ALDERLUX

THE INSIDER · INVESTIGATIVE · #0025

Guard Rails After the Binance Theft: Which UK Protections Would Work, and What Each Leaves Out

1 NOVEMBER 2026

After the theft of about $6.3bn from Binance's hot wallets on 29 October 2026, we assessed seven possible guard rails for British crypto holders against the published record. The UK regime that starts on 25 October 2027 strengthens protection against a firm failing or mishandling client assets: authorisation with a UK presence, client assets held on trust and kept separate, resilience expectations for key management, and access to the Financial Ombudsman. It does far less against theft itself. The sources we examined establish no general guarantee that stolen client assets will be replaced; whether an individual customer has a contractual or other legal right to reimbursement depends on the firm's terms and the circumstances of the loss. The FCA does not plan to extend FSCS cover to cryptoasset activities, proof of reserves shows one moment, and Binance's own make-whole promise rests on its discretion and balance sheet. Holding one's own keys removes the platform from the picture but moves the security burden to the holder.

The question

After what news reports called a record theft from an exchange [6], which protections for UK holders are available or coming, which risks does each address, what evidence is there that it works, and where does it stop?

Method and sample window

We read the legislation that creates the UK regime, the FCA's final-rules overview and two pieces of FCA finalised guidance, the FCA's consumer guidance and its warning on the Binance Group, Binance's own incident statement and fund pages, a US audit regulator staff advisory on proof of reserves, and news reports from 29 October to 1 November 2026. Where we could not read FCA policy statements in full, we relied on law-firm summaries and say so. Sources were accessed on 1 November 2026. The new UK regime is not yet in force, so its effectiveness cannot be assessed from operating experience. We assess what its rules are designed to protect, what they require, and what their published limitations are. We did not contact Binance, the FCA or anyone named.

How the theft was carried out is covered in Insider #0024 [24]; the difference between assets held for you and held by you in Insider #0021 [25]. This piece is about protections.

The starting point

Binance said its hot wallets were compromised at about 20:05 UTC on 29 October, with a loss of about $6.3bn, that it had found no evidence that wallet private keys were leaked, and that about $3bn had been frozen on-chain. [1] It stated: "Binance will absorb the financial impact of these stolen funds, not our users." [1] By 1 November it was reported to have covered 95% and to be restarting withdrawals in phases. [7] The FCA's warning on the Binance Group, last updated in June 2023, states that Binance Markets Limited is no longer authorised by the FCA and that no other entity in the Binance Group holds any form of UK authorisation, registration or licence. [8]

Guard rail 1 — Authorisation, with a presence in the UK

Risk addressed: firms serving UK customers from outside UK supervision. **What exists:** the Cryptoassets Regulations 2026 come into force on 25 October 2027, with some preparatory provisions earlier. [18][19] The FCA's guidance on international firms says it expects firms seeking authorisation for cryptoasset activities to have a presence in the UK, with a UK legal entity as the baseline; generally it does not expect a UK branch alone to meet its minimum standards, and it expects firms safeguarding client cryptoassets to operate from a UK subsidiary, except for a trading platform's settlement wallet. [20] The FCA says it is particularly concerned about the risk of harm if an international firm safeguarding client cryptoassets fails. [20] **Limits:** the same guidance notes that some international firms may not require UK authorisation, depending on their activities and UK customer base. [20] Whether any Binance entity will seek or obtain authorisation

is not known; a CoinTurk News report, citing unnamed reports, said Binance may seek FCA approval for 2027, and Binance declined to comment on speculation about licence applications. [16]

Guard rail 2 — Client assets held on trust and kept separate

Risk addressed: customers' assets being mixed with the firm's and caught up in its failure. **What exists:** the FCA's overview says PS26/11 includes the safeguarding requirements in CASS 17 for cryptoasset custodians, and that respondents strongly supported enhanced protections around ownership rights, record-keeping, reconciliation and private-key management. [10] Simmons & Simmons' summary records that client cryptoassets must be held on a non-statutory trust, be separately identifiable and not be mixed with the firm's own assets, with listed exceptions including a settlement float: a qualifying cryptoasset trading platform may hold up to 2% of each client's cryptoassets, per client and per cryptoasset class, outside the trust for settlement. [12] Freshfields records that firms must immediately notify clients affected by a shortfall. [13] The FCA's stated aim when consulting was that clients' assets should be returned as quickly and as whole as possible if a custodian enters an insolvency process. [11] **Limits:** a trust protects ownership in a failure; it does not stop a theft or refill a hacked wallet. We could not confirm from the FCA's own text whether, or how quickly, a firm must make good a shortfall from its own resources. Whether a customer could claim against a firm for a theft would turn on the firm's terms and the circumstances, which we did not test.

Guard rail 3 — Resilience expectations for key management and cyber incidents

Risk addressed: the operational failure behind a theft. **What exists:** the FCA's operational-resilience guidance for cryptoasset firms describes private-key security risk as the risk of unauthorised access to private keys, and expects firms holding keys to have secure processes for key loss, unauthorised access and disruption. It gives multi-party computation, multisignature and cold and warm wallet segregation among examples of emerging practice, and says these tools should be used in a way that avoids centralising risks. [21] It expects firms to conduct penetration testing and to include cyberattacks in scenario testing, to promptly notify affected clients and stakeholders after a cyber breach, and to notify the FCA of any failure to meet an impact tolerance. [21] **Limits:** this is guidance, and Freshfields records that the FCA is technology-agnostic on private-key management rather than prescribing a wallet design. [13][21] On Binance's own account, it found no evidence that private keys leaked; its initial investigation suggested a compromised laptop, and later investigation found additional points of breach. [1] Expectations about how keys are stored address part of that picture; what a signing system can be made to approve is examined in Insider #0024. [24]

Guard rail 4 — Capital

Risk addressed: a firm's ability to absorb losses without failing. **What exists:** the FCA's overview says the final package introduces two prudential sourcebooks for cryptoasset firms, COREPRU and CRYPTOPRU, which it describes as the "overall prudential framework for cryptoasset firms". [10] The FCA overview lists components of the prudential framework including stablecoin issuance, market and counterparty risk, and public disclosure, and refers to a firm's fixed overheads requirement, K-factor requirement and permanent minimum requirement. [10] **What capital is for, and what it is not:** capital rules concern a firm's own financial resources. They are a measure of how much the firm itself must hold against its risks; they are a different thing from the safeguarding rules, under which client cryptoassets are held separately on trust under CASS 17. [10][12] The FCA overview we examined does not identify a specific capital requirement earmarked for replacing stolen client assets. We have not read PS26/12 in full, so this should not be taken as confirmation that no relevant obligation exists elsewhere in the rules. [10] One of the outcome measures the page lists is firms using own funds "to restore consumer positions where they are liable for harm"; the page describes that as a measure of success, not a rule, and it depends on the firm being liable. [10] **Limits:** we did not test whether the capital these rules require would absorb a loss on the scale of this theft. A firm that meets its capital requirement is not thereby protected against, or obliged to compensate for, theft of customer assets.

Guard rail 5 — Compensation and complaints

Risk addressed: a customer left out of pocket. **What exists today:** the FCA's consumer guidance says access to the FSCS and the Financial Ombudsman depends on the firm being authorised and the service involving a regulated activity that is covered, and that people investing in crypto are unlikely to have access to either if something goes wrong. [9] **From October 2027:** the FCA's policy statement on applying its Handbook says most firms carrying on regulated cryptoasset activities will be subject to requirements including dispute resolution and access to the Financial Ombudsman Service. [17] In PS26/13 the FCA says "We do not plan to extend FSCS cover to new regulated cryptoasset activities", adding that it is too early to identify clear benefits and to assess fully the wider risks [17]; Simmons & Simmons' summary is consistent with this [14], and Val Smith of the FCA was reported in October 2026 as saying the regime does not include FSCS access. [15] **Limits:** the ombudsman decides complaints about firms' acts or omissions [14]; it is not insurance against the failure of a crypto business, and the FCA does not plan to introduce FSCS cover for these activities [17]. The FCA says a complaint is likely to be upheld if the Ombudsman finds that the firm has acted in a way that has caused loss to the consumer [17]; a complaint can lead to redress where the Ombudsman upholds it, but this is not automatic protection against losses caused by theft, and we did not test how a theft complaint would be decided.

Guard rail 6 — Voluntary make-whole funds

Risk addressed: customer losses from a theft. **Evidence it can work:** this is the guard rail Binance says it is deploying in response to the theft. Binance said it had set aside more than $6.34bn of company funds, of which $5bn was held in the same tokens that were stolen, and that it had "already covered approximately 80% of the impacted amount" while it bought the remaining 20%. [1] It said it drew on its corporate treasury, part of its futures insurance fund and the portion of its Secure Asset Fund for Users (SAFU) above the fund's required size. [1][4] **Three figures that should not be read as one.** (1) Funds *set aside*: more than $6.34bn, as Binance describes it. [1] (2) Losses *covered*: Binance's own measure of how much of the loss it has made good, reported as about 80% in its update, 90% by CoinDesk on 31 October (with the remaining 10% in less liquid tokens) and 95% by The National on 1 November. [1][4][5][7] These are Binance's figures for covering the loss from its resources; none of the sources we read describes them as stolen coins being recovered. (3) Funds *frozen*: about $3bn, reported as frozen on-chain, separate from the amount set aside. [1][4] None of these establishes that customer balances have been restored or that customers have received replacement assets, and we have not seen independent confirmation of any of the figures. **Limits:** Binance's SAFU FAQ describes a fund of about $1bn [2] [3] and says Binance keeps full discretion over which types of loss and which claims are eligible, and may change how the fund is used; the cover it says may be included concerns compromise of a user's account login credentials through a deficiency in Binance's systems. [2] Using it here goes beyond what the FAQ describes, to customers' benefit — but it is a choice, and its size depends on the firm. We could not read Binance's terms of use, so we cannot say what its contract promises.

Guard rail 7 — Proof of reserves

Risk addressed: an exchange holding less than it owes. **What had been published by 1 November:** per CoinDesk, a reserves snapshot taken at midnight UTC on 31 October showing coverage ratios of 100% or more for ten named tokens. Binance had said it planned results by 2 November. The full cryptographic proof, which would let customers check that their balances are included in Binance's reported liabilities, was reported as expected by 3 November. [1][4] We did not see that full proof, so we cannot say whether it was published, or what it shows. **Limits:** staff of the US audit regulator's Office of the Investor Advocate warned in 2023 that "PoR engagements are not audits", that such reports reflect one point in time, that their procedures likely do not address the entity's liabilities, that they may not reveal whether assets were borrowed, and that they typically do not address holders' rights and obligations. [22] CoinDesk reported that wallets drained in the theft had been listed in Binance's earlier reserve disclosures as backing user holdings [4] — consistent with hot wallets forming part of reserves. Those disclosures were not evidence that the wallets were secure or that the firm could withstand a theft: a snapshot shows what was held, not how securely.

And outside the regime — holding one's own keys

Holding bitcoin oneself removes reliance on a platform's solvency, security and promises, but transfers responsibility for key security, recovery and transaction management to the holder; it does not remove risk. One reported London case shows the personal-security side. In August 2026, by his account to CoinDesk, a man's unlocked phone was taken in Hackney after two men had seen him enter his passcode; within hours crypto was moved from a self-custody wallet app, another wallet and an exchange account were accessed, and card payments were made, with losses he estimates at about $14,000. [23] It is a single case, and its lesson concerns how keys and app access were protected on a phone, not self-custody as such. We found no reliable UK figures on how often holders are targeted this way.

Summary

GUARD RAIL	MAIN RISK IT ADDRESSES	AVAILABLE TO UK CUSTOMERS OF AN UNAUTHORISED OVERSEAS EXCHANGE?	WHAT IT DOES NOT DO
Authorisation with UK presence	Unsupervised firms	No; future protections depend on the firm obtaining the required authorisation and being within the regime's scope	Reach firms outside scope
Trust and segregation (CASS 17)	Firm failure, mixing of assets	No; future protections depend on the firm being authorised and within scope	Prevent theft, or of itself reimburse it
Resilience and key management (FG26/6)	Operational and cyber failure	No; guidance for firms within the regime's scope	Prescribe a design; guarantee prevention
Capital (PS26/12)	Firm absorbing losses	No; future protections depend on the firm being authorised and within scope	Earmark capital for stolen client assets (not shown) [10]
Ombudsman access	Firm acts or omissions	Unlikely [9]; for most firms carrying on regulated cryptoasset activities, from 25/10/2027, subject to scope and eligibility [17]	Act as insurance
FSCS	Firm unable to pay	Unlikely [9]	FCA does not plan to extend it to crypto [17] [14][15]
Voluntary make-whole fund	Theft losses	Depends on the firm	Bind the firm (terms reserve discretion) [2]
Proof of reserves	Under-reserving	Binance's proof-of-reserves disclosures are voluntary; no equivalent general protection is established here	Show liabilities, continuity or legal rights [22]

Questions to put to an arrangement

Questions a holder or family can put to any arrangement, drawn from the findings:

- **Which entity holds the assets, and is it on the FCA register?** Whether the firm is authorised, and whether the service is a regulated activity, decides whether the ombudsman can be available from October 2027. [9][17]
- **Are client assets held on trust and kept separate?** [12]
- **If the firm promises to cover losses, from what, of what size, and at whose discretion?** [2]

- **Does any proof of reserves include liabilities, and how often is it repeated?** [22]
- **For keys held personally: what could someone do with this phone, this passcode or this backup?** [23]

The case for the opposing view

A fair counter-argument is that the most substantial reported response to the theft this week was not a rule at all. Binance reported covering most of the loss from its own resources — 95% by 1 November, on The National's report — and about $3bn frozen on-chain, a separate matter from the cover. [1][7] Rules on trust status and capital would not by themselves have done that, and no rulebook can stop a determined state-linked attacker; the FBI attributed the theft to a North Korean group. [6] On this view, scale and willingness matter more than regulation. The argument has force for customers of a very large, well-capitalised exchange. Its limit is that it depends on capacity and goodwill at the moment of loss, which a customer cannot verify beforehand from published terms that reserve discretion. [2] Regulation's contribution is narrower but enforceable: who holds what, on what terms, and who to complain to.

Conclusion

The UK guard rails arriving in October 2027 are aimed mainly at firm failure and firm conduct: they settle ownership, require separation and reconciliation, set resilience expectations and open the ombudsman to customers of most authorised firms. The FCA does not plan to extend FSCS cover to cryptoasset activities, and the sources we examined establish no general guarantee that stolen client assets will be replaced; whether a given customer has a right to reimbursement depends on the firm's terms and the circumstances of the loss. Against theft itself, the protections we found are voluntary — a firm's own fund and balance sheet, and disclosures such as proof of reserves — or personal, in the form of holding one's own keys and protecting them. Whether a given protection "works" depends on which risk a holder is guarding against.

The View From The Edge

Most of the new rules are about failure, not theft. That is not a weakness of the regime; it is a description of what it is for. The useful question is which risk each protection covers.

The FCA does not plan to bring FSCS protection to crypto. The Financial Ombudsman may provide a route to redress where a firm is responsible, but it is not insurance. A trust protects what is yours if a firm fails; it does not pay anyone back if the coins are gone.

Self-custody is a security discipline, not an exit from risk. A phone can be the weakest link.

Related: Insider #0021, Held for You, or Held by You — https://alderlux.com/the-insider/held-for-you-or-held-by-you · Insider #0024, What the Binance Theft Actually Teaches — https://alderlux.com/the-insider/what-the-binance-theft-actually-teaches · Alderlux Succession — https://alderlux.com/succession

Basis and limits

This examines published rules, guidance and statements as at 1 November 2026; it is not a legal opinion on any customer's rights. We could not open the press report that described calls for "guard rails", so no proposal is attributed to anyone. The FCA's policy statements PS26/11 (safeguarding) and PS26/12 (prudential) were not read in full, and PS26/13 was read only in Chapter 12 (dispute resolution and compensation); points on trust status, shortfalls and capital rest on the FCA's overview and law-firm summaries, attributed in the text, while the FSCS and Ombudsman points rest on PS26/13 Chapter 12 (paras 12.3 and 12.29 and the response at pp. 60 and 67). We could not read Binance's terms of use, and have not checked the final text against the unread policy statements. The FCA statement on the Binance Group's UK status dates from June 2023 and the FCA register was not checked. Binance's coverage figures come from Binance's posts as reported and were changing daily; we have not seen independent confirmation, nor the full proof of reserves. We did not test the capital rules against a loss of this size, and found no UK data on how often holders are targeted for their phones or keys. We did not contact Binance or the FCA.

Alderlux advises families on Bitcoin custody and succession, so we have a commercial interest in this problem being taken seriously. Every question above can be put without Alderlux's involvement.

Sources

1. Binance, Security Incident Update #2 (2026-10-30), 30/10/2026 — https://www.binance.com/en/support/announcement/detail/d3306d9dca5243548c813b605e1d1751
2. Binance, Frequently Asked Questions on Secure Asset Fund for Users (SAFU), updated 02/02/2026 — https://www.binance.com/en/support/faq/frequently-asked-questions-on-secure-asset-fund-for-users-safu-028799e730294ae4a9b382d60d350116
3. Binance, SAFU Valued at $1bn, 31/01/2022 (updated 28/03/2023) — https://www.binance.com/en/support/announcement/binance-secure-asset-fund-for-users-safu-valued-at-1bn-9c513d91af3f497b99da2962322fb3c3
4. CoinDesk, Binance says it has replaced 90% of stolen crypto after massive $6.3 billion breach, 31/10/2026 — https://www.coindesk.com/business/2026/10/31/binance-says-it-has-replaced-90-of-stolen-crypto-after-massive-usd6-3-billion-breach
5. Investing.com via Yahoo Finance, 31/10/2026 — https://finance.yahoo.com/markets/crypto/articles/binance-says-replaced-90-6-172646569.html
6. Al Jazeera, FBI blames North Korea for record $6.3bn crypto heist from Binance, 01/11/2026 — https://www.aljazeera.com/news/2026/11/1/fbi-blames-north-korea-for-record-6-3bn-crypto-heist
7. The National, Binance to resume withdrawals after covering 95% of $6.3bn crypto heist, 01/11/2026 — https://www.thenationalnews.com/business/markets/2026/11/01/binance-to-resume-withdrawals-after-covering-95-of-63bn-crypto-heist/
8. FCA, Consumer warning on Binance Markets Limited and the Binance Group, updated 07/06/2023 — https://www.fca.org.uk/news/news-stories/consumer-warning-binance-markets-limited-and-binance-group
9. FCA InvestSmart, Investing in crypto, last updated 29/01/2026 — https://www.fca.org.uk/investsmart/investing-crypto
10. FCA, Overview of our cryptoassets regime policy statements, 30/06/2026 — https://www.fca.org.uk/publications/policy-statements/cryptoasset-regime
11. FCA, Consultation Paper CP25/14, May 2025, para 1.28 — https://www.fca.org.uk/publication/consultation/cp25-14.pdf
12. Simmons & Simmons, PS26/11: Crypto Regime — Regulated Cryptoasset Activities, 21/07/2026 — https://www.simmons-simmons.com/en/publications/cmrvg8szg00cquom8p3dhehn8/ps-26-11-crypto-regime-regulated

13. Freshfields, Set in stone: Five landmark crypto Policy Statements, 21/07/2026 — https://www.freshfields.com/en/our-thinking/briefings/2026/07/set-in-stone-five-landmark-crypto-policy-statements
14. Simmons & Simmons, PS26/13: FCA handbook and regulated cryptoasset activities, 22/07/2026 — https://www.simmons-simmons.com/en/publications/cmrw5av9d00eguom8zhay1jfj/application-of-the-fca-handbook-to-regulated-cryptoasset-activities
15. Scottish Financial News, 12/10/2026 — https://www.scottishfinancialnews.com/articles/fca-urges-crypto-firms-to-prepare-for-regulation-in-october-2027-as-investors-face-no-fscs-safety-net
16. CoinTurk News, 17/08/2026 — https://en.coin-turk.com/binance-to-seek-uk-fca-license-for-relaunch-in-2027-report-claims/
17. FCA, PS26/13 Application of the FCA Handbook for Regulated Cryptoasset Activities, June 2026, para 1.2 and Chapter 12 (paras 12.3, 12.29; responses at pp. 60 and 67) — https://www.fca.org.uk/publication/policy/ps26-13.pdf
18. The Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026, SI 2026/102, reg 1(2)–(3) — https://www.legislation.gov.uk/uksi/2026/102/data.htm
19. FCA, New regime for cryptoasset regulation, updated 30/09/2026 — https://www.fca.org.uk/firms/new-regime-cryptoasset-regulation
20. FCA, FG26/7 Approach to international cryptoasset firms, 30/06/2026, paras 5.3, 6.9, 7.3–7.4, 8.15 — https://www.fca.org.uk/publication/finalised-guidance/fg26-7.pdf
21. FCA, FG26/6 Cryptoasset Operational Resilience, 30/06/2026, risk table at para 2.1 and paras 3.2, 9.6, 10.2, 10.4 — https://www.fca.org.uk/publication/finalised-guidance/fg26-6.pdf
22. PCAOB Office of the Investor Advocate (staff), Investor Advisory: Exercise Caution With Third-Party Verification/Proof of Reserve Reports, 08/03/2023 — https://pcaobus.org/resources/information-for-investors/investor-advisories/investor-advisory-exercise-caution-with-third-party-verification-proof-of-reserve-reports
23. CoinDesk, A stolen iPhone, $14,000 in losses and London's crypto theft problem, 31/10/2026 — https://www.coindesk.com/business/2026/11/01/a-stolen-iphone-usd14-000-in-losses-and-london-s-crypto-theft-problem
24. Alderlux, What the Binance Theft Actually Teaches (Insider #0024), 30/10/2026 — https://alderlux.com/the-insider/what-the-binance-theft-actually-teaches
25. Alderlux, Held for You, or Held by You (Insider #0021), 28/10/2026 — https://alderlux.com/the-insider/held-for-you-or-held-by-you

---

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.