THREAT HUNTER

Mastercard Cross-Border Unauthorized Transaction Analysis

September 2026

Threat Hunter · Anti-Fraud Intelligence Research

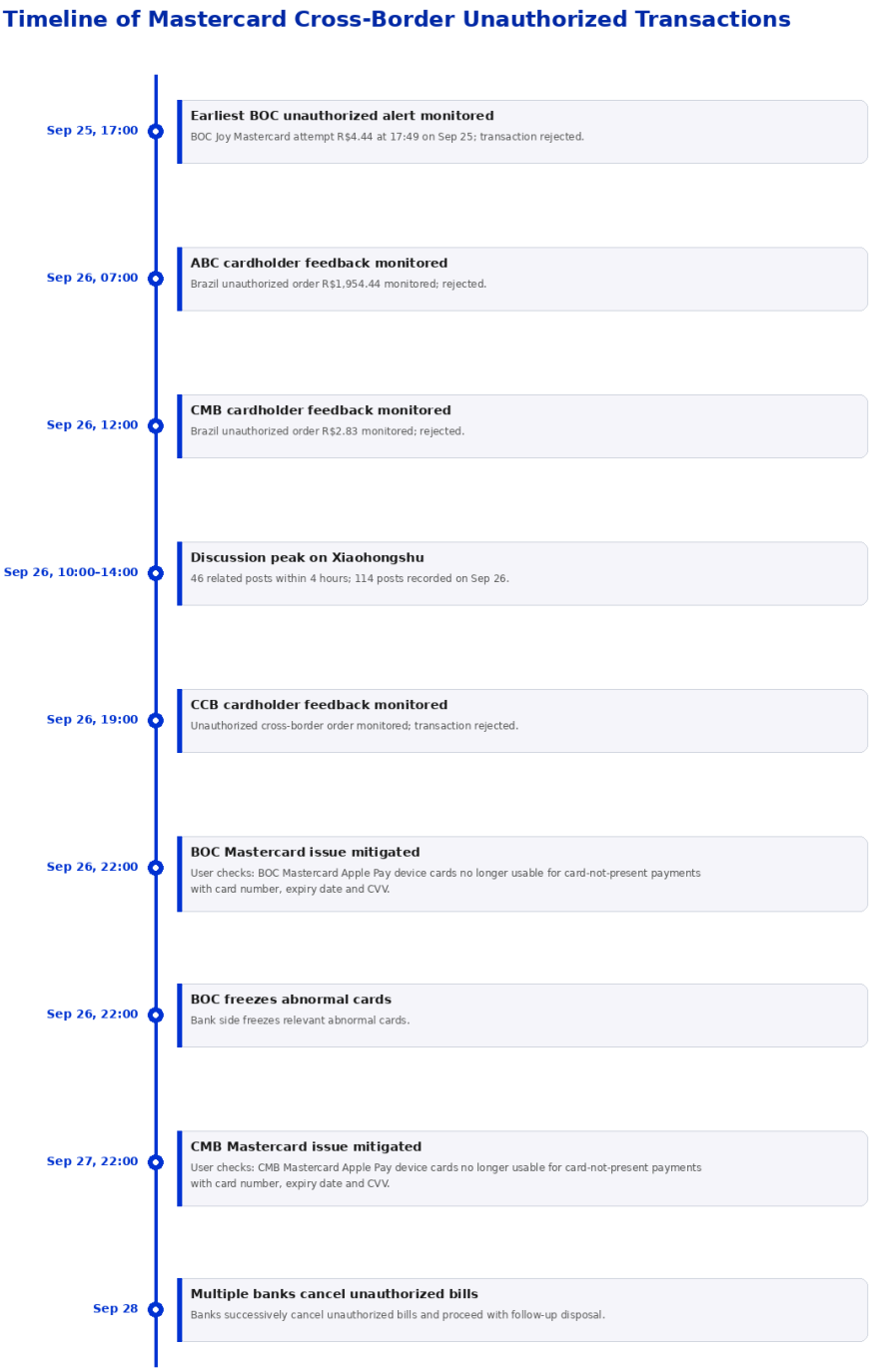


Around 25 September 2026, multiple Mastercard cardholders in mainland China reported receiving alerts for cross-border unauthorized transactions—often involving Brazil and related currencies such as Brazilian real and Uruguayan peso—while they had not traveled abroad, had not made the related purchases, and still held their physical cards. Some alerts occurred in the early morning hours, with amounts reaching several thousand Brazilian reais. Some transaction records indicated a link to Apple Pay.

As similar cases clustered, public information showed that the anomaly was not limited to a single bank or card product: Mastercard credit cards from multiple issuers saw unauthorized cross-border spending. Some attempts were intercepted in time by bank risk controls; others posted successfully and moved into investigation and fund-recovery processes. When “sitting at home while a foreign bill arrives” reappeared at scale, Threat Hunter opened a dedicated intelligence review. This brief focuses on the technical means attackers may have used, and—together with payment-channel abuse and cross-border monetization activity—reconstructs a plausible end-to-end attack chain for this Mastercard unauthorized-transaction event.

I. Anomalous Transactions Clustered Across Multiple Banks in a Short Window

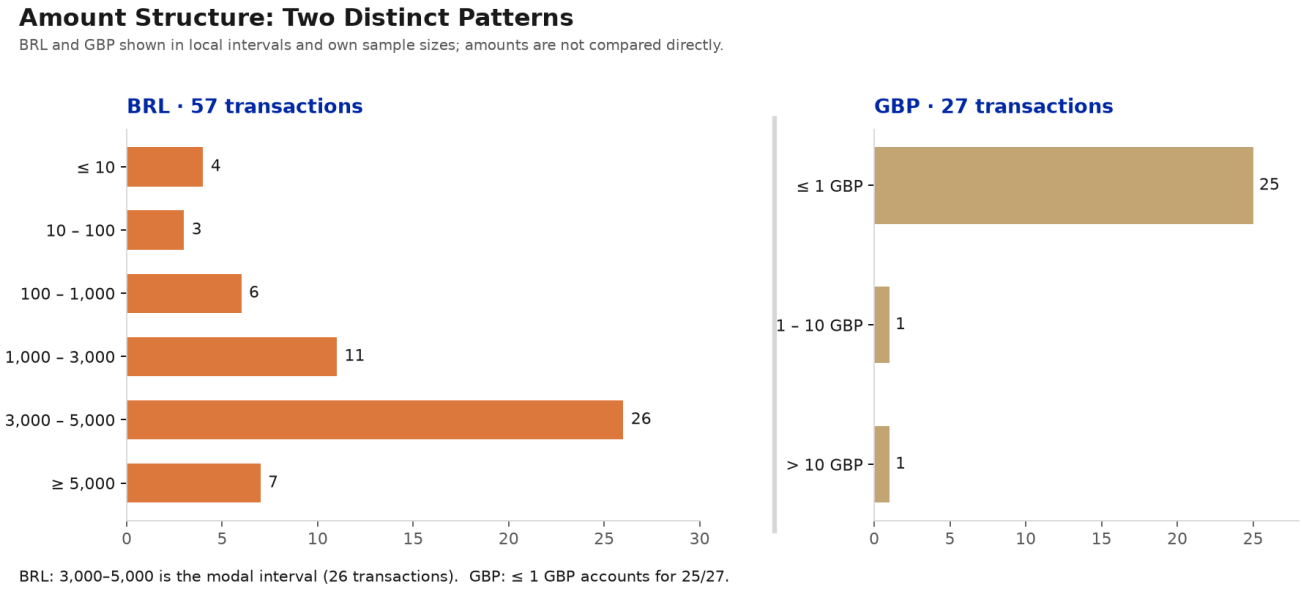
Based on public feedback monitored by Threat Hunter to date, anomalous transactions concentrated rapidly between 25 and 26 September. The related timeline is as follows:

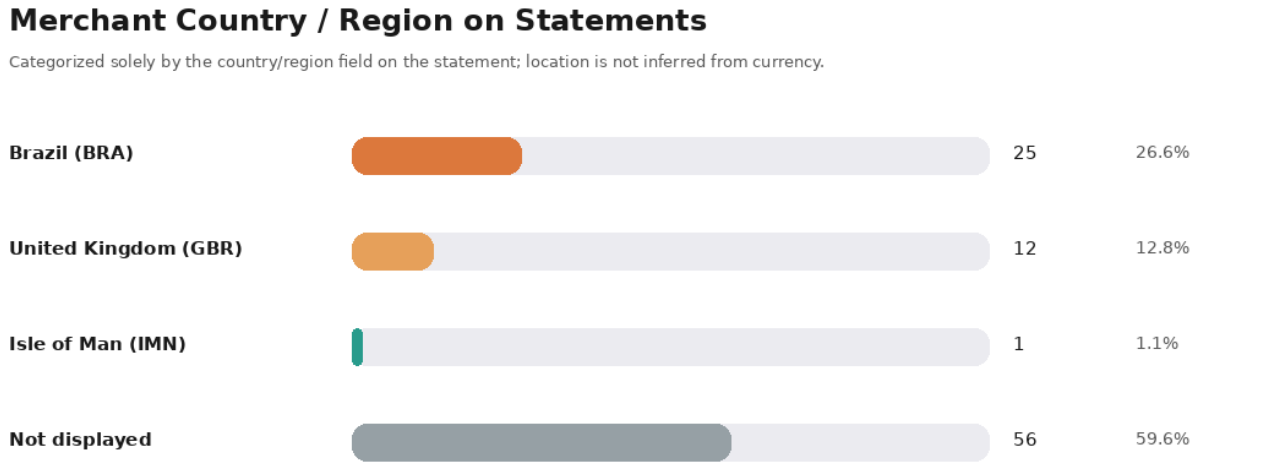


As of 29 September 2026, Threat Hunter had collected 169 related public posts and, after image-by-image verification of payment screenshots, yielded 143 transaction amounts that could be coded.

Existing samples show that anomalous activity mainly clustered around 26 September. Amount stratification across currencies is clear: among 57 Brazilian-real transactions, the 3,000–5,000 BRL band was the largest, with 26 events; among 27 pound-sterling transactions, 25 were no more than £1. Additional currencies such as USD, UYU, and PYG also appeared. Merchant names tied to the anomalous transactions were relatively dispersed—covering personal names, payment platforms, dining, pharmacies, mobile retail, websites, and institutions—with no large concentration on a single merchant observed so far.

Overall, the event shows short-window concentration, multi-region and multi-merchant dispersion, and clear amount stratification. Large numbers of very small GBP transactions may relate to credential liveness checks or payment-channel testing, while BRL transactions more often sit in higher amount bands.



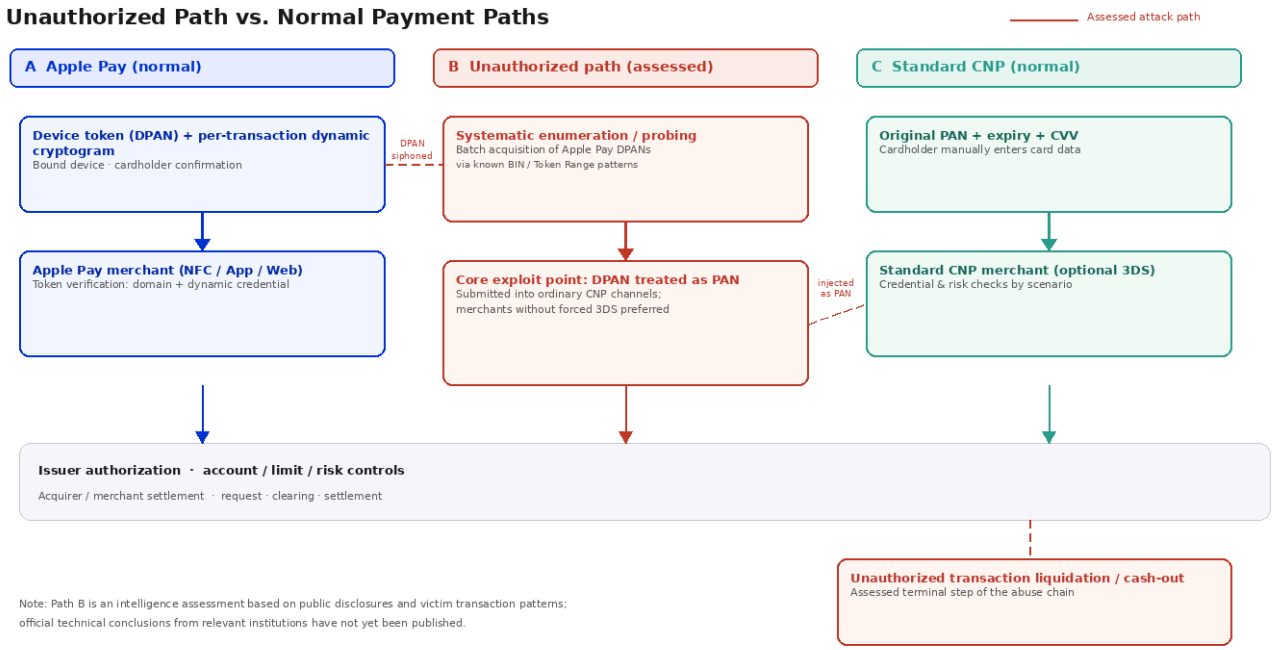


How, then, could attackers complete remote unauthorized spending while the cardholder had not left the country and the physical card had not left their possession? The analysis below addresses that question.

II. Analysis of Technical Means Used by Attackers

Combining public test disclosures and victim transaction information available so far, Threat Hunter assesses that one potential path worth focused attention is as follows:

Attackers are suspected of obtaining Apple Pay device Primary Account Numbers (DPANs) in bulk and submitting them as ordinary bank card numbers into card-not-present (CNP) channels. Where the payment chain did not effectively enforce token usage scope and cardholder authentication, unauthorized transactions were completed.



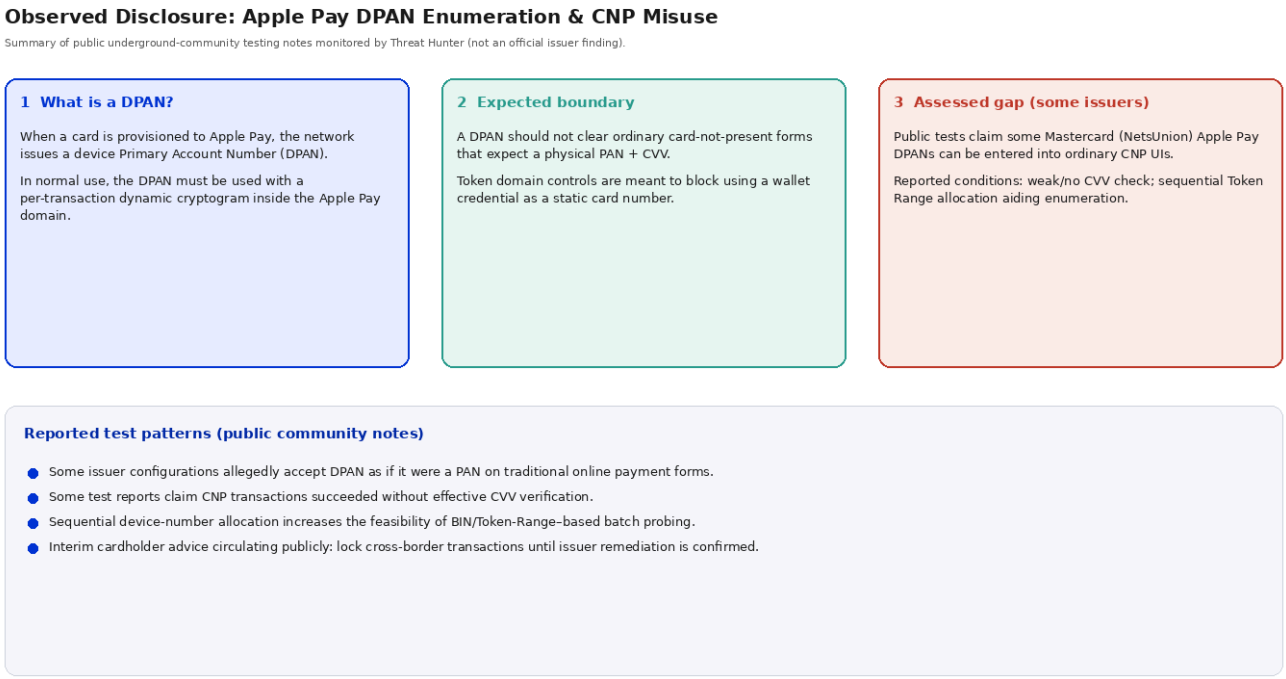
> *It must be emphasized that, as of this writing, relevant institutions have not published a final technical investigation conclusion. The attack chain below is a technical assessment formed from currently available public information; specific risk sources still require further verification.*

2.1 Underground actors suspected of obtaining DPANs via enumeration or batch probing

A prerequisite for large-scale, near-synchronous unauthorized spending is that attackers already hold, in bulk, card identifiers usable for payment. Unlike traditional card fraud that starts by stealing the original bank card number (PAN), the critical starting point in this event points to Apple Pay device card numbers (DPANs).

After a bank card is provisioned to Apple Pay, a device Primary Account Number (DPAN) is generated. Under normal conditions, the DPAN must be used in constrained scenarios together with a dynamic transaction credential.

According to disclosures in underground-related communities, some device card numbers appear to follow allocation patterns. Attackers may construct candidate numbers in bulk from known BINs or Token Ranges, then filter usable DPANs via payment feedback.



2.2 Treating DPANs as ordinary PANs in the CNP flow

The core question in this event is whether the usage boundary between DPANs and ordinary bank card numbers was effectively enforced.

In normal Apple Pay payments, a DPAN must be used with a dynamic transaction credential and pass token usage-scope and transaction-scenario checks. Ordinary CNP (card-not-present) payments, by contrast, authorize by submitting bank card number, expiry, CVV, and related fields through a merchant online-payment entry.

From information and test feedback monitored by Threat Hunter so far, some Apple Pay device card numbers appear capable of leaving the normal Apple Pay payment flow, being submitted through ordinary CNP entries, and being accepted and processed as ordinary PANs. In other words, DPANs that should be constrained by token usage scenarios appear able to be accepted by ordinary CNP payment chains as bank card numbers and enter subsequent authorization.

Public evidence: Apple Pay DPAN used in card-not-present (CNP) tests

Screenshots monitored from open channels; amounts shown are small probe / pre-auth values.



Left: Apple Pay-bound device card (ending redacted) — HKD 8.00 pre-auth freeze at GOOGLE*5SM Hong Kong; caption notes DPAN + expiry enough to start CNP.
Right: Multiple HKD 5.00 approvals on Sep 27; captions state Mastercard Apple Pay device card completed CNP without effective verification.

2.3 Exploiting low-authentication transaction scenarios to reduce friction

Under the method above, attackers would still need transaction environments with weaker authentication requirements.

For example:

- 3-D Secure (3DS) not enabled or not strictly enforced;
- CVV and similar checks not effectively applied.

When the merchant side lacks strong authentication, and the payment chain also fails to effectively validate CVV, token usage scope, or dynamic transaction credentials, limited information such as DPAN and expiry alone may still enter subsequent authorization.

Attackers may therefore be exploiting stacked validation gaps across multiple stages: missing extra authentication at the merchant, ineffective restriction of DPAN usage scenarios in payment processing, and final passage through issuer authorization.

III. Conclusion

The core risk reflected in this event is not only individual unauthorized Mastercard transactions, but whether digital-wallet credentials may still be accepted and authorized by other payment chains after leaving their intended payment context. If that boundary can indeed be bypassed or brute-forced, the risk expands beyond traditional card-number leakage into a seam between digital-wallet token usage scope and CNP authentication mechanisms.

Several key questions still require further verification, including how attackers obtained DPANs in bulk, which specific payment stage failed to restrict token usage scope effectively, and whether a clear link exists between small-amount tests and subsequent higher-amount transactions.

Threat Hunter will continue to monitor acquirers, payment channels, authentication methods, and transaction-linkage features behind related anomalous activity, in order to further reconstruct the full attack chain of this event.