THREAT HUNTER RESEARCH

Paid a Real Corporate Account, Still Defrauded: Impersonated Payment Claiming

How fraud rings link genuine corporate payments to orders they control through impersonated payment claiming, and how platforms, banks and buyers can respond.

Original publication: 2026-11-23
Research team: Threat Hunter Research Team
Source report: 10 pages

Research scope and sample: This report draws on a number of representative corporate procurement fraud cases that were publicly disclosed or collected through monitoring between 2024 and early 2026, in which the amount involved per transaction was mostly in the range of tens of thousands to several hundred thousand yuan. It systematically breaks down how the compound fund chain of "genuine corporate payment + impersonated payment claiming + cash-out through goods" works and where it can be controlled. It is intended for fraud-control teams at business procurement platforms, anti-fraud departments at financial institutions, and finance and procurement leads at companies. All evidential materials in this report have been redacted end to end for compliance.

In conventional business thinking, once a buyer has checked a supplier's business registration, signed a formal purchase and sale contract and paid into the genuine corporate bank account of a well-known company, its money is reasonably safe.

In the corporate procurement fraud run by cybercriminal groups that has surged recently, however, this traditional security assumption is breaking down. Fraud rings no longer rely on personal bank cards or shell company accounts to receive money directly. Instead, they impersonate the victim company, obtain its business license and bank payment receipts, or hijack the reference code in the transfer remarks. In this way, they quietly link the money that the victim paid into a legitimate platform's genuine corporate bank account to a procurement account and order under their own control. They then move the value of those funds and cash it out in another location through ordinary product transactions on the platform.

Across multiple representative cases, this risk chain shows three core characteristics:

1. Traditional verification habits no longer work: "Can sign a formal contract", "the payee is a well-known company" and "the corporate bank account is genuine and verifiable" cannot, on their own, prove that a transaction is safe. The platform name, registered business entity and corporate account number supplied by fraud rings are often entirely real. What is actually forged is the business authorization, the contract seal and the ownership of the order.

2. Risk passes covertly across channels: The low-price lure appears in wholesale or second-hand channels. Price negotiation and contract signing move to messaging apps, workplace messaging apps or email. The corporate payment flows into a genuine bank collection account belonging to a large e-commerce or procurement platform, and a fulfillment order is eventually generated in that platform's procurement section. Each party sees only part of the record, and every part looks compliant, so no single party can reconstruct the full picture on its own.

3. Company documents and financial losses are tied together: Business licenses, invoicing details and electronic bank receipts are normal business documents. In this scam, however, fraud rings used them to register company accounts under a false identity, submit payment claims or file customer service appeals. Leaked documents translated directly into lost control over the money.

End-to-end breakdown: how fraud rings hijack normal corporate procurement

In operational terms, this fraud-linked fund chain has three core stages: an upstream low-price lure, midstream impersonated payment claiming and downstream cash-out through goods. At its heart, the chain is a "mismatch between business and funds": the genuine corporate payment made by the victim and the product order that the platform ultimately fulfils belong to two completely unrelated transactions. Fraud rings exploit verification gaps in company authentication and corporate payment claiming to force the two together.

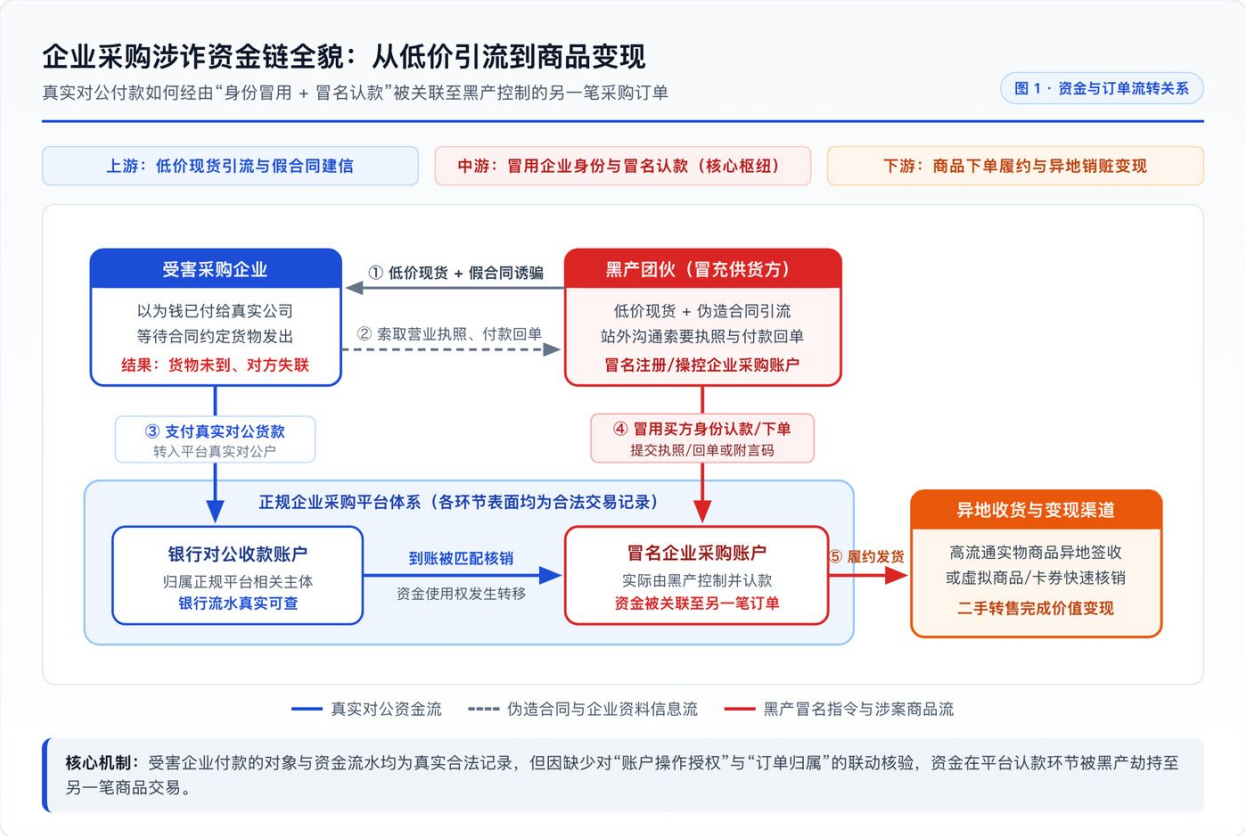

Figure 1. The full fund chain: a genuine corporate payment is matched in payment claiming to an unrelated order controlled by the fraud ring and cashed out through goods.

Source: Threat Hunter. Figure text in Chinese.

Upstream: low-priced stock and a "legitimate appearance" draw buyers past routine due diligence

Unlike common telecom fraud aimed at individual consumers, corporate procurement usually involves requests for quotation, price comparison, contract approval and a corporate bank transfer by the finance team. Fraud rings therefore deliberately build upstream transaction scenarios that closely match normal corporate purchasing habits:

- Targeting high-turnover, time-sensitive product categories: Graphics cards, servers, branded air conditioners, high-end digital products and office electronics are frequent lures. Single purchases in these categories involve large amounts, and buyers often face tight project delivery deadlines, shortages in their usual channels or pressure to cut costs. This makes the bait of "low-priced stock, fast delivery" especially effective.

- Split-character phrasing to evade monitoring and move conversations off-platform: After making initial contact in wholesale or e-commerce channels, fraud rings often insert punctuation inside words, writing the Chinese equivalents of "con, nect", "man, ager" and "dis, count", to slip past platform keyword filters. They then send QR codes and, on the pretext of "applying for an internal bulk discount" or "going through the group purchasing channel", quickly move negotiations to off-platform channels such as messaging apps, workplace messaging apps and email.
- Building trust with the shell of a real large company and a forged contract: Once off-platform, fraud rings sent buyers formal purchase and sale contracts with complete terms (specifying a 13% special VAT invoice, warranty and breach-of-contract clauses, and bearing a supplier company seal suspected to be forged). They also supplied the genuine corporate bank account details and invoicing information of a legitimate, well-known company. Even if the buyer checked the business registry and verified the bank account name, it could only confirm that "the company and the account really exist". It could not verify whether the person it was dealing with actually had lawful authority to act as the company's agent.



Figure 2. Upstream lure: split-character phrasing evades platform keyword filters before the deal moves to an off-platform messaging app to push for payment (redacted).

Source: Threat Hunter. Figure text in Chinese.

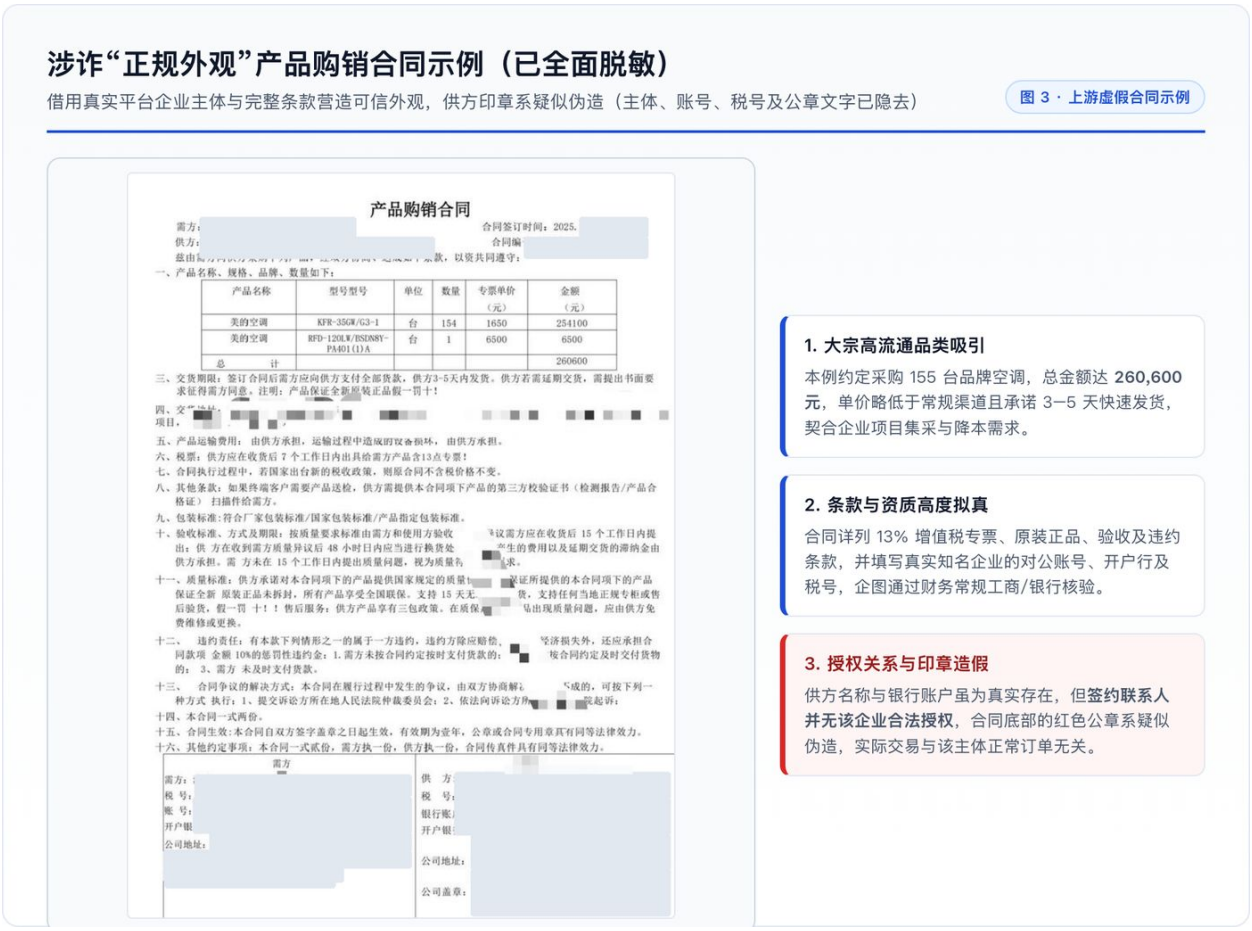

Figure 3. A forged contract borrows a real company's identity and complete terms to look legitimate; the supplier seal is suspected to be forged (redacted).

Source: Threat Hunter. Figure text in Chinese.

Midstream: impersonating the buyer and claiming its payment

The midstream stage is the core hub that makes the entire fraud-linked fund chain possible. Fraud rings do not control the receiving bank account directly. Instead, they target verification gaps in legitimate business procurement platforms' entity authentication and claiming of incoming corporate payments (payment claiming or matching), and take the genuine money the victim paid into the platform's corporate account "for their own use".



Figure 4. A normal corporate procurement loop compared with the two paths fraud rings use to hijack genuine corporate payments through impersonated payment claiming.

Source: Threat Hunter. Figure text in Chinese.

Why can a genuine corporate transfer be claimed by someone else? In business terms, this kind of hijacking usually exploits three key control gaps:

1. The static document authentication gap: When companies register accounts, complete real-name authentication or file appeals against account restrictions, some platforms rely too heavily on a photo of the business license and basic registration details. They lack liveness and consent verification of the legal representative behind the operator, or do not enforce "corporate micro-deposit verification with a remark code". As a result, fraud rings that obtain a business license can open an account in the company's name or take over an account through an appeal.

2. The shared collection account and manual payment-claiming gap: If a platform does not use a "one order, one account" virtual sub-account (VA) at the bank and instead collects payments into a shared corporate collection account, it has to match bank transactions to specific company accounts through manual or semi-automated processes. When payment-claiming checks compare only "transfer amount, date, payer name and a screenshot of the electronic receipt", and do not strictly block cases where "the person claiming the payment is not authorized by the paying company", the door opens to impersonated claims.

3. Hijacking the reference code in the transfer remarks ("order first, payment second"): Besides the sequence in which "the victim pays first and the fraud ring later claims the payment with the license and receipt", fraud rings also often use an impersonated account to create an order for high-turnover goods on the platform first. This gives them the platform-generated corporate receiving account number and unique order reference code. They then induce the victim to make a corporate transfer with that code in the remarks, which directly triggers the system to automatically reconcile the fraud ring's order.

> Two boundaries that fraud controls must keep clear: (1) Genuine company documents (a valid business license and invoicing details) do not mean that the operator submitting them is authorized by that company. (2) A genuine bank payment receipt (with an accurate amount, transaction record and confirmed receipt of funds) does not mean that whoever holds a screenshot of the receipt has the right to dispose of those funds.

In practice, fraud rings used plausible commercial pretexts such as "the platform's review requirements are strict", "we need to file it in the system", "we need to register after-sales information" or "finance needs to reconcile the account before arranging shipment" to ask victims for complete, unwatermarked photos of their business license, their invoicing details and electronic bank receipts. After obtaining the documents and receipts, they repeatedly delayed inspection and shipment until they disappeared altogether.



Figure 5. Midstream document harvesting: the business license is requested for "platform review" or "after-sales filing", followed by stalling and silence (redacted).

Source: Threat Hunter. Figure text in Chinese.



Figure 6. A bank payment receipt, obtained on the pretext of reconciling accounts, is the key document fraud rings use for impersonated payment claiming (redacted).

Source: Threat Hunter. Figure text in Chinese.

Downstream: cashing out through ordinary purchases, which makes funds far harder to trace and recover

Once the payment has been linked under a false identity to a procurement account or order controlled by the fraud ring, the funds move quickly into purchase and delivery. Fraud rings favor items with strong market liquidity, low resale discounts and quick resale, including high-value digital and electronic products, high-end hardware, and virtual goods and electronic vouchers that platform rules allow buyers to purchase.

Although "buying high-value goods or vouchers to cash out" is not a new technique in itself, embedding it in a corporate procurement fund chain makes it considerably more adversarial and harder to handle than traditional money-mule laundering through personal bank cards or consumer-side fake-order cash-out schemes. This shows in three ways:

- Bypassing personal limits and conventional anti-money-laundering models: The money enters a large, legitimate platform as a genuine corporate payment for goods, and a single payment can reach tens of thousands to several hundred thousand yuan. This naturally avoids the non-counter transaction limits on personal bank cards and the typical fraud-linked transaction pattern of "fast in, fast out, split across many layers".
- Traditional bank stop-payment and freezing mechanisms are hard to apply directly: The payee is the corporate collection account of a large, legitimate platform that carries a huge volume of lawful commercial settlements. Banks and judicial authorities cannot freeze the whole account, as they would a fraud-linked personal card or a shell company account. They must rely on the platform to trace the specific sub-account and order involved.

- Delays across multiple delivery steps create a time gap that hinders recovery: After claiming the payment and placing orders, fraud rings often continued to placate the victim with excuses such as "transferring stock between warehouses", "finance is reviewing it", "logistics delays" or "the refund is being processed". This bought them a window to have physical goods signed for and forwarded in another location, sell them through second-hand channels, or redeem virtual vouchers within seconds. By the time the victim noticed and reported to the police, the money had long since become goods delivered in good faith, making cross-platform, cross-region tracing extremely costly.

Case review: a CNY 140,000 professional graphics card payment claimed under a false identity

The following is a representative professional graphics card procurement fraud case for which the police opened a criminal investigation (case filed in 2024):

- Upstream deception and contract signing: Because its usual supply channel was out of stock, the victim procurement company came into contact through an outside channel with a "supplier" who claimed to have ten professional 24 GB graphics cards in stock. The supplier quoted a unit price of CNY 14,000 and a total of exactly CNY 140,000 (slightly below the prevailing spot market price at the time). Through a workplace messaging app, coordination among several "sales staff" and a formal Sales Contract (expressly including a 13% special VAT invoice and a three-year warranty), it created the appearance of a legitimate supplier and led the victim to transfer the full amount in a single payment to a genuine corporate bank account.
- Midstream document harvesting and impersonated claiming: After the payment was made, the other party obtained the victim's business license and bank payment receipt on the pretext of "confirming receipt of funds, registering the invoice and arranging shipment". The fraud ring then used a company procurement account it controlled under a false identity to link the genuine CNY 140,000 payment to a different procurement order on the platform that had nothing to do with the original contract, transferring control over the funds.
- Downstream delay, disappearance and case filing: The fraud ring kept stalling with claims that it was "arranging shipment", and cut off all contact once the corresponding order had completed the transfer of assets. After the victim realized it had been defrauded and reported the case, the investigating authority found that it met the criteria for filing and formally opened a criminal investigation into it as a case of telecom and online fraud.

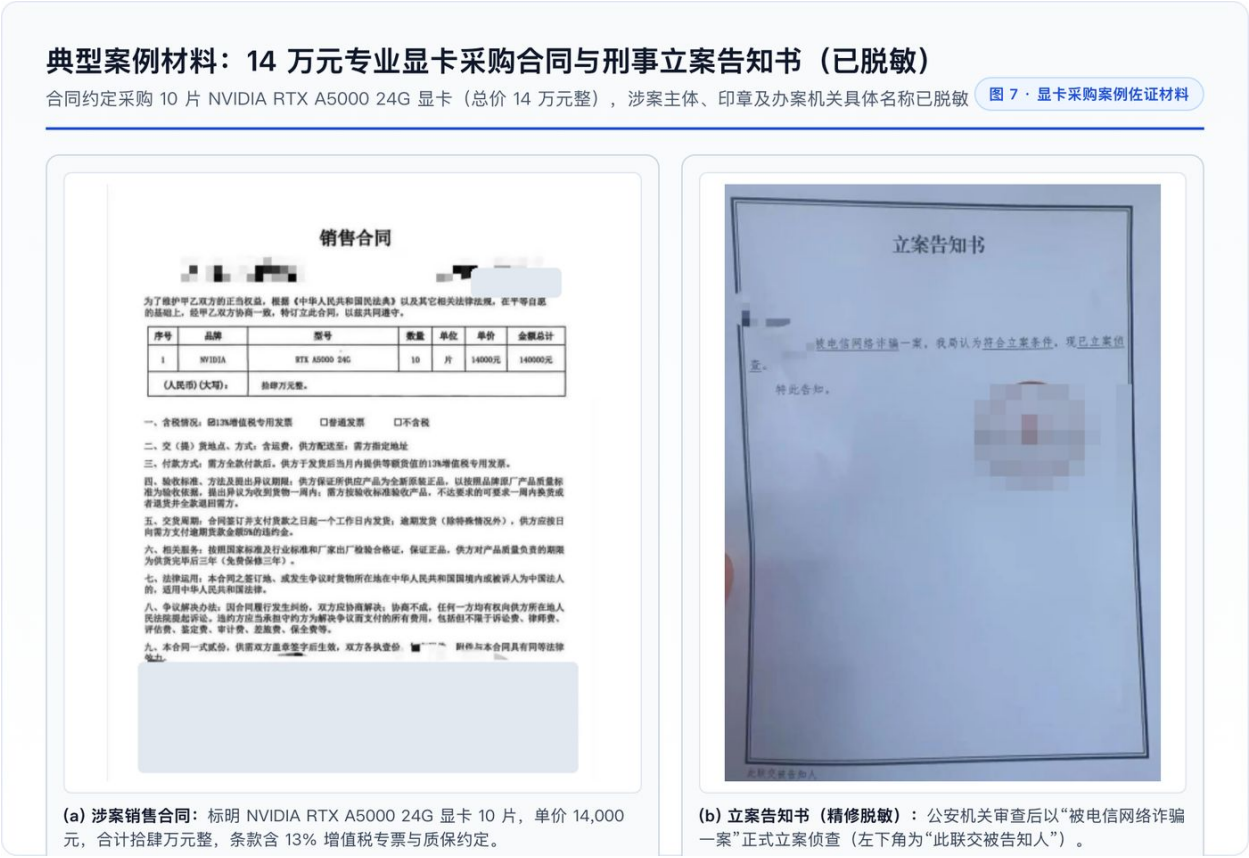

Figure 7. Evidence from the CNY 140,000 graphics card case: (left) the sales contract; (right) the police notice of criminal case filing (both redacted).

Source: Threat Hunter. Figure text in Chinese.

The case shows that even with a well-drafted contract, a genuine bank payee and a complete order fulfillment record inside the platform, a fraud-linked transfer of funds running through the upstream, midstream and downstream stages still cannot be stopped unless the paying entity, account authorization, payment-claiming record and the actual destination of the delivered goods are verified together.

Blind spots and an assessment framework: from single-point checks to four-flow cross-verification

This kind of fraud-linked fund chain is hard to detect because fraud rings precisely exploit a blind spot in which "local authenticity masks global anomalies". The company's registration details are real, the corporate account is real, and the platform's order and delivery records are equally real, yet the chain of authorization across the steps has already been broken. The table below summarizes three types of risk blind spot that traditional single-point verification most easily misses:

Risk dimension	Common traditional verification	Anomaly in the fraud-linked fund chain	Core risk that is easily missed
Company identity	Check the business license, business registration details and contract letterhead	Fraud rings use a real company's documents to register, authenticate or file appeals on the platform and take control of a procurement account	The registered company really exists, but the person actually operating the account is not authorized by that company
Ownership of funds	Check the corporate receiving account, the amount received by the bank and the payment receipt	The victim's genuine corporate payment is matched to an account controlled by the fraud ring through an impersonated receipt claim or the reference code in the transfer remarks	The corporate bank transaction and receipt of funds are genuine, but the actual payer differs from the entity that claims and uses the funds
Order fulfillment	Check the platform order status, payment reconciliation and delivery sign-off records	Fraud rings use the wrongly claimed funds to buy high-turnover digital goods or vouchers and arrange delivery in another location for resale	The platform order and shipping records are genuine, but the order was not authorized by the paying company, and the paying company never received the goods

Fraud controls must therefore move beyond the perspective of "a single transaction" and "a single entity". They should build a "four-flow cross-verification" model covering the information flow, funds flow, order flow and logistics (fulfillment) flow, with a focus on checking whether entity authorization and the destination of the transaction form a consistent closed loop.



Figure 8. Four-flow cross-verification: the paying company, authorized operator, funds claimant and final recipient must all match; any break triggers a high-risk alert.

Source: Threat Hunter. Figure text in Chinese.

Joint defense: securing funds across the procurement chain

Preventing fraud-linked fund chains in corporate procurement cannot depend on after-the-fact remediation by any single party. Business procurement platforms, financial institutions and buying companies need to work together, closing gaps in authentication and payment claiming, transfer alerts and internal procurement processes respectively.

Business procurement platforms: tighten authentication and payment-claiming checks, and adopt "one order, one account"

- Upgrade company account authentication and authorization checks: Stop allowing company authentication or customer service appeals to succeed on the strength of a static business license photo alone. Introduce corporate micro-deposit verification with a remark code (requiring reverse verification from the paying company's genuine corporate account) and real-name liveness and consent verification of the legal representative or authorized agent, so that "the account operator" is firmly bound to "the company".
- Replace manual claiming on shared accounts with dynamic virtual sub-accounts: Where technically feasible, gradually roll out automatic reconciliation through bank virtual sub-accounts (VA) on a "one customer, one code" or "one order, one account" basis. For business that still relies on manual claiming with receipts, enforce a check that the paying bank account name exactly matches the authenticated entity of the claiming account, and strictly control claims for payments made on behalf of a different entity.
- Strengthen interception of high-risk fulfillment after payment claiming: For newly registered or newly authenticated company accounts that claim large corporate payments from other regions and then, within a short time, concentrate purchases on high-turnover digital products, high-end graphics cards or servers, or virtual vouchers, or whose delivery address deviates clearly from the paying company's registered location, trigger delayed shipment and a verification call-back to the phone number in the public business registration record, so that assets do not leave during the critical window for stopping losses.

Financial institutions: flag fraud signals in large corporate transfers and coordinate targeted investigations

- Strengthen alerts for a company's first large corporate payment through online banking: Banks and payment institutions should not assume low risk simply because the payee is the corporate account of a well-known large platform. When a corporate customer makes its first large transfer to a large platform's collection account that is not a historical counterparty, and the transfer remarks contain an unusual order number or reference code, or several round-sum payments are made within a short time, an online banking pop-up can prompt the customer to confirm "whether the order was placed from your own official account".
- Build precise joint investigation channels for fraud-linked corporate transactions on large platforms: Since a large platform's corporate collection account is not suited to traditional

blanket account freezes, financial institutions should combine external fraud intelligence with customer complaint leads and, in accordance with the law, work with the relevant procurement platforms and anti-fraud authorities to establish precise joint investigation at the level of individual transactions and linked emergency stop-payment mechanisms, helping platforms quickly lock down the payment-claiming sub-account and undelivered orders involved.

Buying companies: order only through your own official account and watermark licenses and receipts

- Hold the line on "ordering from your own official account": For large procurement, never sign and pay unilaterally in messaging apps, workplace messaging apps or email outside a legitimate platform. Before transferring money, verify the supplier's agency authority, the order details and the ownership of the corporate payment reference code yourself, through the platform's official public customer service number or by logging in to the official procurement back office controlled by your own company.
- Require purpose-restricting watermarks on business licenses and payment receipts: When providing scanned business licenses, invoicing details or electronic bank receipts to outside partners, add a diagonal semi-transparent watermark across key areas (for example, "Only for filing the contract No. XX signed with XX Company; invalid for platform account opening, payment claiming or appeals"). This greatly increases the chance that documents submitted by fraud rings under a false identity will be blocked at review.
- Stop losses on two fronts at the first sign of abnormal fulfillment: If, after payment, the other party repeatedly delays shipment with excuses such as "finance cannot find the payment", "the warehouse is doing a stock count" or "there is a system fault", immediately contact the official fraud-control or enterprise service line of the platform that owns the receiving corporate account to check whether the payment has already been claimed by someone else and used to place orders. At the same time, report the matter to your bank and the police and preserve the evidence.

Conclusion and continued monitoring

The real threat of fraud-linked fund chains in corporate procurement lies not in how complex the money's path is, but in how fraud rings have borrowed the trust infrastructure of legitimate commerce: genuine registered businesses, genuine corporate bank accounts and genuine platform transaction fulfillment. They hide illegal transfers of funds inside highly standardized corporate procurement processes.

Countering this risk requires procurement platforms, financial institutions and corporate finance teams to update their thinking together, moving from checking "whether the entity and the transaction are genuine" to checking "whether authorization, funds, order and logistics are consistent". Threat Hunter will continue to monitor how cybercriminal groups' techniques evolve in corporate procurement, bulk trade and corporate payment scenarios, and will publish actionable intelligence on high-risk fraud-linked entities, anomalous payment-claiming patterns and new cash-out routes, providing an ongoing reference for platform fraud controls and anti-fraud work at financial institutions.