by sanctioned entities to obfuscate their activities.

TRM IN ACTION

TRM takes a multidisciplinary approach to attribution, combining technology, domain expertise, and legal acumen to ensure that sanctioned networks and entities – as well as those operating in comprehensively sanctioned jurisdictions – are uncovered in our platform and appropriately flagged.

For example, TRM's domain expertise allowed us to easily understand and expand the on-chain activity associated with the sanctioned LockBit affiliate and EvilCorp member, Aleksandr Viktorovich Ryzhenkov, also known as "Beverley."



TRM also regularly conducts attribution expansion investigations into sanctioned entities and jurisdictions to ensure businesses have a comprehensive overview of their direct and indirect sanctions exposure – particularly essential for entities subject to secondary sanctions.

CASE STUDY

Iran's use of crypto to evade sanctions

In the wake of recent attacks on Israel, there have been increased sanctions on Iran for the regime's part in providing financial and material support to Hamas, Houthis in Yemen, and Hezbollah in Lebanon. In addition to recent sanctions, over the years we have seen comprehensive sanctions on Iranian financial institutions. That means that US persons are not allowed to engage with Iranian financial institutions including crypto exchanges. TRM continuously identifies, investigates, and maintains attribution on VASPs located in Iran.

Iran's crypto economy is made up of a large breadth of crypto businesses and individual actors. However, it is dominated by Nobitex, Iran's largest exchange, which received 89% of all funds flowing to Iranian exchanges in 2023. As we see continued sanctions on Iran, it is more important than ever that cryptocurrency businesses and other financial institutions have a complete view of Nobitex and other Iranian VASPs.

You can learn more about TRM's coverage of the Iranian crypto landscape in our report on Iran's Crypto Economy.

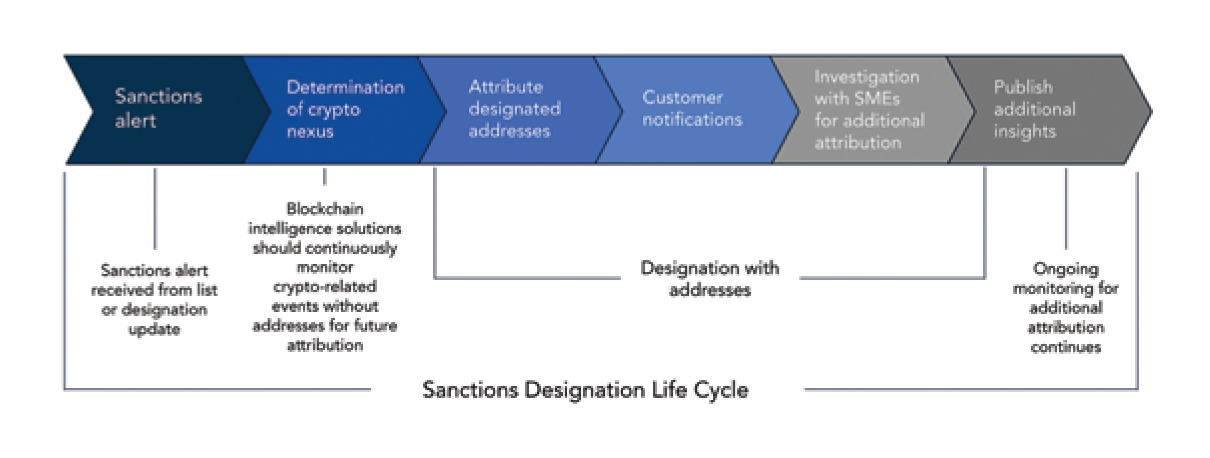
3. Speed of attribution

The growing landscape and increasing occurrence of crypto-related sanctions, combined with the rapid pace of crypto transactions, requires compliance teams to adapt rapidly to sanctions designations. Time gaps between a designation and any transactional activity by a sanctioned entity can result in significant penalties. That's why it's critical to use a blockchain intelligence solution like TRM, which brings new sanctions designations into the platform in a matter of hours after publication.

TRM IN ACTION

TRM's real-time monitoring of major sanctions lists and designations allows for swift attribution updates in our platform, enabling businesses to rapidly identify their exposure to sanctioned entities.

Here's what this looks like in TRM:


Sanctions alert
Determination of crypto nexus
Attribute designated addresses
Customer notifications
Investigation with SMEs for additional attribution
Publish additional insights
Sanctions alert received from list or designation update
Blockchain intelligence solutions should continuously monitor crypto-related events without addresses for future attribution
Designation with addresses
Ongoing monitoring for additional attribution continues
Sanctions Designation Life Cycle

This process enables TRM to get new sanctions designations into the platform – often with expanded attribution – and communicate updates to customers in a matter of hours after publication.

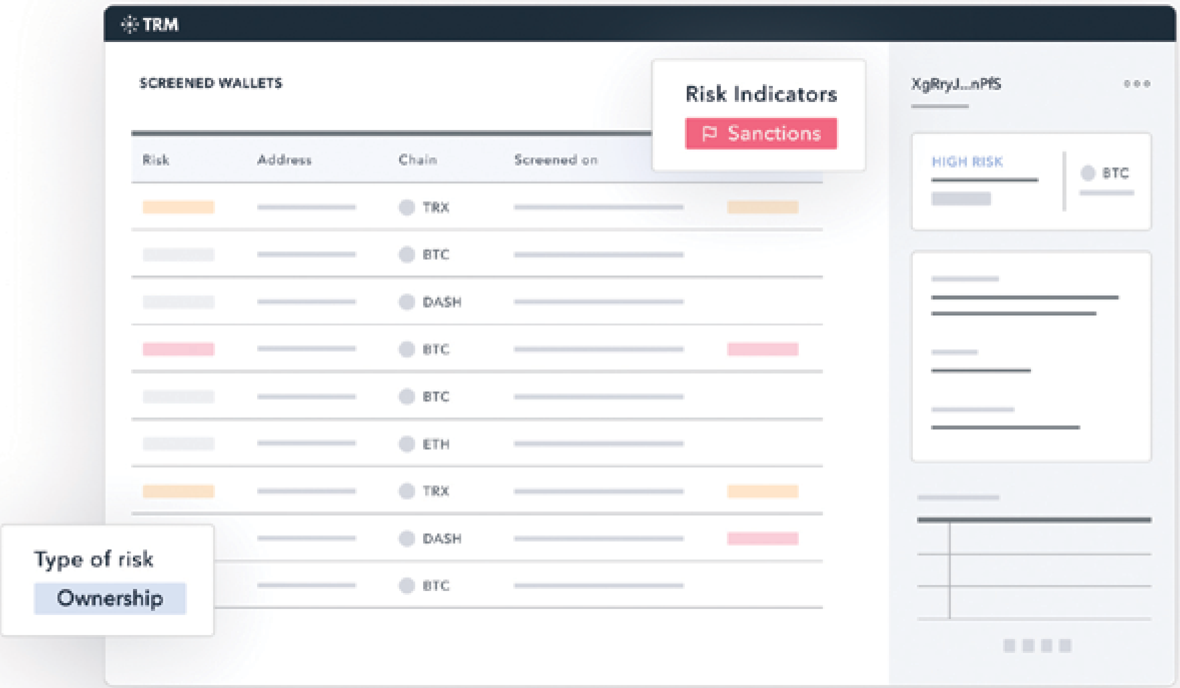
CASE STUDY

How Zodia Custody vets prospective exchanges using TRM

The assessment and monitoring of sanctions exposure extends not only to real-time screening of transactional activity, but also to the process of conducting due diligence on the potential sanctions exposure of prospective customers during enhanced due diligence exercises.

As a registered entity in the digital asset space, Zodia Custody (Zodia) plays a critical role in supporting compliance with international sanctions regimes. Through its robust compliance operations, Zodia helps not only ensure that sanctioned entities are effectively blocked from accessing the digital asset ecosystem, but also plays a key role in helping upskill other entities transacting in digital assets who may have the need for Zodia's custodial solutions.

As part of the company's due diligence processes, Zodia used TRM's blockchain intelligence platform to screen prospective exchanges' wallet addresses in order to identify and assess financial crime risk exposure, including sanctions-related risk. In one due diligence case, this review noted that an exchange had direct and indirect exposure to sanctioned entities. TRM's sanctions intelligence further enabled Zodia to identify not only which sanctioned entities the exchange was exposed to, but also address-level specifics to pinpoint volumes, values, and dates of the transactions – enabling a holistic and granular picture of the exchange's potential sanctions risk.



Zodia went a step further and used TRM's intelligence as part of their assessment to initiate discussions with the prospective exchange regarding its sanctions exposure, and flagged the specific instances of risk exposure. These discussions focused on how the exchange could implement a remediation and enhancement program to strengthen their own sanctions control environment.

The information garnered from TRM's sanctions intelligence was a significant contributor to Zodia's due diligence process, enabling the team to make an informed decision with respect to establishing a business relationship with the prospective crypto exchange.

4. Dynamic alerts for facilitation and blocking

The ever-increasing global nature of crypto businesses and financial institutions means that each organization is likely to have a varied interest in sanctions lists, sanctions regimes, regulatory frameworks, and risk appetites. As such, it's critical to leverage blockchain intelligence solutions with controls that can be adjusted to meet the needs of specific types of customers.

TRM IN ACTION

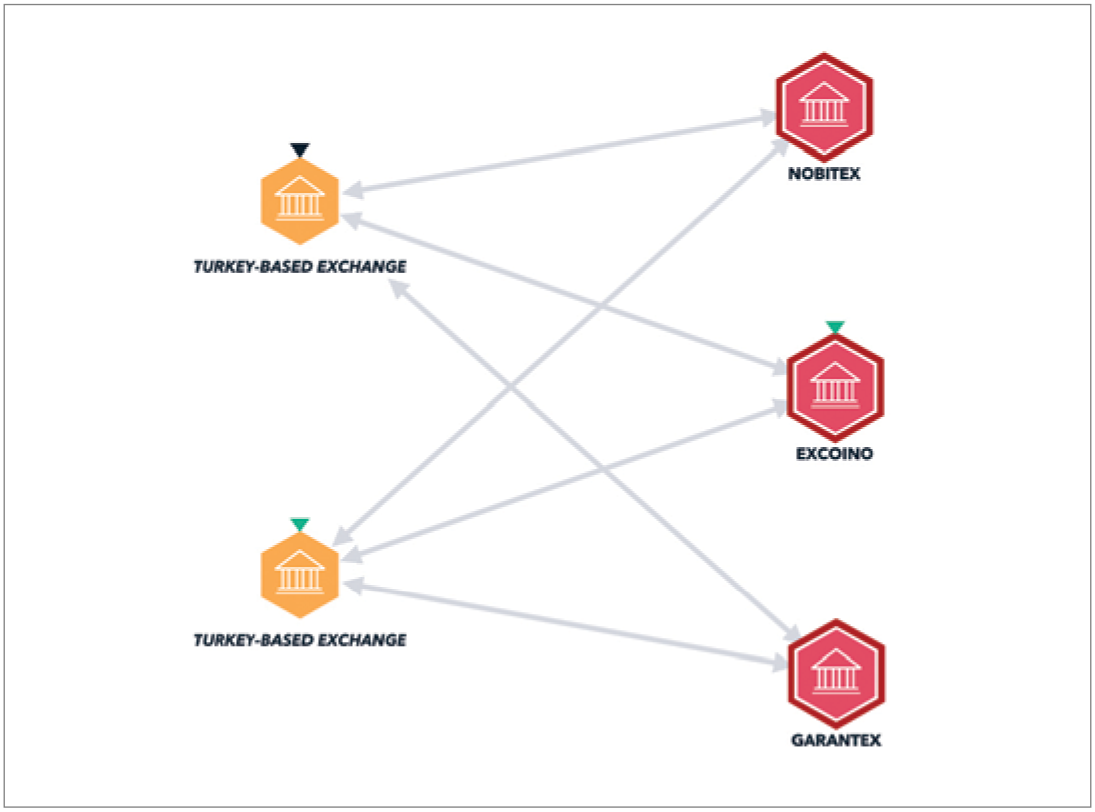
TRM's alert rules enable users to define highly customized criteria to flag transactions, including the ability to define rules based on a counterparty's country.

CASE STUDY

Building jurisdictional awareness with blockchain intelligence

When it comes to identifying sanctions risks in transactions, crypto businesses and financial institutions cannot only be focused on entities in comprehensively sanctioned jurisdictions (e.g. Iran). **They also need to be able to identify sanctions risk stemming from third-party jurisdictions that may be acting as sanctions evasion facilitators.**

For example, while Turkey was removed from Financial Action Task Force (FATF)'s list of "jurisdictions under increased monitoring" (also known as the "gray list") in June 2024, the country may still present a third-country sanctions risk for businesses interacting with Turkey-based crypto businesses. Over 90% of the illicit counterparty risk for Turkey-based crypto businesses in 2024 has been from sanctioned entities or entities in sanctioned jurisdictions.



TRM graph showing three sanctioned entities interacting with Turkey-based exchanges

Crypto exchanges, fintech companies, and financial institutions should leverage blockchain intelligence to monitor transactions with jurisdictions that their established risk assessment deem to be "high-risk" for sanctions exposure.

TRM IN ACTION

In TRM, users can define highly customizable rules to flag transactions based on interactions with a named entity or with specific countries to match the risk appetite of their business.

CASE STUDY

How TRM enables proactive threat detection

Proactive threat detection through wallet screening is an essential strategy for identifying and mitigating risks associated with sanctioned entities and jurisdictions before they escalate.

By continuously monitoring cryptocurrency wallets, financial institutions can detect suspicious activity linked to sanctions in real-time. With TRM Labs, financial institutions can detect sanctioned actor activity – even if assets move across blockchains. This proactive approach ensures compliance with international sanctions regimes and strengthens overall security.

TRM IN ACTION

TRM Labs allows businesses to integrate wallet screening into their comprehensive compliance programs to stay ahead of emerging threats – so they can protect both their operations and the broader financial ecosystem.

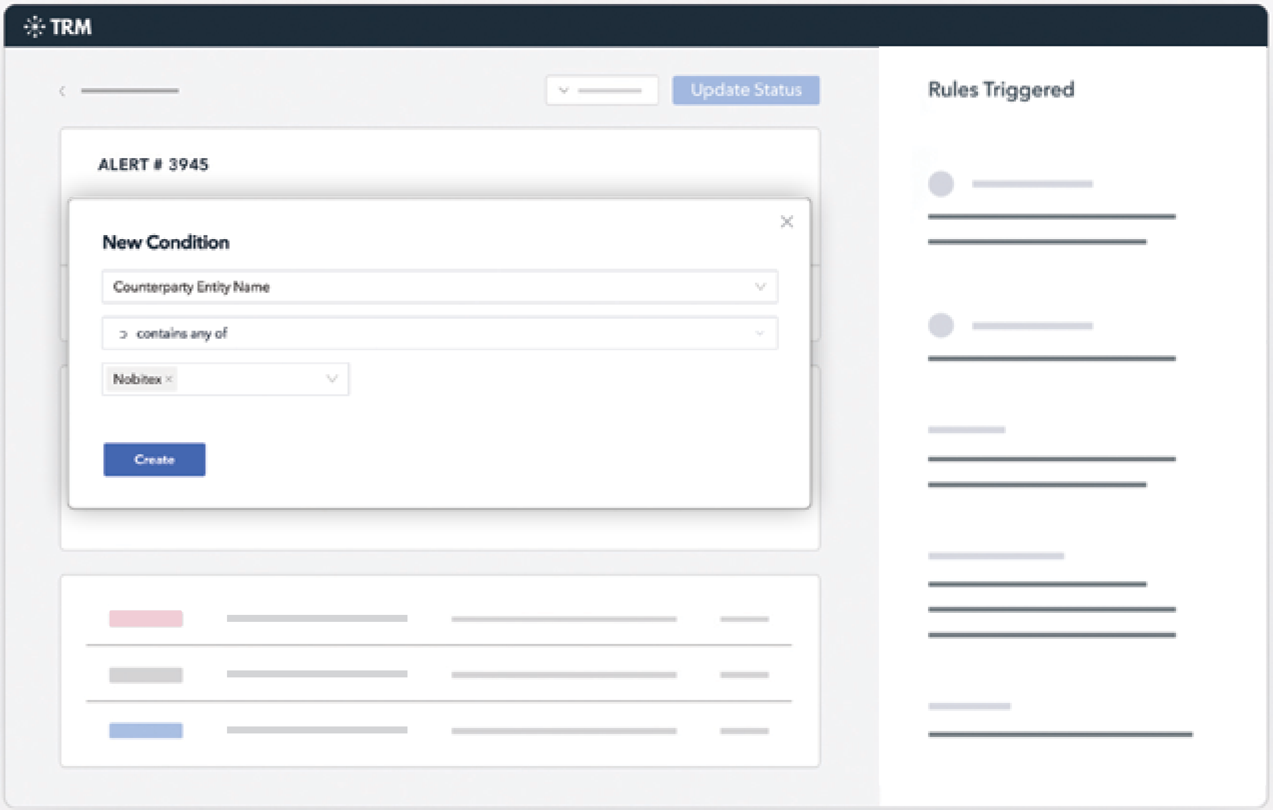
TRM's Wallet Screening rapidly screens for the risks that matter most to businesses.

- Companies can configure risk engine rules across 150+ risk categories based on what constitutes low, medium, high, or severe risk for their organization
- Automatic cross-chain indirect exposure surfaces risk to sanctioned actors when they move assets across blockchains
- Multi-layered risk exposure enables businesses to identify the holistic footprint of threat actors with ownership, counterparty, and indirect exposure
- Fast response time provides wallet screening results, including trading volume, a full list of risks, and attribution in less than 400 milliseconds

TRM's robust sanctions coverage enables compliance teams to surface exposure to entities not only on national sanctions lists, but also to entities in jurisdictions that are comprehensively sanctioned by OFAC, such as Iran.

TRM IN ACTION

Nobitex – Iran's largest cryptocurrency exchange – conducts billions in transaction volume each year. However, it does not appear on a national sanctions list. TRM Labs enables crypto businesses to screen wallets for ownership, counterparty, and indirect risk to the dozens of entities in Iran (like Nobitex) that may not appear in traditional sanctions screening tools – meeting regulatory obligations quickly and efficiently.



ALERT # 3945

New Condition

Counterparty Entity Name

contains any of

Nobitex ×

Blockchain intelligence for sanctions compliance is critical

With the increasing pace of crypto-related sanctions designations and crypto activity in sanctioned jurisdictions, it is absolutely critical for businesses to invest in blockchain intelligence with robust coverage of entities and individuals – so they can assess their exposure in real-time. However, not all blockchain intelligence tools are created equal.

TRM Labs has the most proactive and expansive coverage of the illicit crypto ecosystem, allowing businesses to monitor not only current sanctions risk, but also stay ahead of threats that may become sanctions targets in the future.

Click here to learn more about how TRM can help your organization stay compliant with sanctions enforcement.

About TRM Labs

TRM Labs provides blockchain analytics solutions to help law enforcement and national security agencies, financial institutions, and cryptocurrency businesses detect, investigate, and disrupt crypto-related fraud and financial crime. TRM's blockchain intelligence platform includes solutions to trace the source and destination of funds, identify illicit activity, build cases, and construct an operating picture of threats. TRM is trusted by leading agencies and businesses worldwide who rely on TRM to enable a safer, more secure crypto ecosystem. TRM is based in San Francisco, CA, and is hiring across engineering, product, sales, and data science.

To learn more, visit www.trmlabs.com