THREAT HUNTER

Fraud Fund Chains in Underground Operations: Divergent Bank-Account Risk Patterns, and Fraud Proceeds Mixed into Merchant Settlement Flows

2026

Monitoring window: January–October 2026

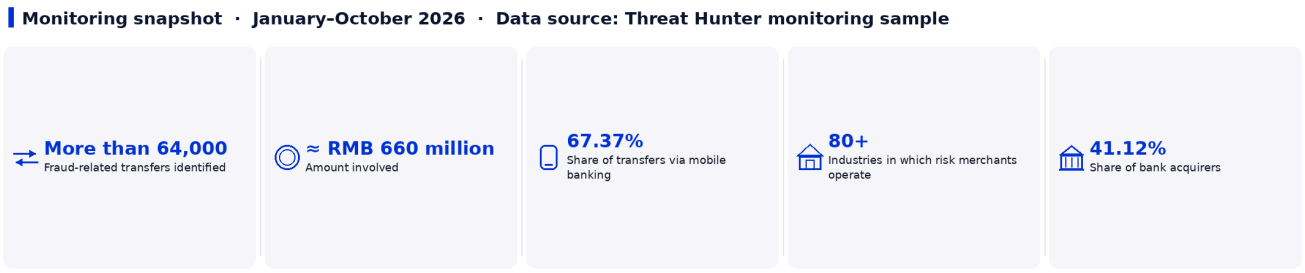
Threat Hunter · Anti-Fraud Intelligence Research



A transfer can look like an ordinary movement of funds in a bank's transaction systems.

In a fraud fund chain, however, the receiving account may be only the first hop in the movement of a victim's funds. Once the money arrives, it may be pooled, split, and transferred across multiple hops, and ultimately mixed into merchant operating flows. Personal bank cards, corporate accounts, and merchant acquiring channels can all become links in that chain.

Threat Hunter continuously monitors fraud-related fund activity by underground operators. In the January–October 2026 monitoring window, it identified more than 64,000 fraud-related transfers, involving about RMB 660 million. Mobile banking accounted for approximately 67.37% of those transfers by count. Risk merchants spanned more than 80 industries; among the acquirers linked to those merchants, bank acquirers accounted for about 41.12%.



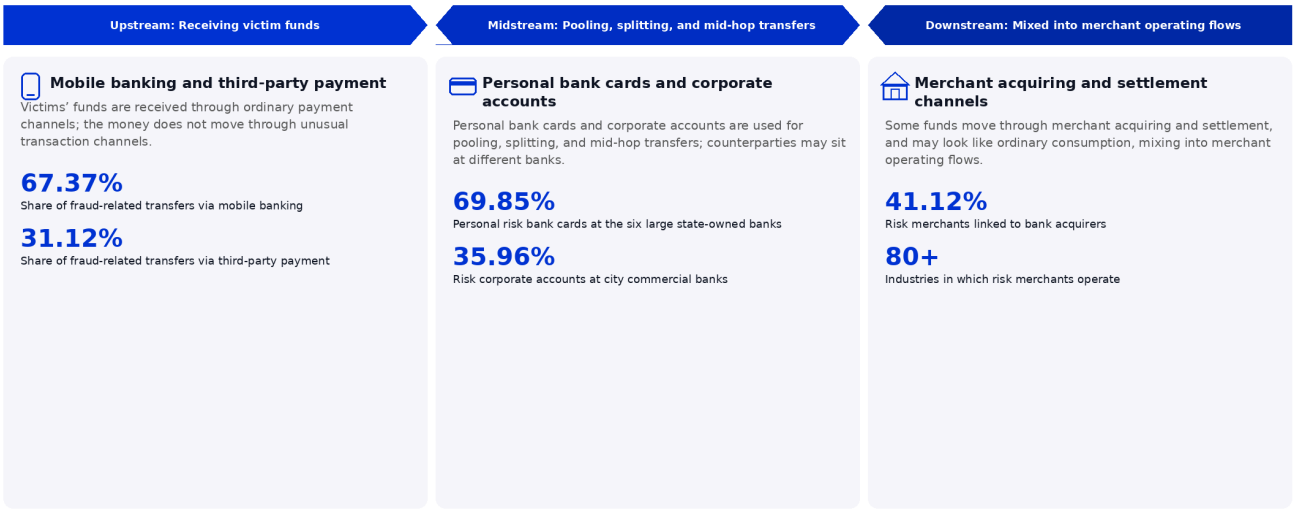
Drawing on this monitoring sample, this report examines risk characteristics across the upstream, midstream, and downstream stages of fund flows—channel mix, account-party structure, and merchant acquiring. Several features of the activity stand out:

> **Finding 1.** Fund transfers are concentrated in ordinary payment channels.
>
> **Finding 2.** Personal and corporate accounts show a structural difference in bank-type distribution.
>
> **Finding 3.** Downstream, funds enter merchant operating flows through acquiring channels.

I. How Fraud Funds Move

In the fraud-related activity monitored here, funds move across multiple account parties and payment channels. Upstream, ordinary payment channels receive victims' funds. Midstream, personal bank cards and corporate accounts are used for pooling, splitting, and mid-hop transfers. Downstream, some of the funds are mixed into operating flows through merchant acquiring channels.

Three stages of fraud fund flows, and key figures



Data source: Threat Hunter monitoring sample, January–October 2026

1.1 Upstream: Fraud-Related Funds Move Through Ordinary Payment Channels

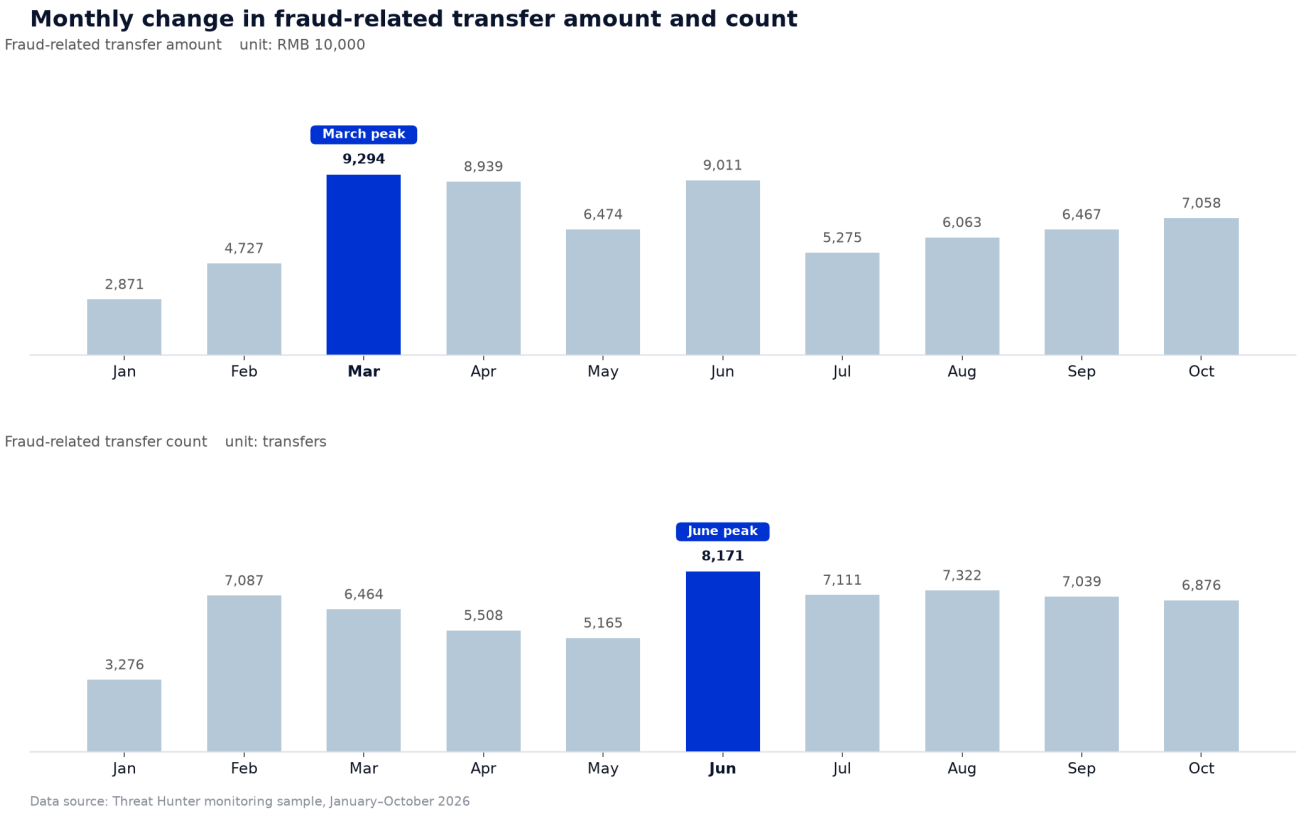
At the upstream end of the fraud fund chain, underground operators mainly use bank cards, third-party payment accounts, and similar instruments to receive and move victims' funds. The money does not travel through unusual transaction channels; it moves, in large volume, on the ordinary payment tools of everyday financial activity.

Monthly peaks in amount and transfer count are not synchronous

From January to October 2026, Threat Hunter monitored more than 64,000 fraud-related transfers, involving about RMB 660 million, or an average of about RMB 10,000 per transfer.

Month to month, the amount peaked in March, while the transfer count peaked in June—the two series are not synchronous. The scale of fraud-related fund activity and its frequency do not move in lockstep.

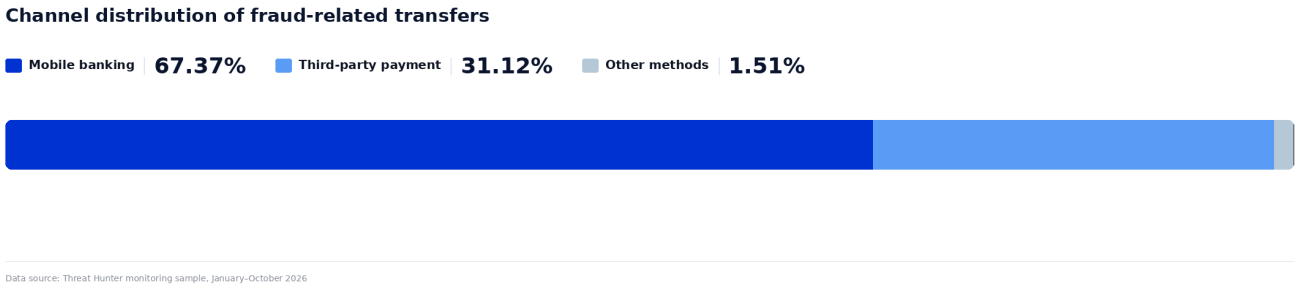
For financial institutions, identifying this activity cannot rest on the size of a single transfer alone. Frequency, counterparties, and account linkages also need to enter the judgment.



Mobile banking accounts for about seven in ten fraud-related transfers

By transfer channel, mobile banking accounted for approximately 67.37% of fraud-related transfers by count, and third-party payment for approximately 31.12%. In this monitoring sample, mobile banking was the primary channel for moving fraud-related funds.

The distribution shows that much of the activity takes place on ordinary financial-service channels. For banks, the key to identifying risk is not only the channel on which a transfer is initiated, but the role the bank's own account plays in it: whether the account is a risk payee receiving fraud-related funds, or a victim payer sending funds out.



1.2 Midstream: Personal Bank Cards and Corporate Accounts Show Different Patterns

Midstream, underground operators use personal bank cards, corporate accounts, and similar vehicles to pool, split, and transfer funds. Counterparties may sit at different banks, so the flow can involve multiple financial institutions.

In the monitoring sample, fraud-related personal risk bank cards and risk corporate accounts show a clear difference in bank-type distribution.

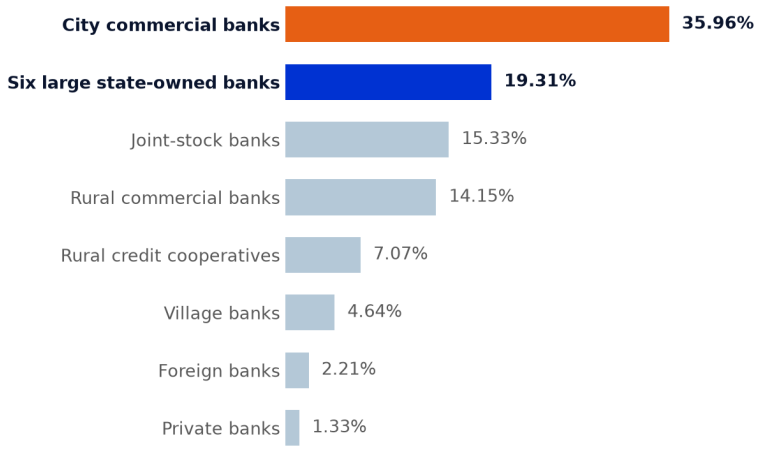
Risk corporate accounts: city commercial banks account for the largest share

Among risk corporate accounts tied to fraud, city commercial banks accounted for approximately 35.96%, the six large state-owned banks for approximately 19.31%, and joint-stock banks for approximately 15.33%.

In the accounts identified in this monitoring window, city commercial banks had the largest share of the risk corporate-account sample. This suggests that, when reviewing corporate-transaction risk, financial institutions should not look only at counterparties at large banks. Cross-bank relationships also need to be brought in, so that risk corporate accounts at different bank types can be checked in combination.

Bank-type distribution of risk corporate accounts

Shared x-axis scale with the companion bank-type chart. Blue = six large state-owned banks; orange = city commercial banks



Data source: Threat Hunter monitoring sample, January–October 2026

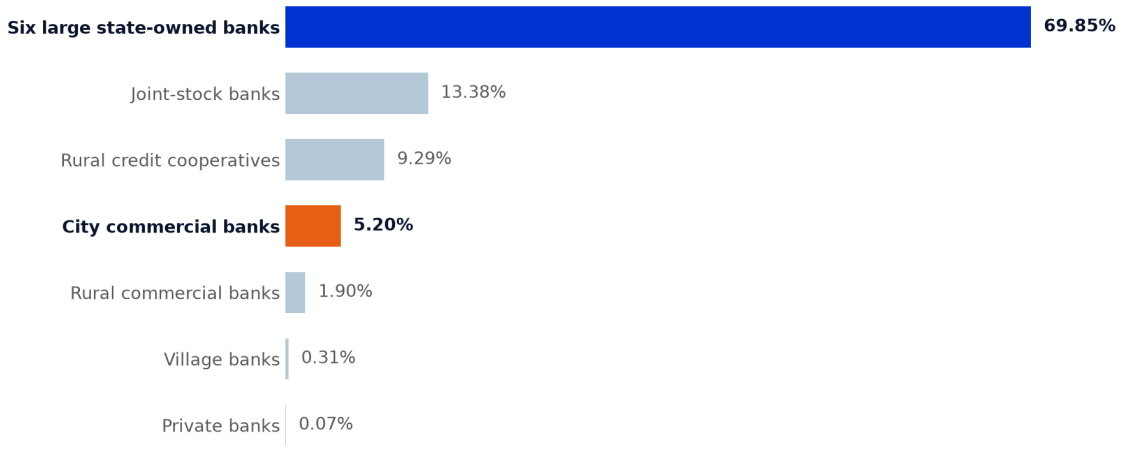
Personal risk bank cards: nearly 70% sit at the six large state-owned banks

Unlike the distribution of risk corporate accounts, the personal risk bank cards identified in the monitoring are more concentrated at the six large state-owned banks, which account for nearly 70%.

The contrast underscores the difference in bank-type mix between personal risk cards and risk corporate accounts. For the large state-owned banks, attention to external risk counterparties needs to be accompanied by tighter review of existing on-us personal accounts and their related activity.

Bank-type distribution of personal risk bank cards

Shared x-axis scale with the companion bank-type chart. Blue = six large state-owned banks; orange = city commercial banks



Data source: Threat Hunter monitoring sample, January–October 2026

> *The figures above reflect the distribution of risk accounts in this monitoring sample; they do not, by themselves, represent the overall fraud-risk level of each bank type.*

1.3 Downstream: Fraud-Related Funds Mix into Merchant Operating Flows

Merchant acquiring is one of the risk scenes that warrants close attention in the fraud fund chain. Downstream, some funds move through merchant acquiring and settlement channels. In form, the related transactions may look like ordinary consumption, allowing fraud-related funds to mix into merchant operating flows.

Risk merchants are linked to multiple acquirer types; bank acquirers account for more than 40%

Among the acquirers linked to risk merchants, third-party acquirers accounted for approximately 58.88%, and bank acquirers for approximately 41.12%.

Fraud-related risk merchants, then, are not confined to the third-party payment acquiring system; bank acquiring business is exposed to the same class of risk.

For financial institutions, merchant-risk review needs to cover merchants linked to different acquirers, and to combine actual operating conditions, transaction behavior, and external fraud-risk leads. A single anomalous feature should not, on its own, be used to treat a legitimate merchant as a risk party.

Acquirer distribution among risk merchants



Data source: Threat Hunter monitoring sample, January–October 2026

Risk merchants span 80+ industries; retail and wholesale together account for nearly 70% of the top 10, with catering third

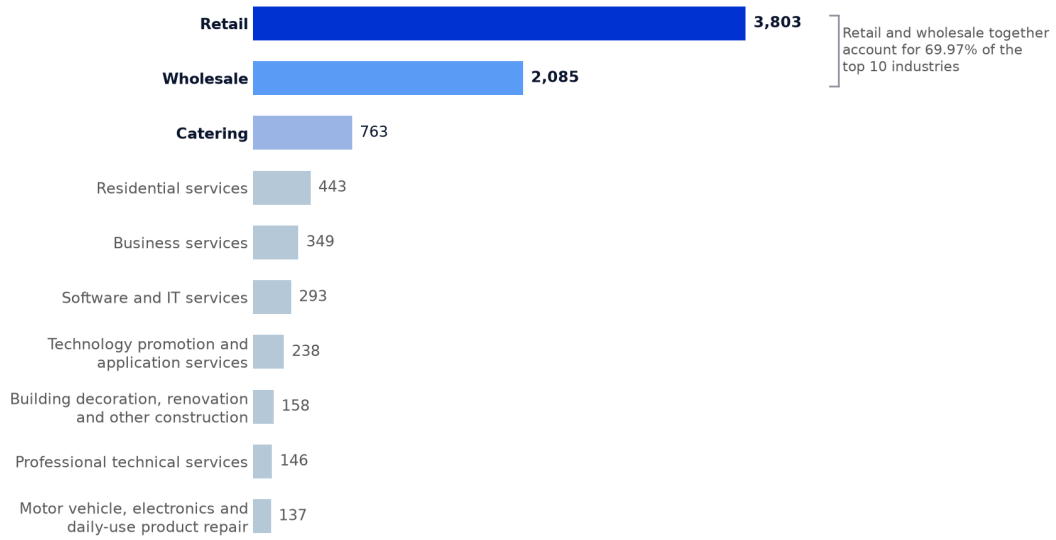
By industry, the risk merchants identified in this monitoring window span more than 80 industries, a relatively dispersed mix.

Among the ten industries with the largest numbers of risk merchants, retail and wholesale together account for nearly 70%, and catering ranks third. The mix shows that risk merchants appear across everyday business scenes.

Banks and acquirers can give priority attention to industries with larger numbers of risk merchants, but industry category itself should not be the sole basis for judging fraud risk. Actual review still needs to combine merchant operating characteristics, transaction activity, and external risk information.

Top 10 industries by number of risk merchants

Unit: merchant accounts



Data source: Threat Hunter monitoring sample, January–October 2026

II. Identification Cannot Be Limited to a Single Account, Channel, or Scenario

From the upstream receipt of funds, through midstream pooling and mid-hop transfers, to downstream merchant acquiring, fraud-related fund activity involves different account parties, payment channels, and business scenes.

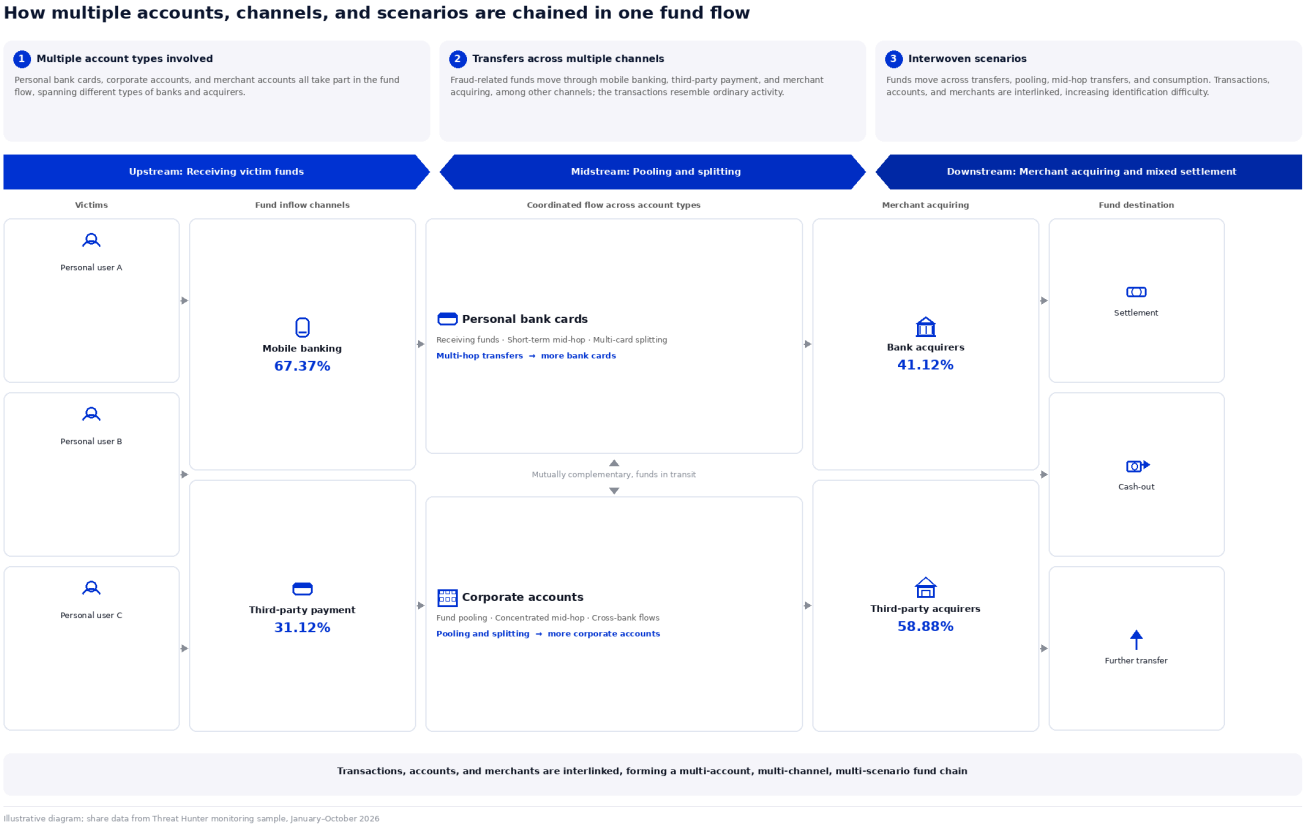
If a financial institution identifies risk from only one account type, one payment channel, or one industry, it may not be able to see the full set of related parties and transaction relationships involved.

The monitoring points to three dimensions in which identification of fraud fund chains can leave a blind spot.

Three Blind Spots in Identifying Fraud Fund Chains

Dimension	Common assumption	More typical fund-chain pattern in the monitoring	What risk reviews easily miss
Account type	Focus mainly on personal bank cards, or treat corporate accounts as relatively safe	Personal bank cards are more often used for split collection and mid-hop transfers; corporate accounts are more often used for pooling and concentrated movement of funds	Reviewing only one account type can miss the links between personal and corporate accounts, as well as cross-bank fund flows
Payment channel	Put identification effort mainly on unusual or exceptional payment channels	Large volumes of fraud-related funds move through ordinary channels such as mobile banking and third-party payment	Judging risk by channel alone can overlook counterparty identity and accounts linked before and after the transfer
Transaction scenario	Focus mainly on direct transfers between accounts	Some fraud-related funds move through merchant acquiring in industries such as retail, wholesale, and catering, in forms that can resemble ordinary consumption	Looking only at account transfers can miss risk in merchant acquiring; judging solely by industry can also harm legitimate merchants

Taken together, these features indicate that identification cannot rest on a single dimension. The links among personal bank cards, corporate accounts, and risk merchants—and the movement of funds across channels and institutions—are information financial institutions need when reviewing fraud-related risk.



Illustrative diagram; share data from Threat Hunter monitoring sample, January–October 2026

III. Financial Anti-Fraud Fund-Chain Profiling Supplements External Risk Visibility

Banks can monitor risk from on-us account information and transaction flows. Visibility can still fall short, however, on whether an off-us counterparty is a fraud-risk party, whether the funds are linked to other risk bank cards or corporate accounts, and whether the activity involves a risk merchant.

That gap is especially likely when fraud-related funds move across banks and different acquirers: a single on-us transfer is often not enough to reconstruct the relationships among the risk parties involved.

To address this, Threat Hunter's Financial Anti-Fraud Fund-Chain Profiling, built on continuous monitoring of underground fraud fund activity, provides financial institutions with external intelligence leads—centered on fraud-related transactions, risk accounts, and risk merchants—that can be used in risk verification and related-party review.

The product comprises four risk profiles, each corresponding to a different fund-chain identification scene.

Four Risk Profiles in Financial Anti-Fraud Fund-Chain Profiling

Profile type	What it provides
Fraud transaction profile	Provides payer and payee account information in fraud-related transactions, helping financial institutions identify risk receiving accounts and review related activity. Along the payer trail, it can also surface suspected victims, supporting risk alerts, dissuasion, and loss containment.
Risk bank-card profile	Provides leads on fraud-related risk bank cards, supporting risk screening of existing personal accounts and, together with on-us transaction data, identification of related-account risk.
Risk corporate-account profile	Provides leads on fraud-related risk corporate accounts, supporting risk verification of corporate accounts and related reviews of suspicious corporate transactions.
Risk merchant profile	Provides leads on fraud-related risk merchants and related transactions, supporting screening of existing merchants, transaction verification, and differentiated risk controls.

In bank risk-control operations, these four classes of intelligence can be combined with existing account-management, transaction-monitoring, and case-review processes, and applied mainly before, during, and after an event.

Three Application Stages of Fund-Chain Intelligence in Bank Risk Control

Pre-event risk screening	In-event transaction monitoring	Post-event case review
In screening existing personal accounts, corporate accounts, and merchants, introduce external fraud-risk lists to identify potential risk parties that warrant closer verification, then follow up with on-us information.	In transaction-risk monitoring, match external intelligence on risk accounts and counterparties, providing supporting judgment for unusual-transaction identification, risk alerts, and necessary intervention.	In fraud-event investigation and disposition, combine external leads on fraud-related transactions, risk accounts, and related merchants to supplement cross-bank account linkages and related transaction information, supporting case review and follow-up action.

By combining external intelligence on fraud-related funds with existing risk-management processes, financial institutions can move beyond identification of a single transfer and extend combined review to risk accounts, counterparties, and related merchants.

Closing

The concealment of fraud fund chains lies not only in the repeated movement of funds, but in the use of ordinary financial channels and business scenes to mask the risk.

For financial institutions, identifying that risk cannot rest on a single transfer or a single account. It also requires counterparty risk, cross-bank account linkages, and risk-merchant leads, so that fraud fund chains can be identified and reviewed more completely.

Threat Hunter will continue to monitor underground fraud fund activity, tracking changes in risk accounts, transfer channels, and merchant acquiring, and will provide the financial industry with further observation and research reference.