ALDERLUX

THE INSIDER · FOUNDATIONS · #0015

# What a Review Actually Consists Of

9 September 2026

The previous issue set out that exchanges read the history of the coins you send them. This one is about what happens next: how a flag is generated, what a review consists of, why nobody will tell you what triggered it, and what a holding structure looks like when it is designed so that one flag cannot reach everything.

# What a Review Actually Consists Of

## In brief

- Screening is probabilistic, not binary. Analytics firms assign risk scores to addresses and clusters, and exchanges set their own thresholds against those scores. Two exchanges can read the same deposit differently.
- Taint propagates through transaction graphs by rules the holder cannot see and did not agree to, and different methods produce materially different answers about the same coins.
- A review has three possible characters — automated hold, manual compliance review, or a law-enforcement matter — and they are not distinguishable from the outside, which is why the answers are vague.
- Separation is the whole defence. Not secrecy, not evasion: the ordinary practice of not putting everything through one counterparty.

## Part one: how a flag is generated

### The scoring layer

Transaction analysis is a licensed product. Exchanges buy it rather than build it. Blockchain analytics providers maintain databases that map addresses to entities — exchanges, mining pools, darknet markets, sanctioned entities, mixing services, gambling sites, ransomware wallets — and assign risk characteristics to each.

This mapping is built from a mixture of public information, subpoenaed records, exchange cooperation, purchased datasets, and heuristics that infer common ownership from spending patterns. Some of it is highly reliable. Some of it is inference presented with more confidence than the underlying evidence supports.

Three things follow from that, and they matter more than the general fact of screening.

**Attribution can be wrong.** An address labelled as belonging to a particular service is a claim, not a fact on the ledger. Clustering heuristics group addresses by inferred common ownership, and inference is fallible. In practice a holder has no direct route to see or challenge the label applied to their history, because the attribution sits with a vendor rather than on the ledger.

**The labels are retroactive.** When a platform is designated or a hack is attributed, the analytics database updates. Coins that produced no risk flag last month can produce one this month without anything about them having changed. Screening is applied to history, so the update reaches backwards.

**Different vendors disagree.** Exchanges can use different providers, datasets, clustering and thresholds, so the same deposit may produce different outcomes at different venues. This is not a scandal; it is what happens when a probabilistic method is sold as a product. But it means “clean”

is not a property of a coin. It is a property of a coin, a vendor and a threshold, at a moment in time.

## How taint travels

The question every holder eventually asks is: how far back does this go?

There is no single answer, because there is no single method. Different analytical models can treat indirect exposure differently, and commercial systems combine several signals — entity attribution, clustering, exposure category, confidence scoring, temporal and behavioural analysis — rather than applying one rule. What follows is a simplified illustration of why two defensible methods can reach different conclusions about the same coins, not a description of any particular provider's model.

**Proportional tracking** treats a mixed output as carrying a proportional share of each input's characteristics. Send one flagged coin and nine unflagged into a transaction, and every output carries ten per cent of the flag.

**Ordering rules** — first-in-first-out, or last-in-first-out — treat outputs as drawn from inputs in a stated sequence. These produce different answers from proportional tracking on the same data, sometimes dramatically so, and which is applied is a policy choice rather than a fact.

**Hop-limited tracing** stops after a set number of transactions. Beyond that distance the association is treated as too dilute to act on. Where that limit sits is set by the vendor or the exchange, and it is not published.

The practical consequence is that a holder cannot reliably predict how an exchange will assess their exposure. The transaction data is public and anyone can analyse it; what is not available is the provider's attribution, its clustering, the exchange's thresholds and its internal policy. Two defensible methods applied to the same coins can return "negligible" and "significant." Anyone who tells you your coins are clean is telling you which method they used, whether they say so or not.

## What actually triggers the flag

In broad terms, three categories.

**Direct exposure.** The deposit came from, or recently passed through, an address associated with a sanctioned entity, a hacked platform, a darknet market or a mixing service. This is the clearest case and the one exchanges act on most decisively.

**Indirect or aggregate exposure.** No single link is damning, but the accumulated association across the history crosses a threshold. In our advisory work this is the category that surprises people, because nothing in the recent history looks wrong.

**Behavioural signals unrelated to the coins.** Deposit patterns, a mismatch between stated source of funds and observed activity, structuring-like behaviour, a login from an unexpected jurisdiction, or a name matching a screening list. These have nothing to do with transaction history at all, but they surface identically to the holder.

The holder cannot tell which of the three applies. That is not evasiveness on the exchange's part — see below — but it is the reason the experience is so disorienting.

## Part two: what a review consists of

### Three different things wearing the same face

From the outside, a restriction looks like one event. Internally it can be one of three, and they behave completely differently.

**An automated hold.** A threshold was crossed and the system acted. No human has looked at it. Because no human has yet examined it, this is the category that can clear without the holder doing anything — on a queue the holder cannot see.

**A manual compliance review.** A person is examining the account: the deposit, the history, the account's own activity, and whatever the holder has provided about source of funds. This is where source-of-funds documentation matters and where a well-prepared response can materially change the outcome.

**A law-enforcement matter.** A request, order or notice from an authority. Here the exchange's obligations run primarily to the authority rather than to the customer, and in some jurisdictions the exchange may be prohibited from disclosing anything at all — including that a request exists.

That third category can explain the vagueness. Where disclosure restrictions apply, a compliance team saying "this is not a law-enforcement matter" in the cases where it is not would, by elimination, disclose the cases where it is. A uniform non-answer may therefore be a structural requirement rather than poor service. That will not be true of every restriction at every venue, but it is worth assuming before concluding you are being fobbed off — and it stops you spending effort trying to extract information nobody may be permitted to give.

### What a compliance team is actually asking

Where a human review is under way, the questions behind it are consistent:

- Where did these assets originate, and can it be evidenced rather than asserted?
- Is the account's activity consistent with what the holder said it would be?
- Does the transaction history support the stated purpose of the account?
- Is there a plausible innocent explanation for the association that triggered this?

The last one matters. A review is not a determination of guilt; it is a request for a coherent account. A holder who can produce one — purchase records, exchange statements, wallet histories, dates, counterparties — is answering the question being asked. A holder who cannot is asking the reviewer to take an assertion on trust.

### What a holder can actually do

Little, but not nothing.

**Provide documentation once, completely.** Incomplete responses can delay a review by prompting further requests for information. Assemble everything before responding: acquisition records, prior exchange statements, the wallet path, and dates.

**Answer the question asked.** Compliance reviews are not persuasion exercises. Volume of correspondence does not help and can extend the process.

**Escalate through the stated channel, in writing.** Public complaint sometimes accelerates matters, but it is unpredictable, it can harden a position, and it puts the holder's affairs in public — which is a poor trade for anyone holding meaningful value.

**Know the regulatory route.** Where an exchange is licensed, its regulator has a complaints process. Whether that helps depends entirely on the jurisdiction and the character of the review, and it should be a considered step rather than a first response.

**Accept the timeline.** In our advisory work the costliest error is making decisions — moving other assets, opening accounts elsewhere in a hurry, sending further deposits to the same venue — under time pressure, during a period when nothing can be resolved anyway.

## Part three: structure

This is the part that actually reduces exposure, and it is worth being precise about what is being proposed. Nothing here is about concealment, and none of it is about defeating screening. It is the same principle that governs not banking your entire estate with one institution: **separation, so that one event cannot reach everything.**

### The four principles

**Separate function from storage.** An exchange account is an operational tool — it converts, it provides liquidity, it handles fiat. Everything on it should be there for a reason and for a period. The balance you would be materially harmed to lose access to for thirty days is the wrong balance to hold there.

**Separate provenance.** Assets with different histories, from different sources, held through different arrangements, are not exposed to the same flag. Where coins acquired from an unverifiable source and coins acquired through a documented purchase sit in the same place, the first carries risk to the second.

**Separate counterparties.** Different exchanges use different analytics vendors and different thresholds. This is not a reason to spread balances everywhere — more accounts means more surface — but it is a reason not to have a single venue as the only route between your assets and the banking system.

**Document at acquisition, not at review.** This is the highest-return item on the list, and the one that requires acting before there is a problem. The moment to record where an asset came from is when you acquire it, while the counterparty, date, rate and route are all available. Reconstructing that history years later, under time pressure, with an account already restricted, is a materially harder task — and for older holdings it is sometimes impossible.

### What this looks like in practice

For most holders the working shape is simple:

- A small operational balance on a platform, sized so that losing access for a month is an inconvenience rather than an event.
- The substantive holding self-custodied, where no third party is positioned to act on what the ledger shows.
- Provenance records kept for everything, in a form somebody else could follow.
- Where amounts justify it, arrangements requiring more than one party to move assets — which addresses a different risk, but is built at the same time.

For families and businesses the shape is the same and the documentation burden is higher, because the person who can explain where the assets came from may not be the person who eventually has to.

### What structure does not do

Structure does not make coins clean. It does not defeat screening, and it will not help anyone whose assets genuinely originate in an unlawful source — nor should it.

What it does is limit the blast radius of a decision made by a third party using a probabilistic method against a database you cannot inspect, about coins you may have acquired in good faith years ago.

That is a narrower claim than the industry usually makes, and it is the true one.

## The View From The Edge

The uncomfortable observation in all of this is that the screening industry has quietly introduced a property that Bitcoin was specifically designed not to have.

A bearer asset is one where possession is the whole of the claim. That is the point of holding one: no counterparty, no permission, no view taken by anyone else about whether you are entitled to it. But an asset that must eventually pass through a regulated venue to become spendable in the ordinary economy is not purely a bearer asset. At the boundary, it acquires a history, and the history is read.

So there are effectively two Bitcoins now, and the difference is not technical. Held yourself, it behaves as designed — the history exists, and nobody is positioned to act on it. Presented to a regulated venue, it becomes an asset whose acceptability is determined by a third party applying a method it does not disclose, against a database it did not build, using a threshold it sets itself.

Neither of those is wrong. Sanctions compliance is a legal obligation and exchanges are right to meet it. But the two states are genuinely different, and most holders have never noticed they are moving between them.

The practical conclusion is not to avoid exchanges. It is to be deliberate about the boundary — to know when you are crossing it, to cross it with assets whose history you can account for, and to keep the crossing narrow enough that a decision made on the other side cannot reach everything you own.

Where the amounts justify building that structure properly — and building it alongside the succession arrangements it overlaps with — that is what Succession is for.

## Basis and limits

This issue describes screening and compliance practice at custodial exchanges, drawn from published analytics methodology, the public record of sanctions designations, and how these processes are documented to operate. It names no platform and no vendor.

It is not a study. No figure is given for how often accounts are restricted, how long reviews take, or how frequently attribution is wrong, because those figures are not published and we have not measured them. Where the text describes what typically happens, read it as a description of how the process is structured rather than a rate we have established.

The description of how risk association propagates through a transaction graph is a simplified illustration written to show why different methods can reach different conclusions. Commercial monitoring systems are more complex than the three approaches named, and no provider's model is described here.

Practice varies by exchange and by jurisdiction, and both change. Nothing here is specific to any platform, and anything that matters to a decision should be checked at the time it matters. Where a review involves law enforcement, or where assets are already restricted, that is a question for a solicitor rather than for us.

**Alderlux advises families and businesses on Bitcoin custody and succession, so we have a commercial interest in this problem being taken seriously.** The principles above you can apply without us.

## Sources

The regulatory framework described in this issue is set out in the following primary material. Nothing in the sources below describes any particular provider's methodology, which is proprietary and not fully published.

- Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2021)
- Financial Action Task Force, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (seventh update, 16 July 2026)
- Financial Conduct Authority, *Cryptoassets: AML / CTF regime*
- Financial Conduct Authority, *Money laundering and terrorist financing*
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, as amended

---

Alderlux provides education and information only. We do not provide regulated financial advice, investment recommendations, legal or tax advice. Alderlux is not authorised by the Financial Conduct Authority.