Contents

Virtual Asset Sanctions Red Flags: A Field Guide for the New Compliance Officer

Prepared August 2026. This is a snapshot, not a static reference: the blockchain analytics vendor landscape moves quickly (CipherTrace wound down its core compliance products in 2024, and Tornado Cash went from sanctioned to delisted between 2022 and 2025), and OFAC, FinCEN, and FATF all revise their virtual asset guidance regularly. Confirm current features, legal status, and access before relying on anything below for a live decision.

Virtual assets cover a wider span than the phrase "cryptocurrency" suggests: convertible virtual currencies like Bitcoin and Ethereum, stablecoins pegged to fiat or other assets, the exchanges and custodians that hold and move them, and the decentralized finance (DeFi) protocols and smart contracts that let value move without any intermediary at all. A company can meet sanctions risk from several directions at once: as an exchange, a custodian, a payment processor, an investor, or simply a counterparty to any of these. OFAC issued its first tailored guidance for the industry in October 2021, and the typologies below have been refined since through enforcement actions, an April 2022 joint advisory on North Korean crypto theft, and FATF's ongoing monitoring of how virtual asset service providers (VASPs) implement its standards. What follows is organized in two parts: first, the red flags themselves and how the industry generally responds to each; second, every data source, platform, and service named in that first part, regrouped by what kind of solution it is, with a plain synopsis of what it does and how well.

One thing is different here from a physical-asset compliance program: the blockchain itself is public. Every transaction is visible to anyone who looks, which is both why blockchain analytics became a viable industry at all and why the tools below can do things a maritime or trade-finance compliance program cannot. But that same transparency is also why the evasion techniques below are almost all about breaking the link between an identity and an address, rather than hiding the transaction itself. Nothing below substitutes for judgment. These tools narrow down where to look. They don't make the call for you.

Part 1: The Red Flags, and How the Industry Responds

1. Sanctioned wallet addresses transacting directly

Since November 2018, OFAC has identified specific digital currency addresses, not just names, as part of individual designations, and it has kept adding them since. A designated address is about as close to a bright line as sanctions compliance gets: if a wallet is listed, sending funds to it is a violation, full stop. The complication is scale and currency: OFAC's list spans addresses across a dozen-plus digital currencies, and new addresses appear with every fresh designation, so a screening program built once and left alone falls behind within weeks.

The response is automated, continuous address screening rather than a one-time or manual check, run at the point a transaction is initiated and re-run against the current list rather than a cached one. Chainalysis, TRM Labs, Elliptic, and Crystal Intelligence all build real-time address and transaction screening around exactly this list (among others), and Chainalysis and TRM both offer a free, no-relationship-required tool built for smaller platforms that only need this most basic check. This is the most mechanically solvable red flag in the set, since it's literal matching against a published list, but it's also the narrowest: it only catches an address after OFAC has already designated it, so it says nothing about a wallet that hasn't been listed yet, however suspicious its behavior.

2. Mixers and tumblers used to obscure the trail

A mixer pools funds from many users and redistributes them, breaking the direct link between a deposit address and a withdrawal address that would otherwise be visible on-chain. It is the most direct on-chain analogue to money-laundering layering, and OFAC has targeted mixers with three different designations that illustrate three different flavors of the same problem: Blender.io (a custodial mixer, May 2022), Tornado Cash (a non-custodial, autonomous smart-contract protocol, first designated August 2022), and Sinbad.io, widely reported as a Blender.io successor (November 2023). Tornado Cash's history matters specifically because of what happened next: developers sued, the Fifth Circuit ruled in November 2024 that immutable smart contracts aren't "property" a foreign national can hold under the International Emergency Economic Powers Act, and OFAC delisted Tornado Cash's contracts in March 2025 while keeping one of its developers individually sanctioned under the North Korea program. The underlying reason it was designated in the first place, laundering for the Lazarus Group, is undisputed; what's now unsettled is whether sanctioning the autonomous code itself, as opposed to a person or a custodial business, is legally available at all.

Practically, the response hasn't changed much despite that legal uncertainty: treat any address shown to have interacted with a known mixer as elevated risk requiring enhanced due diligence, and use tracing tools built to probabilistically reconnect pre-mix and post-mix funds ("demixing") rather than treating the mixer as an opaque wall. Chainalysis Reactor, Elliptic Investigator, and TRM Forensics all include demixing and advanced clustering capability aimed specifically at this. It works reasonably well against older, well-studied mixers where enough historical data exists to build reliable heuristics, but it's probabilistic rather than certain, new mixing approaches keep appearing, and the Tornado Cash litigation leaves genuinely open whether the sanctions tool itself can reach a non-custodial protocol the next time one appears.

3. Privacy coins and privacy-enhancing protocols

Monero uses ring signatures and stealth addresses so that, by default, even a full copy of its blockchain doesn't reveal the sender, receiver, or amount of a transaction. Zcash offers an optional "shielded" transaction type with similar properties. This is a different problem from a mixer, where the underlying chain is transparent and the obfuscation is a tactic layered on top: here the base protocol itself is built not to disclose the information a compliance program needs.

The industry's response has mostly been a business decision rather than a technical one: most large regulated exchanges have delisted or severely restricted Monero specifically because it defeats the screening approach everything else in this guide depends on, and treat any conversion into or out of a privacy coin as a red flag requiring enhanced due diligence regardless of amount. No blockchain analytics vendor can reliably trace a default Monero transaction the way they trace Bitcoin or Ethereum; some offer limited visibility into Zcash's optional transparent pool, but that's a narrower claim than full transaction tracing. This is worth stating plainly rather than glossing over: it is a genuine, openly acknowledged capability gap across the industry, not a feature any vendor is close to closing.

4. Chain-hopping and cross-chain bridges

A bridge protocol locks an asset on one blockchain and mints a wrapped equivalent on another, and a cross-chain swap does something similar through a decentralized exchange aggregator. Both are entirely legitimate infrastructure, and both are also a convenient way to break a single-chain trail: funds that are easy to trace on Ethereum become a different, wrapped asset on a different chain, and a screening tool that stops at the chain boundary loses the thread exactly where it matters.

The response is cross-chain tracing that follows value through a bridge contract's mint and burn events rather than treating each chain as a separate investigation. TRM Labs markets tracing across 400-plus bridges, Elliptic covers 65-plus blockchains and bridges with what it calls a unified view of value flows, and Chainalysis builds cross-chain correlation into both Reactor and KYT. This capability has matured substantially and is now a standard vendor feature rather than a niche one, but Elliptic's own 2026 outlook flags that many live deployments still only check three to five hops deep by default and haven't turned on full cross-chain coverage, which means the gap in practice is often a configuration choice rather than a genuine technical limit.

5. Peeling chains and structuring across many hops

A peel chain splits a large sum into many smaller transfers routed through a long sequence of intermediate addresses, each transaction small enough to sit under an alerting threshold and the sequence long enough that manual tracing becomes impractical. It is a direct crypto analogue to structuring in cash transactions.

Automated graph-based clustering, following a chain of addresses programmatically rather than one manual lookup at a time, is the standard response, and it's the core function of the major investigation tools: Chainalysis Reactor, Elliptic Investigator, and TRM Forensics are all built around exactly this kind of visualization and automated tracing. These tools do this well for clusters that are already well-attributed to a known entity, since the surrounding context narrows the graph considerably. Attribution confidence drops the further a trail gets from a known starting point, though, and state-sponsored actors in particular design peel chains specifically to defeat clustering heuristics, so the tooling is stronger at confirming a suspected link than at cold-starting an investigation from an anonymous address alone.

6. Unhosted wallets and nested or unregistered VASPs

Funds can move to a self-custodied ("unhosted") wallet with no counterparty at all to screen, or through a smaller "nested" exchange or OTC desk that operates as an unregistered intermediary riding on a larger, regulated exchange's infrastructure. Either way, the receiving side of the transaction may present no compliance program for a sending institution to rely on.

The response is counterparty due diligence on the receiving platform itself, not just the transaction, combined with enhanced scrutiny triggers for unhosted-wallet withdrawals above a threshold. Elliptic Discovery is built specifically to assess a VASP's own compliance posture before an institution transacts with it, and Notabene's Travel Rule infrastructure inherently requires confirming a receiving VASP is a real, identifiable, information-sharing-capable entity before a transfer goes out. This works well against a real, licensed, cooperative counterparty. It's considerably weaker against a genuinely unhosted wallet, where there's no institution to diligence at all, or a VASP deliberately operating from a non-cooperative jurisdiction, which is exactly the gap the sanctioned-exchange rebranding pattern in section 10 below exploits.

7. DeFi protocols and smart contracts used to bypass KYC entirely

A decentralized exchange or lending protocol executes through a smart contract with no onboarding step of any kind, letting a party swap illicit-origin assets for cleaner ones, or borrow against them, without ever touching a screened intermediary. This is qualitatively different from every red flag above it: there is no institution in the loop to run a check at all unless one is built into the protocol itself.

Treasury's own 2023 illicit finance risk assessment of DeFi treats this gap directly, and the industry's most concrete response is putting the screening on-chain: Chainalysis's free Sanctions Oracle is a smart contract that any other smart contract can call to check whether an address is sanctioned before completing a transaction, deployed on most major EVM chains and free to use without a Chainalysis relationship. It's a genuinely elegant fix where it's adopted. The catch is that adoption is optional: a protocol has to choose to call it, and a user interacting directly with a contract rather than through a compliant front-end bypasses it entirely. Combined with the same legal uncertainty raised by the Tornado Cash litigation over whether

autonomous code can be sanctioned at all, this remains one of the least mechanically solved categories in virtual asset compliance.

8. Stablecoins as a sanctions-evasion payment rail

A fiat-pegged token combines price stability with the speed and pseudonymity of crypto rails, which makes it attractive for entirely legitimate cross-border payments and equally attractive for moving sanctioned-jurisdiction value. Beyond established dollar-pegged tokens like USDT and USDC, newer state-linked instruments have appeared specifically to route around Western issuers: the ruble-pegged A7A5 stablecoin, sanctioned by the U.S. Treasury in August 2025, was created by people connected to the sanctioned Russian exchange Garantex specifically to give its successor network a stable-value settlement asset.

The one mitigant here that doesn't exist for most other crypto assets is issuer-level freezing: a major stablecoin issuer can, and sometimes does, freeze funds at specific addresses at its own discretion, independent of any government order. Tether's freezing of wallets was part of what let law enforcement disrupt Garantex in March 2025. Chainalysis's Sentinel product is built specifically around stablecoin-issuer risk. This lever is powerful but entirely dependent on the issuer's willingness and jurisdictional reach to use it, and it doesn't exist at all for a stablecoin created specifically to sit outside that reach, which is precisely why instruments like A7A5 got built.

9. State-sponsored theft laundered through crypto

North Korea-linked actors, tracked across government advisories as the Lazarus Group, APT38, BlueNoroff, and TraderTraitor, steal virtual assets directly through hacking rather than transacting through any conventional channel at all, then launder the proceeds to fund the regime's weapons programs. The scale has grown sharply: TRM Labs and Chainalysis both reported North Korea stole roughly $1.3 to $1.4 billion in crypto across 2024, and that was before the February 21, 2025 theft of about $1.5 billion from the exchange Bybit, the largest crypto theft on record, which the FBI publicly attributed to the group within days.

Because the initial theft is a cybersecurity failure rather than a sanctions-compliance one, the response that actually matters for a compliance program happens after the fact: rapid post-incident tracing of the specific stolen funds, paired with industry-wide coordination to freeze or blacklist those addresses across exchanges before laundering completes. Chainalysis, Elliptic, and TRM all publicly tracked the Bybit theft's fund movements in near real time, and the FBI/CISA/Treasury joint advisory from April 2022 remains the reference document for the group's tactics generally. Attribution has become fast and confident, and coordinated freezing has recovered meaningful portions of some past thefts, but the group visibly adapts its laundering speed and technique after each major incident, and no compliance tool addresses the theft itself, only what happens to the money afterward.

10. Sanctioned exchange rebranding under a new name

A designated or law-enforcement-disrupted exchange can simply reappear under a new legal wrapper, often run by the same people, serving the same clientele within weeks. Suex re-emerged as Chatex after its 2021 designation; more recently, after the Russian exchange Garantex was sanctioned in 2022 and then had its domains and servers seized in a March 2025 international law-enforcement operation, it resurfaced almost immediately as Grinex, which the U.S. Treasury sanctioned in August 2025 alongside the A7A5 stablecoin, and researchers have since traced further successor entities operating under names including Exved and MKAN Coin. This is the closest crypto-space equivalent to the maritime industry's flag-hopping: the underlying operation survives by discarding its identity rather than its business.

The response is attributing a new platform to its predecessor's known wallet clusters and infrastructure rather than treating a new name as a genuinely unconnected counterparty. This is squarely within blockchain analytics vendors' core competency: both Chainalysis and Elliptic published public analysis linking Grinex to Garantex within days of the rebrand becoming apparent, based on shared wallet clusters and infrastructure rather than the new entity's own disclosures. Vendors have gotten fast at spotting this technical link once a rebrand happens, but there's an unavoidable lag between the rebrand occurring and it being confirmed, and a compliance program screening only against the current, formal list of designated names has a window in which the new name still looks clean.

11. The baseline: sanctions list and entity screening itself

Underneath all of the above sits the same basic requirement that still catches most formal designations: screening the legal entities and individuals behind a VASP relationship, not just wallet addresses, against the actual sanctions lists, and re-screening on a recurring schedule rather than only at onboarding. This is the same screening discipline that applies to any counterparty in any industry, and it's worth stating alongside the blockchain-specific tools above because it's easy to treat crypto compliance as purely an on-chain problem when the people and companies behind a wallet are just as much a sanctions target as the address itself.

Automating this screening against a current, regularly updated list, and covering the beneficial ownership layer behind a corporate counterparty the same way any other industry would, is the standard practice. OFAC's own free Sanctions List Search, the EU Sanctions Map, and the open, aggregated OpenSanctions database serve as free or low-cost starting points; LSEG's World-Check and Dow Jones Risk & Compliance remain the two most widely used curated commercial datasets across financial-crime compliance generally, crypto included. As with the address-level tools above, name-and-entity matching reliably catches known names, but the entire point of most of the tactics in this guide is to keep the actual controlling party off any list in the first place, so this baseline catches only the portion of exposure that's already been formally identified.

Part 2: The Same Tools, Organized by Type of Solution

Every synopsis below reflects the provider's own public description of the product, alongside independent reporting where it exists. Capability claims, coverage figures, and similar performance numbers quoted by any vendor are that vendor's own claim, not an independently audited benchmark; treat them as marketing until verified against your own experience.

A. Regulatory guidance and reference documents (free, public)

Sanctions Compliance Guidance for the Virtual Currency Industry (October 15, 2021) — U.S. Department of the Treasury, Office of Foreign Assets Control
https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf
OFAC's first tailored sanctions guidance for the industry: technology companies, exchanges, administrators, miners, wallet providers, and users. Sets out compliance-program expectations and the FAQ definitions (559, 646, and others since) that everything downstream refers back to.

FinCEN Guidance on the Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019) — Financial Crimes Enforcement Network
https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf
Consolidates FinCEN's prior guidance on how the Bank Secrecy Act applies to different virtual currency business models. Predates OFAC's 2021 brochure and remains the reference point for the AML/BSA side rather than sanctions specifically.

North Korean State-Sponsored Cyber Actors Use TraderTraitor Malware to Facilitate Cryptocurrency Heists (April 18, 2022, alert AA22-108A) — FBI, CISA, and U.S. Treasury, jointly
https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a
The reference document for Lazarus Group's tactics against crypto exchanges and DeFi protocols, naming the actors, their techniques, and mitigation recommendations. Still the standing baseline advisory for this category, updated in practice by each subsequent incident's after-action reporting.

Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (October 2021) — Financial Action Task Force
https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html
FATF's guidance on implementing Recommendation 15, including the Travel Rule, stablecoins, and DeFi. FATF publishes a periodic targeted-update report tracking global implementation progress; the current one is on FATF's virtual assets topic page.

Illicit Finance Risk Assessment of Decentralized Finance (April 2023) — U.S. Department of the Treasury
https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf
Treasury's own assessment of how DeFi's lack of intermediaries changes illicit-finance risk, including money laundering, sanctions evasion, and proliferation financing. The clearest primary-source statement of why DeFi is treated as its own category rather than folded into general virtual-currency guidance.

B. Free and public blockchain data and crypto sanctions-screening tools

Etherscan — Etherscan (independent, not affiliated with the Ethereum Foundation)
https://etherscan.io
A free, public block explorer for the Ethereum blockchain: any address, transaction, or smart contract can be looked up directly, with equivalent explorers available for other chains (Bitcoin, Solana, and so on, each generally maintained by a separate provider). The rough equivalent of a free vessel registry lookup: authoritative for what's actually on-chain, but it won't tell you who controls an address unless that attribution has been published somewhere else.

OFAC Sanctions List Search (digital currency address search included) — U.S. Department of the Treasury
https://sanctionssearch.ofac.treas.gov
The same free, official OFAC lookup tool used for any sanctions search, covering the digital currency addresses that have been part of SDN and Consolidated List entries since 2018 alongside conventional identifiers. The primary source; not built for automated, high-volume, or batch screening.

Chainalysis Sanctions Oracle and Sanctions Screening API — Chainalysis
https://go.chainalysis.com/chainalysis-oracle-docs.html
A free, no-relationship-required way to check whether an address is sanctioned: an on-chain smart contract that any other contract can call directly, plus a REST API for wallets, apps, and exchanges. Deployed on most major EVM chains and built specifically to give DeFi protocols and smaller platforms a way to screen without a paid compliance stack.

TRM Labs free sanctions screening tool — TRM Labs
https://www.trmlabs.com
A free, API-based tool alerting platforms when a sanctioned address engages with them, covering multiple blockchains simultaneously so a match on one chain surfaces a corresponding address on others. Aimed at smaller crypto businesses that need a baseline check without a full enterprise contract.

C. Commercial blockchain analytics and compliance platforms

Chainalysis (Reactor and KYT) — Chainalysis
https://www.chainalysis.com
The largest and most widely cited blockchain intelligence vendor. KYT (Know Your Transaction) is real-time transaction and wallet monitoring built for exchanges and financial institutions; Reactor is the investigation and fund-tracing tool used to visualize flows, demix funds, and build evidentiary cases. Its data and attributions have been used in major law-enforcement actions and court cases, which is both a mark of credibility and a reason vendor claims about coverage and accuracy carry real weight here.

Elliptic (Lens, Navigator, Investigator, and Discovery) — Elliptic
https://www.elliptic.co
Lens screens individual wallets and transactions in real time; Navigator does the same at scale for continuous transaction monitoring; Investigator handles cross-chain fund tracing for deeper investigations; Discovery screens VASP counterparties for their own compliance posture before onboarding. Elliptic markets coverage across 65-plus blockchains and bridges and has been a partner since 2015 for a number of major exchanges.

TRM Labs (Forensics, Wallet Screening, and Transaction Monitoring) — TRM Labs
https://www.trmlabs.com
Forensics is the investigation and cross-chain tracing product, including AI-assisted case-building tools; Wallet Screening and Transaction Monitoring cover the real-time compliance side. TRM markets risk screening across 184-plus blockchains as of mid-2026, with deeper real-time tracing on a smaller subset carrying what it calls enhanced support, and is used by banks, exchanges, and government agencies alike.

Crystal Intelligence (Crystal Expert) — Crystal Intelligence (formerly Crystal Blockchain, built by Bitfury)
https://crystalintelligence.com
An institutional blockchain analytics platform aimed squarely at compliance officers and MLROs, covering 330-plus blockchains, with jurisdiction-specific threshold logic built in (the EU's €1,000 MiCA (Markets in Crypto-Assets Regulation) threshold, FinCEN's $3,000 threshold, and similar). Positioned as a strong fit for EU-regulated VASPs given its MiCA-specific tooling, and integrates with several Travel Rule providers rather than handling that transmission itself.

D. Travel Rule compliance

Notabene — Notabene
https://notabene.id
The most widely cited end-to-end solution for FATF Recommendation 16, the "Travel Rule," which requires VASPs to exchange originator and beneficiary information on transfers above a jurisdiction-specific threshold. Handles counterparty VASP identification, encrypted data exchange across multiple messaging protocols, and risk-based transaction rules in one dashboard, and integrates with several blockchain analytics vendors for the underlying risk data.

E. Smart contract and DeFi security auditing

CertiK — CertiK
https://www.certik.com
Audits smart contract code using a combination of manual expert review, formal verification (mathematical proof techniques beyond standard testing), and AI-assisted analysis, across essentially any chain or language. Its free public Security Leaderboard scores thousands of DeFi and NFT projects by audit history and security posture, and its Skynet and Security Oracle products offer real-time on-chain monitoring after launch rather than a one-time audit snapshot. This addresses a different risk than the transaction-screening tools above: whether the protocol itself is safe to interact with, not whether a given counterparty is sanctioned.

F. General sanctions-list and entity screening

EU Sanctions Map — European Commission
https://www.sanctionsmap.eu
The same free, visual EU sanctions reference tool useful for any counterparty screening, including the legal entities behind a VASP relationship. Not built for automated or batch screening.

OpenSanctions — OpenSanctions Datenbanken GmbH
https://www.opensanctions.org
An open, aggregated database of several hundred sanctions, PEP, and other watchlist sources, free for non-commercial use with a paid API and license for commercial deployment. A transparent, independent alternative or supplement to the large commercial vendors for the entity-level screening layer.

World-Check — LSEG (London Stock Exchange Group)
https://www.lseg.com/en/risk-intelligence/financial-crime-risk-management/sanctions-screening
One of the two dominant curated sanctions and PEP screening datasets across financial-crime compliance generally, covering several hundred sanctions programs. Screens the corporate and individual entities behind a VASP relationship, distinct from and complementary to blockchain-native address screening.

Dow Jones Risk & Compliance — Dow Jones
https://www.dowjones.com/professional/risk/
The other of the two dominant curated screening datasets, covering sanctions, PEP, and adverse media, with specific content addressing indirect ownership exposure under the 50% Rule. Used as an underlying data source by several of the vendors in section C as well as directly by compliance teams.

Appendix: Use Cases for Sections C, D, and E

The synopses above describe what each tool does. What follows is how that plays out in practice, for the tools in sections C, D, and E specifically, since those are the ones most often described only by their feature list. Each numbered item is an illustrative scenario grounded in the tool's documented capabilities, not a reported case, except where noted otherwise.

C. Commercial blockchain analytics and compliance platforms

Chainalysis

1. A customer deposits funds at your exchange. Before the deposit is credited, KYT checks the funds' origin against Chainalysis's dataset of sanctioned addresses, darknet markets, and other high-risk sources, and flags anything with a match so the deposit can be held or escalated before the funds ever hit the customer's balance. This is real-time, transaction-level screening, running automatically on every deposit.
2. A theft is publicly reported at another exchange and the stolen funds start moving through addresses your compliance team doesn't recognize. Reactor lets an investigator trace those funds across wallets and chains, visualize the flow, and produce a report suitable for law enforcement or an internal escalation, the same workflow Chainalysis used publicly to help trace the Bybit theft. This is investigative and post-incident, typically resolved over hours to days depending on how far the funds have already moved.

Elliptic

1. A customer requests a withdrawal to an external address. Lens screens that destination address in real time and returns a risk score; if the address is on a sanctions list or otherwise high-risk, the withdrawal can be blocked before it settles rather than investigated after the fact. This is real-time, pre-settlement screening.
2. Your institution is considering a new correspondent relationship with an overseas exchange. Discovery assesses that exchange's own compliance posture, licensing, and historical exposure to illicit activity before you commit to the relationship, the VASP-level counterparty due diligence a Travel Rule relationship depends on. This is a one-time or periodic due diligence pull, not a per-transaction check.

TRM Labs

1. Funds tied to a suspicious deposit passed through a cross-chain bridge on their way to your platform, and a single-chain screening tool would lose the trail at that point. TRM Forensics follows the bridge's mint and burn events to reconstruct the full path across chains, so the investigation doesn't stop at the chain boundary. This is investigative, typically resolved same-day to a few days depending on how many hops and chains are involved.
2. Your bank is launching a crypto custody product and needs every wallet under custody screened continuously, not just at onboarding. TRM Wallet Screening re-screens the existing book against current sanctions and risk data and alerts when a wallet's status changes. This is ongoing, automated monitoring rather than a point-in-time check.

Crystal Intelligence

1. Your VASP operates under MiCA and needs to apply the EU's specific €1,000 Travel Rule threshold correctly across every transaction, not a generic figure. Crystal Expert applies jurisdiction-specific threshold logic automatically as part of its screening, so the right rule is applied without a compliance analyst manually checking the transfer amount against the applicable regime each time. This runs continuously as part of standard transaction processing, not as a separate periodic exercise.

D. Travel Rule compliance

Notabene

1. Your exchange is about to send a transfer above the applicable threshold to a customer at another exchange. Before the transfer goes out, Notabene identifies the receiving VASP, confirms it can actually receive and handle the required originator and beneficiary information, and transmits that data securely alongside the transfer. This is a pre-transaction check that happens in the seconds before a transfer is sent, not an after-the-fact filing.
2. A counterparty VASP sends your exchange a Travel Rule data request for an inbound transfer your customer initiated. Notabene routes that request to your team, validates the data against your own risk rules, and lets you respond or flag it for manual review within the same dashboard used for outbound transfers. This is transactional and typically resolved within the settlement window, though a flagged request can take longer if it needs manual review.

E. Smart contract and DeFi security auditing

CertiK

1. Before your company integrates with or lists a new DeFi protocol, you want to know whether its underlying smart contract has been independently reviewed. CertiK's public Security Leaderboard shows whether the protocol has been audited, by whom, and what was found, a one-time or periodic due diligence check done before you commit to the relationship rather than something run per transaction.
2. Once your company already relies on a protocol, a live exploit somewhere in its contracts would be a very different kind of emergency than a screening alert. CertiK's Skynet and Security Oracle products monitor deployed contracts in real time and can flag anomalous on-chain activity as it happens, giving your team a chance to react while an incident is still unfolding rather than learning about it after the fact.

A closing note on how to use this: no single item above, free or paid, is sufficient by itself. The tools that work best in practice combine address- and transaction-level blockchain screening (to catch what's moving on-chain), entity-level sanctions and beneficial-ownership screening (to catch the people and companies behind a wallet), and Travel Rule infrastructure (to make sure the counterparty on the other end of a transfer is who it claims to be), because each catches a different piece of the same underlying evasion pattern. Privacy coins and, for now, the legal reach of sanctions over autonomous smart contracts are the two places where no combination of tools fully closes the gap; knowing where those limits sit is as important as knowing what the tools can do.