



INTERNAL PREVIEW / PUBLISHED

Research report preview

Back to editor

All reports

Signed in as 洪婷 · Publisher. This internal preview is not indexable.

Research report / Threat Research

H1 2026 China Data Leakage Risk Trends Report

Threat Hunter analyzes China's data leakage landscape in H1 2026, covering underground data trading, distribution channels, affected industries, and major data categories, with a focus on dark web migration, lending-data supply chain exposure, and illegal information lookup services.

Original publication date
2026年9月7日

Research team
Threat Hunter Research Team

Report year
2026

更早看见风险，及时采取行动

THREAT HUNTER · 威胁猎人

跳到主要内容

Content overview

Report summary

- Full English web edition
- 黑灰产
- 业务欺诈
- 风险手机号
- 风险 IP
- 网络洗钱
- 风险邮箱
- 数据泄露
- 钓鱼仿冒
- 品牌保护
- 信贷欺诈

In H1 2026, Threat Hunter verified 23,645 data leakage incidents involving 3,426 organizations. The report examines the growing concentration of high-risk data on the dark web, lending-data leakage across third-party supply chains, and the commercialization of illegal personal information lookup services. It also traces how leaked data is repeatedly resold and used for fraud, fake debt collection, targeted marketing, and profile enrichment.

This draft contains the full English web edition. Compare every section with the approved source and complete all publication checks before release.

01 Data Leakage Trends and Dark Web 跳到主要内容	02 Lending Data Leakage, Supply Chain	03 Commercialization of Illegal Financial Information Lookup Services
---	--	--

Research content

H1 2026 China Data Leakage Risk Trends Report

Full English edition · 2026 · Threat Research

Foreword

Data breaches are no longer isolated security incidents. They have become an underground industrial chain with stable supply, clear division of labor, and continuous trading. Around personal information and enterprise data, underground channels have formed relatively mature operating mechanisms covering acquisition, processing, pricing, and distribution, and continue to adjust their forms in response to external governance conditions and downstream demand.

This report is based on Threat Hunter’s long-term observation of underground data trading channels. It covers publicly observed trading dynamics in the first half of 2026, and presents the scale of traded data, circulation channels, affected industries, major categories, and structural changes, as a reference for enterprises across industries assessing their external exposure.

Core Thesis

In H1 2026, the underground data trading market showed five defining characteristics: persistently high supply, increasingly covert channels, supply-chain sourcing of formalized circulation of lending data, and commoditization of query
跳到主要内容
anonymous group chats remained the primary trading venue, while the

applications also stayed at high levels; manufacturing and retail saw notable growth in major-risk incidents. Lending data continued to run through the full chain of leakage, resale, and downstream abuse, while financial record checks further exhibited commoditized features of delivering query results on a per-person, per-query basis.

Key Findings

Underground data trading remained elevated. Incident volume in H1 2026 rose about 7.0% versus H2 2025, and the supply of traded data stayed high.

The dark web's share of circulation channels rose markedly, from about 10.6% to about 20.9%. Under public-platform governance, anonymous-chat risk controls, and normalized ransomware disclosure, high-risk data and public pressure disclosures increasingly concentrated on the dark web.

Broader financial services remained the most concentrated sector for data breaches. Manufacturing and retail saw notable growth in major-risk incidents, and breach risk continued to spread across more industries.

Third-party supply chains were a major source of data breaches. In lending and other businesses that heavily depend on external services, supply-chain-related risk was especially concentrated. Direct insider leakage accounted for a relatively small share, and a considerable portion of such claims came only from seller assertions.

Lending-related data was the most active category in H1 2026, with the highest degree of industrialization and the most complete downstream monetization chain. Once leaked, such data may be repeatedly resold and used for outbound fraud calls, fake collections, precision marketing, and record-check enrichment. Risk does not end when the original leak source is cut off.

[跳到主要内容](#)

mobile numbers, ID numbers, and bank card numbers—can be further enriched with information on linked cards, balances, transaction histories, credit reports, and payment activity, expanding a single business record into a personal financial profile.

I. Overall Data Breach Landscape

1.1 H1 2026: 23,645 data breach incidents involving 3,426 enterprises; monthly average up about 7.0% versus H2 2025

According to Threat Hunter’s Data Breach Monitoring Platform, after dual validation by the authenticity verification engine and DRRC human analysis, 23,645 confirmed valid data breach incidents were recorded from January to June 2026, involving 3,426 enterprises across banking, consumer finance, e-commerce, social tools, and other key industries. On a monthly average basis, incident volume rose about 7.0% versus H2 2025.

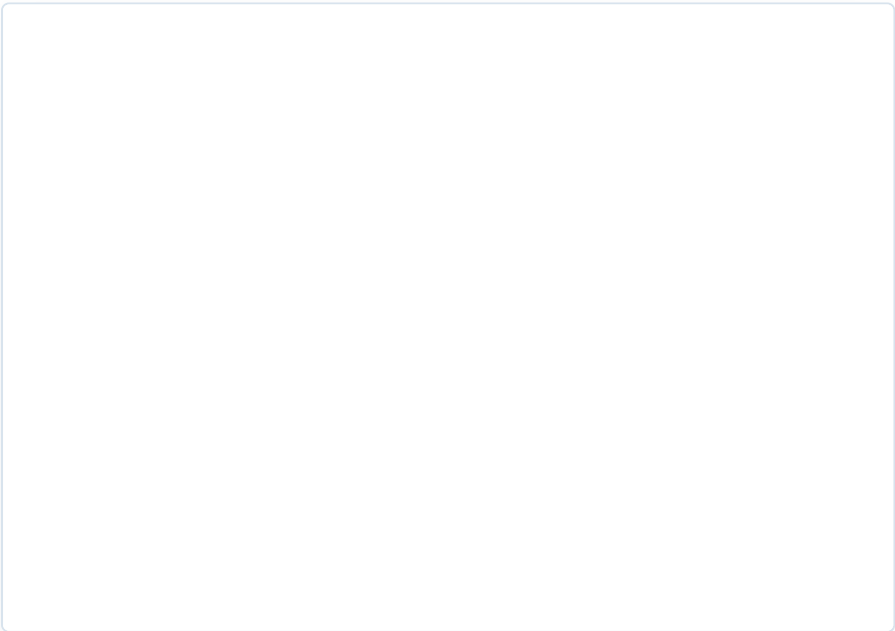
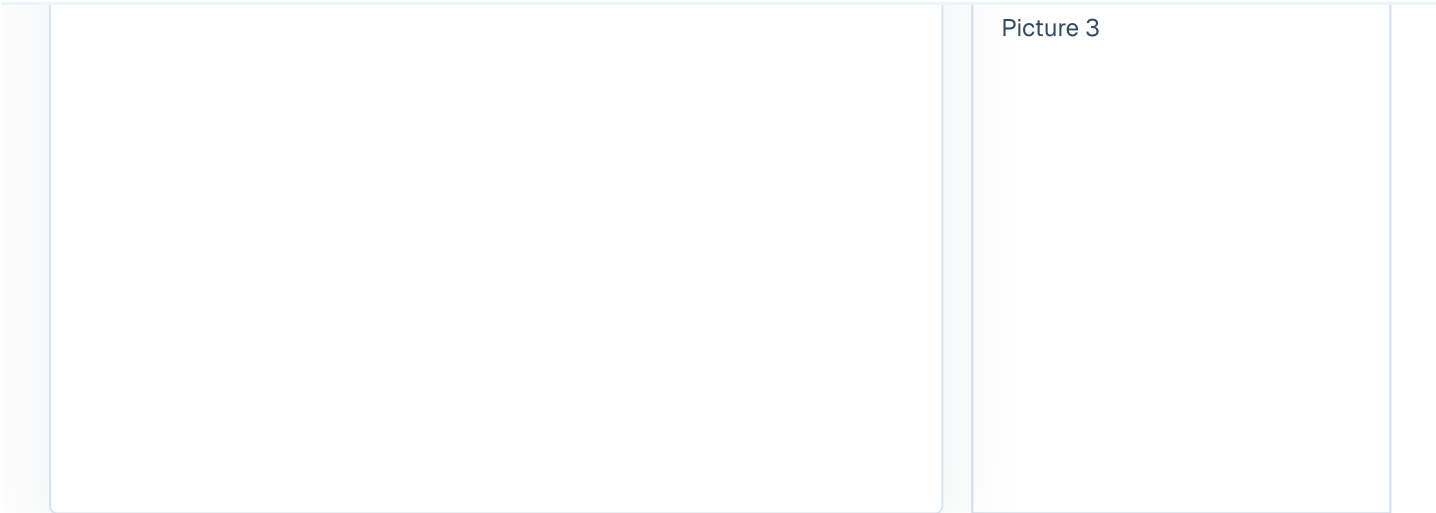


FIGURE CONTEXT

Picture 2

Original DOCX, near paragraph 15

跳到主要内容



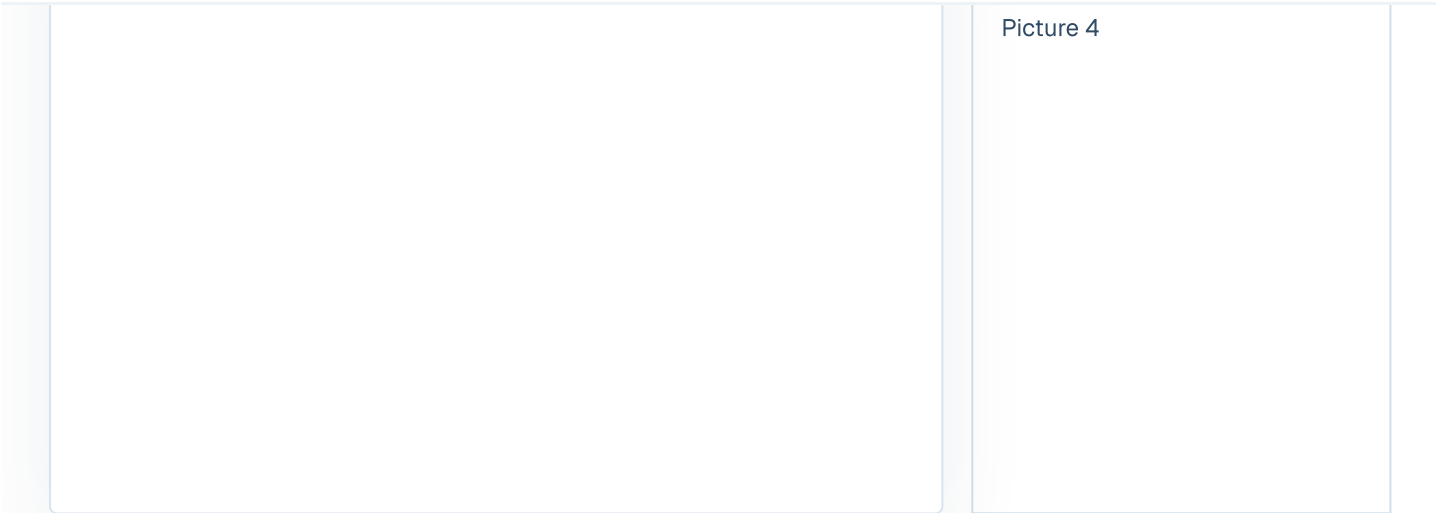
Original DOCX, near paragraph 15

1.2 Major-risk incidents rose 22.90%; dark-web disclosure highly concentrated; manufacturing and retail led growth

According to Threat Hunter statistics, H1 2026 saw 542 “major-risk incidents” involving large data volumes or potential harm to public security, up 101 from 441 in H2 2025, an increase of 22.90%.

Major-risk incidents: large data volume, highly sensitive fields, involvement of core business data, public disclosure by ransomware/hacker groups, or potential for significant compliance, reputation, or public-safety impact.

跳到主要内容



Picture 4

Original DOCX, near paragraph 18

The share of major-risk incidents disclosed on the dark web rose from about 76.4% to 95.0%, up roughly 18.6 percentage points. Public disclosure of major-risk incidents clearly concentrated on the dark web.

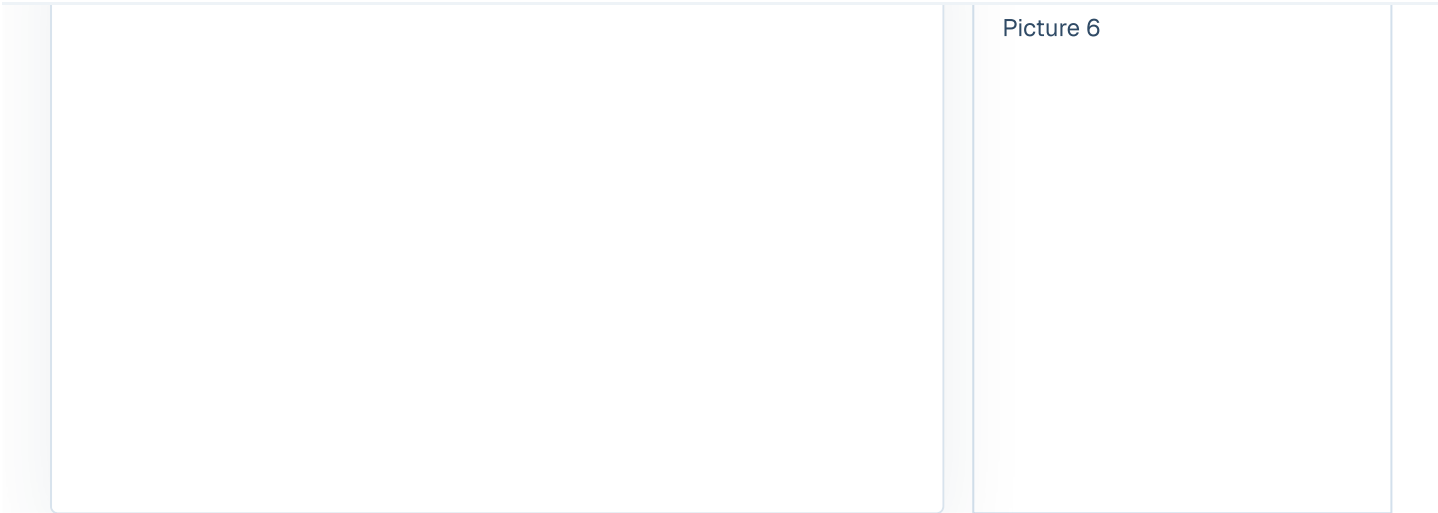


FIGURE CONTEXT

Picture 5

Original DOCX, near paragraph 19

跳到主要内容



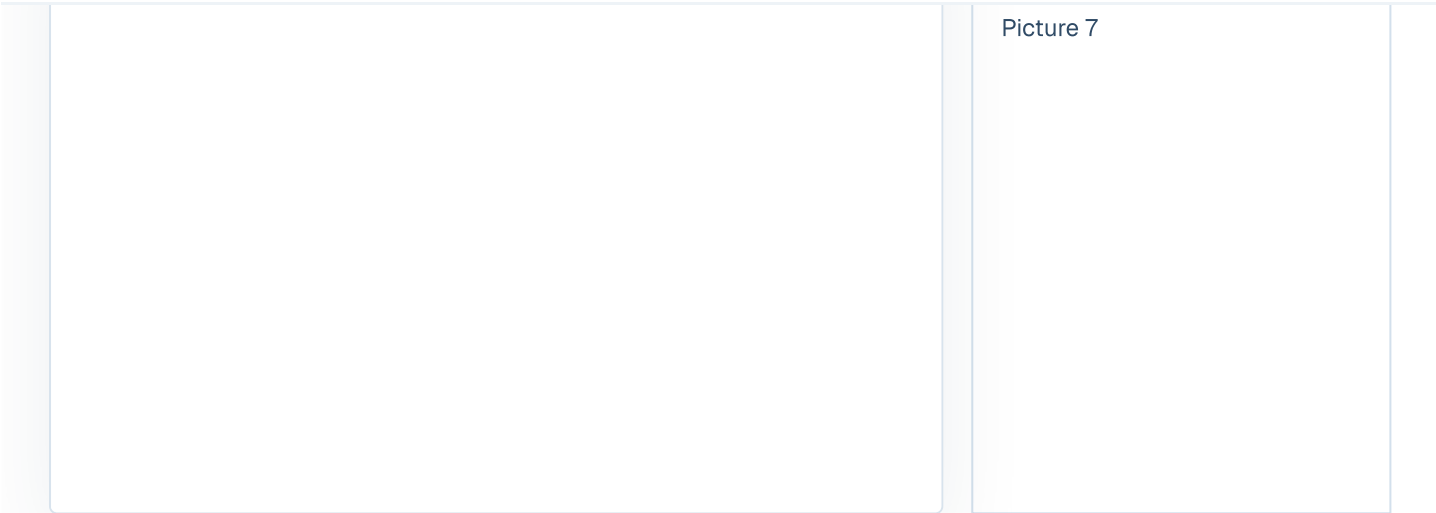
Picture 6

Original DOCX, near paragraph 19

By industry, major-risk incidents in H1 2026 were mainly concentrated in manufacturing, internet, public services, finance, and retail. Manufacturing major-risk incidents rose 82.14% versus H2 2025—the largest increase among the top five industries—followed by retail at 59.26%. By contrast, public services and finance saw declines versus H2 2025. Overall, incremental risk incidents concentrated more in manufacturing and retail, showing diffusion toward physical production and consumer distribution.

Manufacturing incidents mainly involved automotive, consumer electronics, machinery and equipment, and electronic component manufacturing.

跳到主要内容



Picture 7

Original DOCX, near paragraph 21

Further analysis of manufacturing and retail, the two sectors with larger H1 2026 major-risk growth, identified 196 incidents, of which 134 (68.37%) were ransomware/hacker-group disclosures involving 37 organizations.



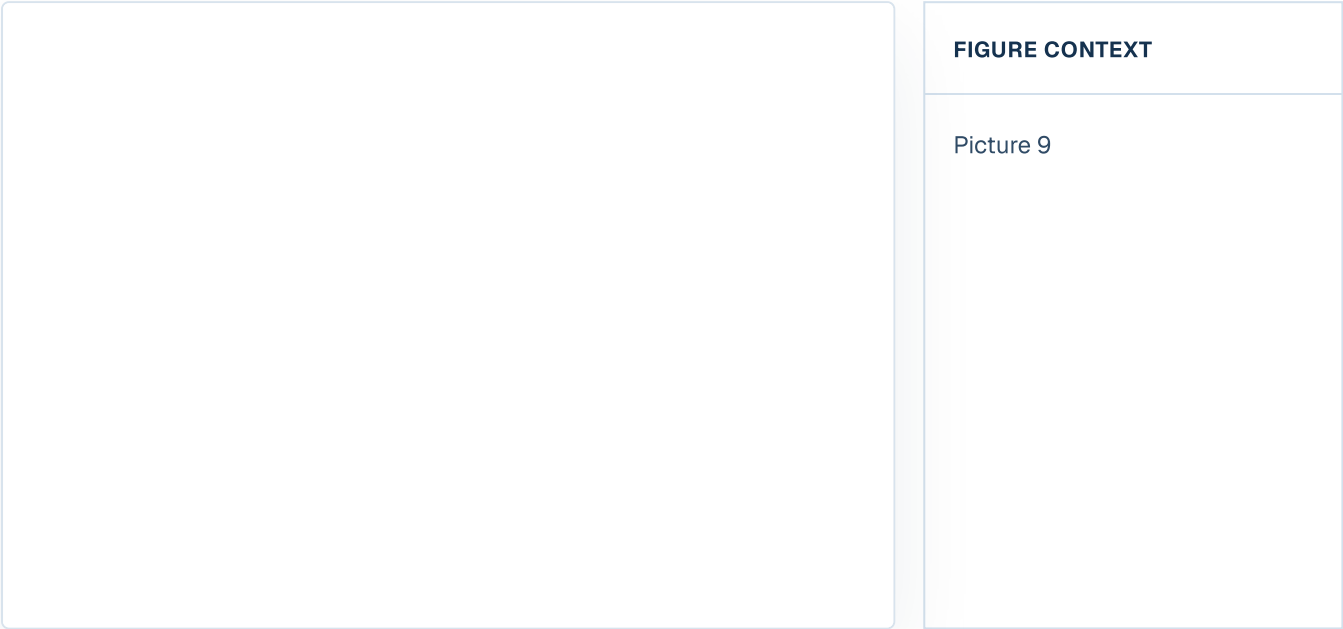
FIGURE CONTEXT

Picture 8

Original DOCX, near paragraph 22

Among those 134 ransomware/hacker disclosures, the five most active groups were 跳到主要内容 (23), Qilin (17), Akira (10), Inc Ransom (10), and LockBit 5.0 (9). The top

Figures above cover only China-related manufacturing and retail incidents in H1 2026 and do not represent a global ranking of ransomware group activity.



Original DOCX, near paragraph 24

1.3 Data breaches still mainly via anonymous chats and the dark web; dark-web incidents up 110.5%

According to Threat Hunter’s H1 2026 monitoring platform statistics, anonymous group chats and the dark web remained the primary breach channels, together accounting for 93.9%. Dark-web channel incidents rose from 2,353 in H2 2025 to 4,952, an increase of about 110.45%.

Anonymous chats still handle substantial trade matching, but high-risk incidents and public pressure disclosures are migrating more to the dark web. Enterprise monitoring and response need to cover forums, leak sites, aggregators, ransomware leak sites, and other dark-web scenarios.

跳到主要内容

Normalized trading typified by financial customer and business data continues to enter underground channels and is used for fraud, marketing, collections, and secondary resale.

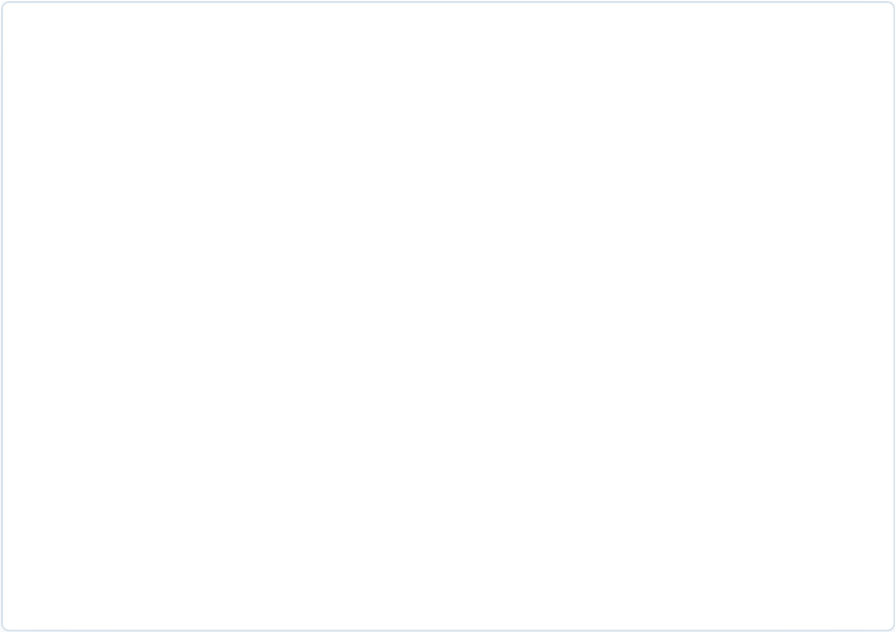


FIGURE CONTEXT
Picture 10

Original DOCX, near paragraph 28

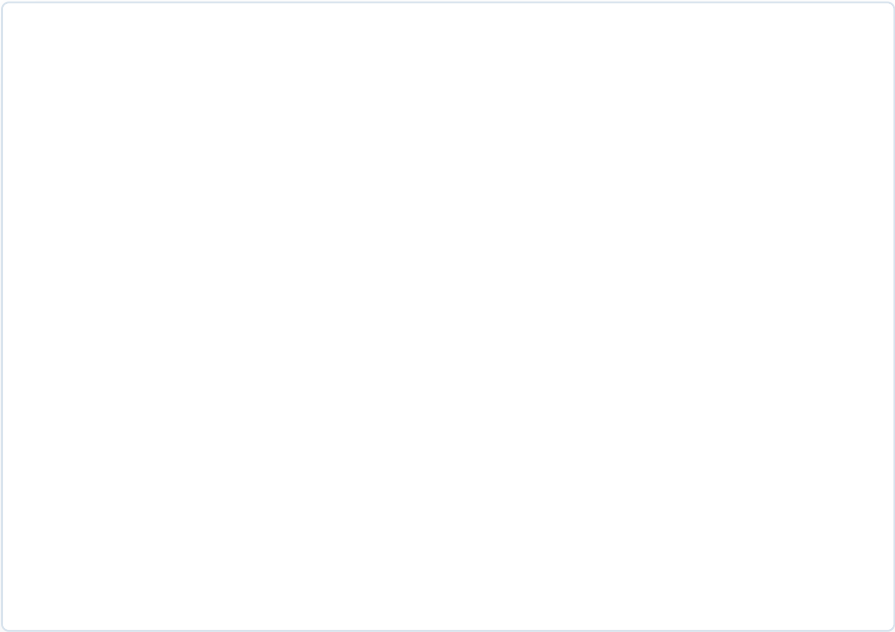


FIGURE CONTEXT
Picture 11

Original DOCX, near paragraph 28

跳到主要内容

In H1 2026, data breach incidents in the broader financial sector remained at a high level. Banking, consumer finance, securities, payments, and related areas together accounted for about 12,500 incidents—more than half of all monitored data breach incidents online—and remained among the most concentrated trading segments.

By sub-industry, banking had the highest number of data breach incidents, followed by consumer finance.

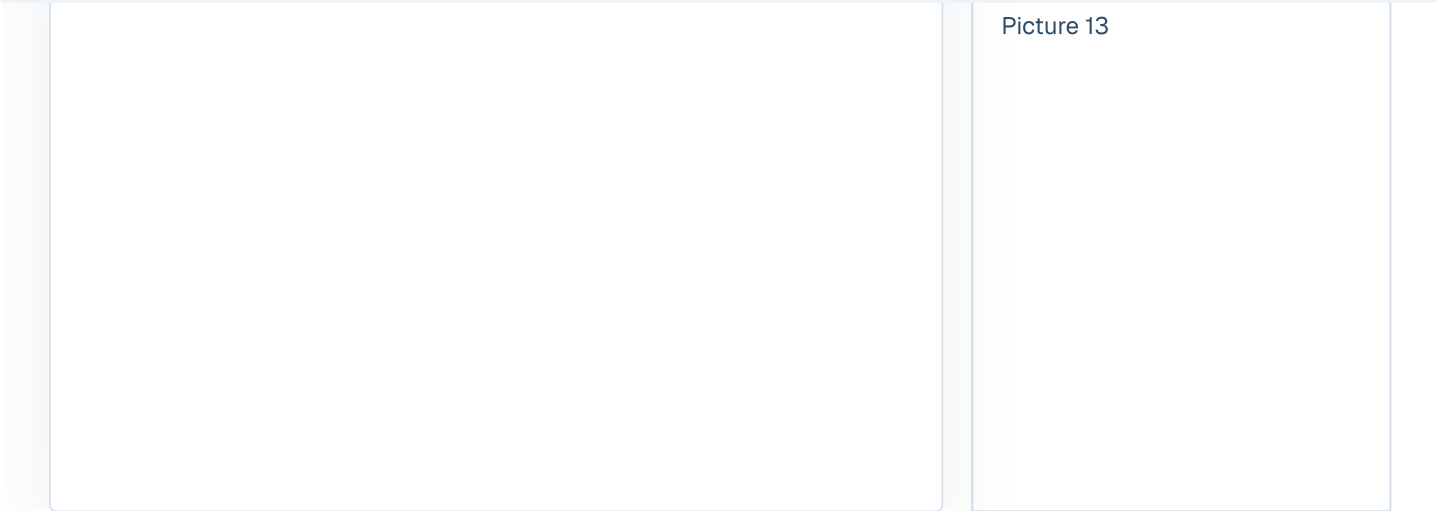


Original DOCX, near paragraph 31

From the perspective of market participants, underground attention to financial data rose further. In H1 2026, while the overall number of active groups across the network remained broadly stable, the number of groups trading financial data increased, rising from 57.0% to 68.3% of all active groups.

This indicates that more underground trading groups are treating financial data as a priority commodity, and financial data’s market attractiveness continues to strengthen.

[跳到主要内容](#)



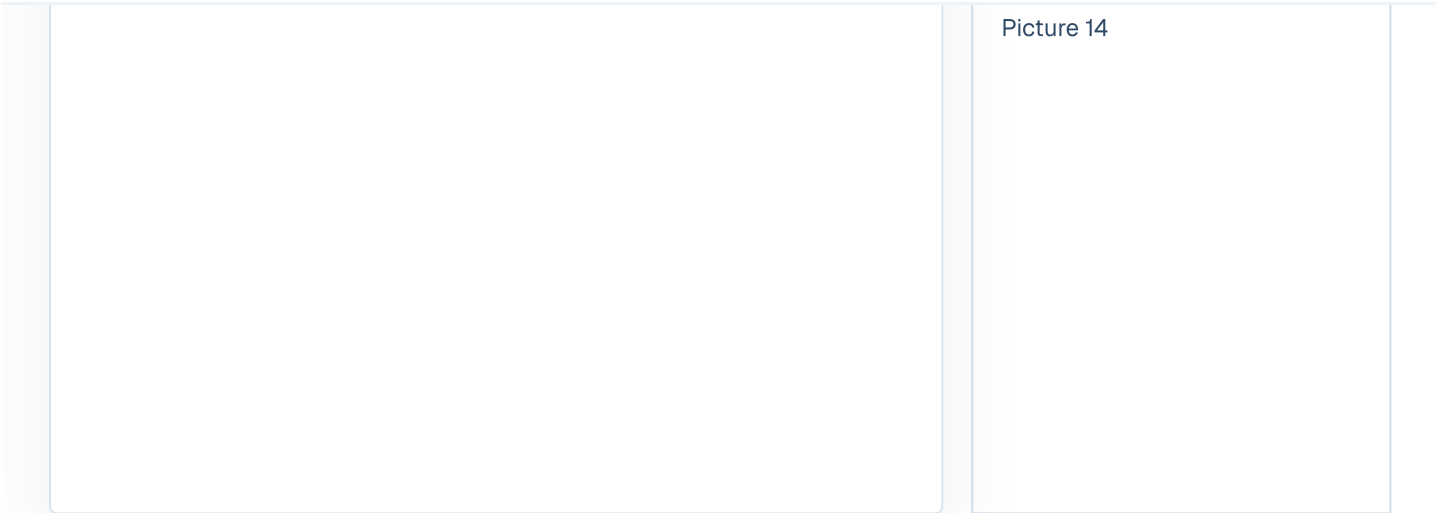
Original DOCX, near paragraph 33

By data subtype within broader financial incidents, H1 2026 financial data leaks showed divergence. Lending data still dominated and continued to grow versus H2 2025; asset management and payment data grew more notably; securities data remained broadly stable; insurance data declined.

Overall, incremental leaks continued to concentrate in lending, payments, asset management, and other datasets “closer to money.” Lending data had the largest volume and continued to grow versus H2 2025. Part II focuses on its leak pathways, sources, and downstream abuse.

Lending data breach incidents cover banks, consumer finance, online microlending, loan facilitation, risk control, collections, and other entities.

跳到主要内容



Original DOCX, near paragraph 36

II. Lending Data Breaches: End-to-End Pathways and Root Causes

Synthesizing the overall H1 2026 landscape, underground data trading currently shows two typical risk patterns:

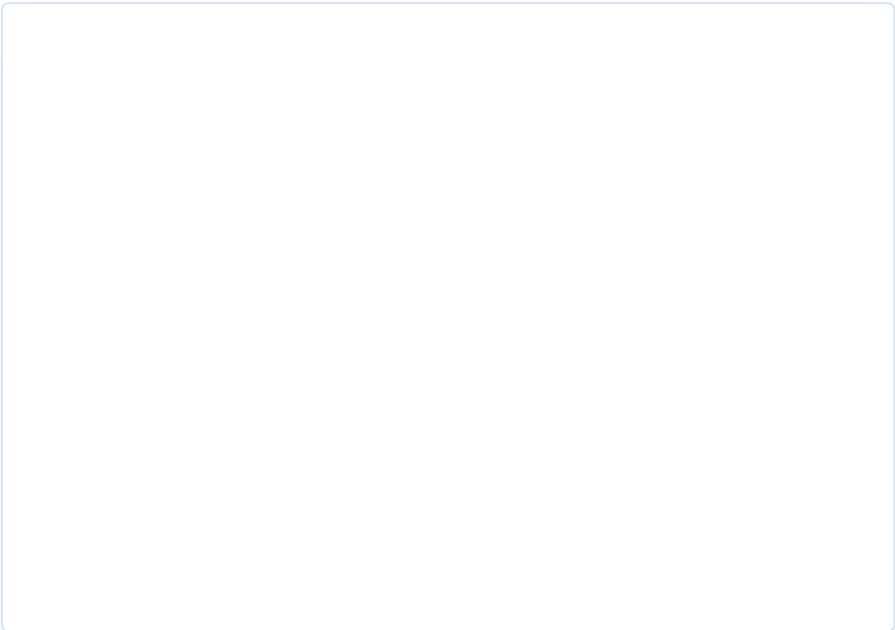
The broader financial domain covers payment transactions, asset management, securities investment, insurance policies, lending, and more. Among these, lending data has the largest incident volume, covers the most business stages, and has the most complete downstream monetization chain. Part II therefore uses lending data as a representative sample to analyze leak pathways, sources, and continued exploitation.

2.1 Lending data is the most active high-value category in the underground market

Lending data was the largest subcategory in broader financial underground trading in H1 2026, with about 6,000 related incidents—the highest industrialization level and the most complete monetization chain. Historical data continues to be repeatedly resold; newly leaked data keeps entering the market; and downstream demand from collections and fraud keeps lending data in normalized circulation.

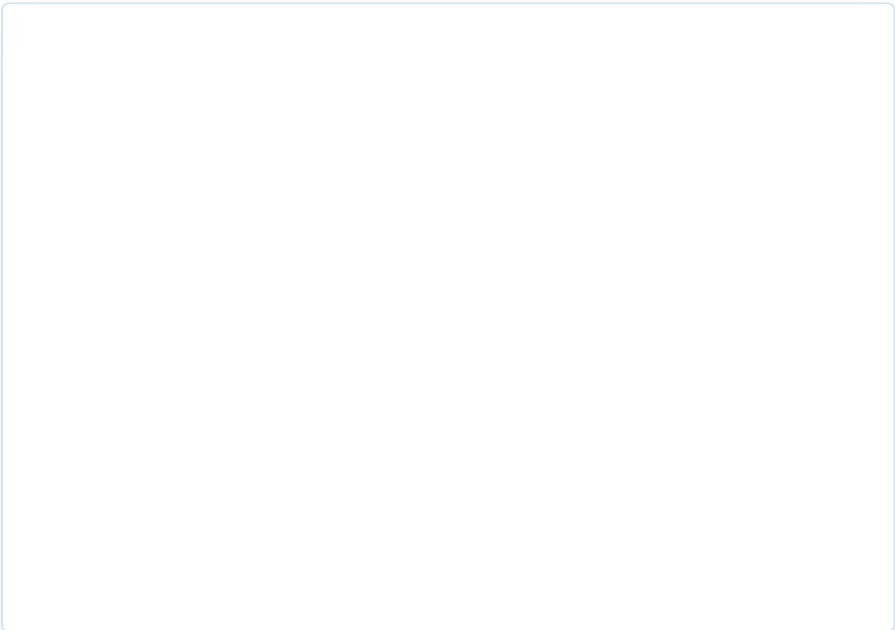
跳到主要内容

query data.



Original DOCX, near paragraph 42

FIGURE CONTEXT
Picture 15



Original DOCX, near paragraph 42

FIGURE CONTEXT
Picture 16

2.2 Lending data leaks span the full business lifecycle

跳到主要内容

intent through application, approval, disbursement, repayment, and post-loan collections, the journey typically passes through customer-acquisition platforms, registration pages, risk-control queries, credit approval, payment settlement, SMS notifications, outsourced collections, and more.

Based on traded data in the underground market, leakage and abuse of lending-related information roughly span four stages.

(1) Customer acquisition and registration

Carrier traffic and SDK/tracking data form real-time intent lists. Before a user even submits an application—while merely browsing a lending product or landing page—visit behavior may be captured at the network layer or recorded by embedded components, producing lists of people who “recently visited a lending product.” Accuracy may be limited, but coverage is wide and freshness is high; such lists are often used for telemarketing and precision marketing.

(2) Pre-loan approval

Multi-lending and risk-control query data are higher value. These records capture query actions after a user initiates an application and may include maximum overdue amount, longest overdue days, and current/historical lender counts. Originally used for risk identification, once leaked they reverse into tools for screening multi-liable or urgently cash-strapped populations. Field characteristics and trading descriptions in some incidents suggest sources may involve upstream risk-control, credit reporting, and data-service supply chains—not necessarily the lenders themselves.

(3) Mid-loan and disbursement

disbursement lists are the trading mainstay. Online lending, loan facilitation, financing guarantees, phone rental, IOUs, and similar scenarios accumulate

[跳到主要内容](#)

smaller platforms and extensive external system integrations may be among the reasons such data continues to leak.

(4) Post-loan

Overdue collection data and SMS-channel data create long-tail harm. Overdue and collection lists point to populations under repayment pressure and are easily abused for fake collections, secondary collections, and impersonation of customer service. SMS-channel risk should be distinguished into two types: number leads produced by carrier-side bulk SMS signature channels; and plaintext SMS content from breached or hijacked SMS channel providers—the latter may span multiple carriers and platforms and have broader impact.

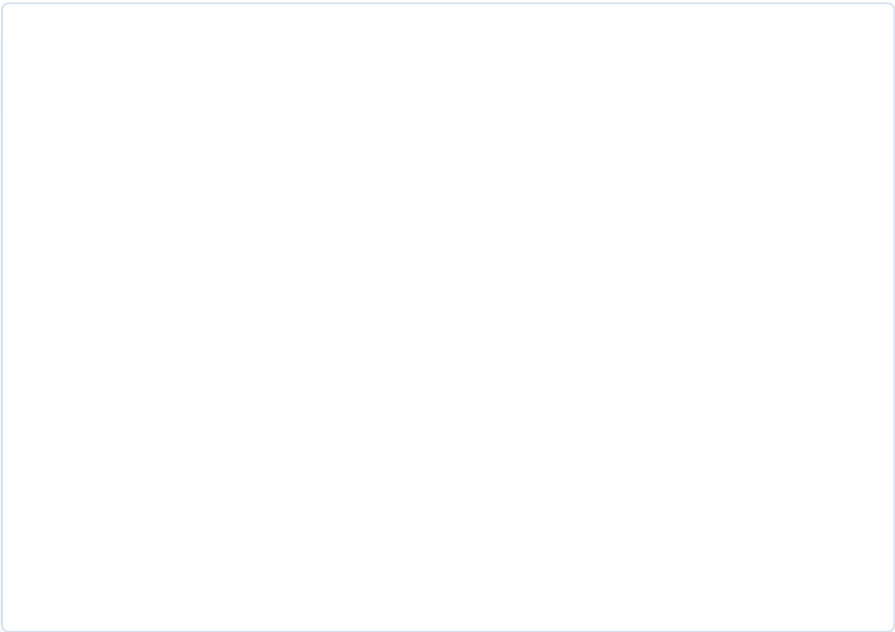


FIGURE CONTEXT

Picture 17

Original DOCX, near paragraph 53

Institutions involved: large banks and online lending / loan-facilitation platforms share high exposure

跳到主要内容 data breach incidents where the involved institution could be clearly identified, large state-owned banks and online microlending / loan-facilitation

finance institutions about 7.4%; and city/rural commercial banks about 5.8%.

This structure shows that lending data risk is not limited to smaller platforms with weaker security. Although large licensed institutions typically have more mature internal security systems, their businesses still require external services such as loan facilitation, risk control, credit reporting, SMS, and collections—and related data may still leak along those external service chains.

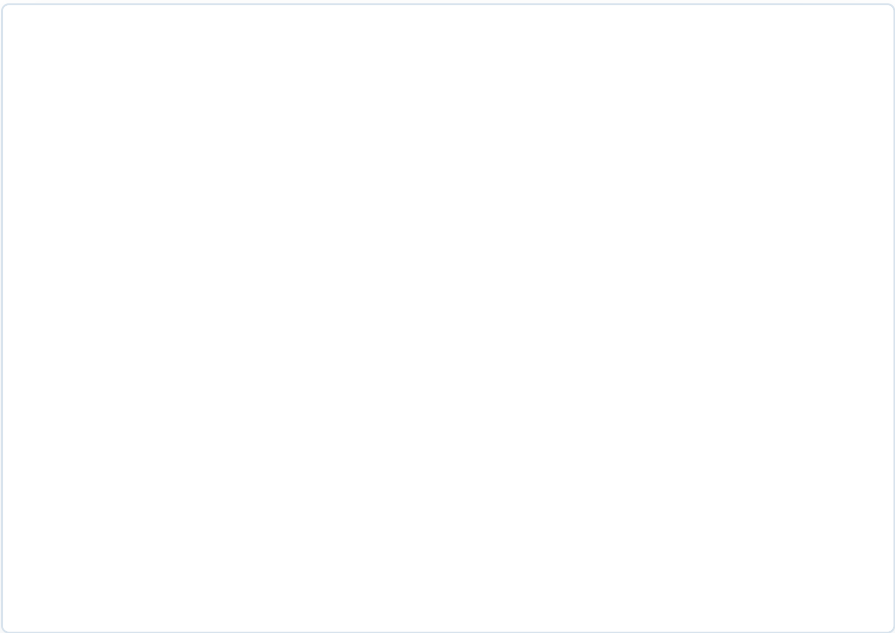


FIGURE CONTEXT

Picture 18

Original DOCX, near paragraph 56

2.3 Third-party supply chains are the primary source of lending data leaks

Based on Threat Hunter’s source analysis of lending data breach incidents, among attributable cases in H1 2026, third-party supply chains accounted for about 44%; carrier channels about 23%; system penetration about 16%; API privilege abuse about 9%; insider leakage about 6%; and SMS-channel-related risk about 2%.

In attributable samples, third-party supply-chain leaks held the largest share. Lending
跳到主要内容 early diffused from single institutions’ interiors toward external service

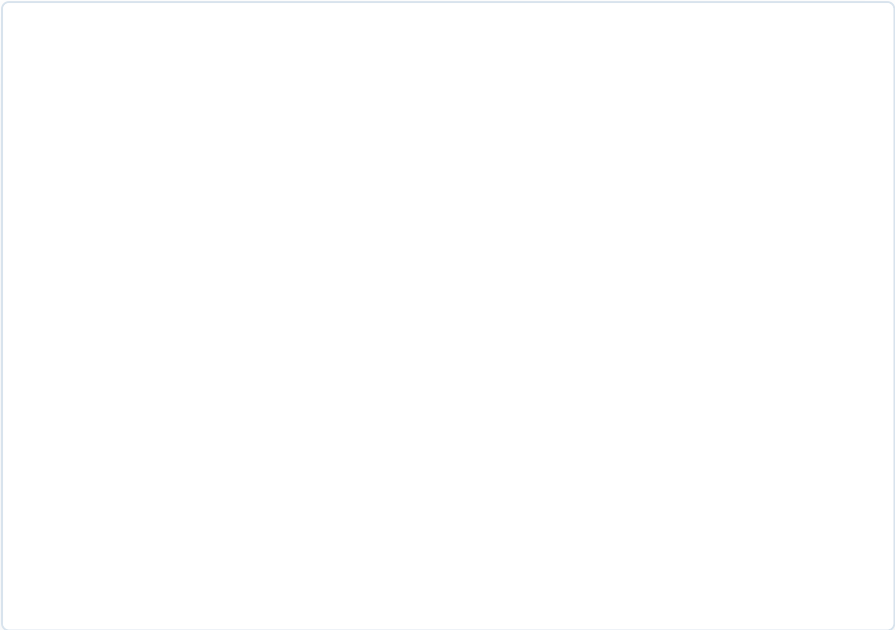


FIGURE CONTEXT

Picture 19

Original DOCX, near paragraph 59

By source, H1 2026 saw a further rise in third-party supply-chain-related incidents, while SMS-channel hijacking incidents fell notably. Even so, the business harm and diffusion potential of SMS-channel hijacking remain significant and warrant continued monitoring. Poorly managed SMS channels can still be used for fake collection messages, fraud SMS, phishing links, and precision user outreach.

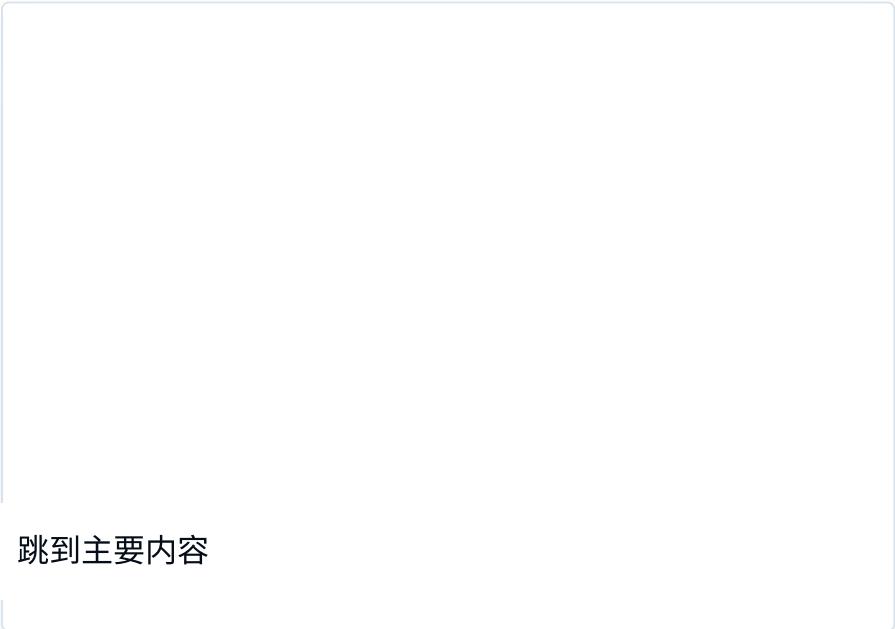


FIGURE CONTEXT

Picture 20

跳到主要内容

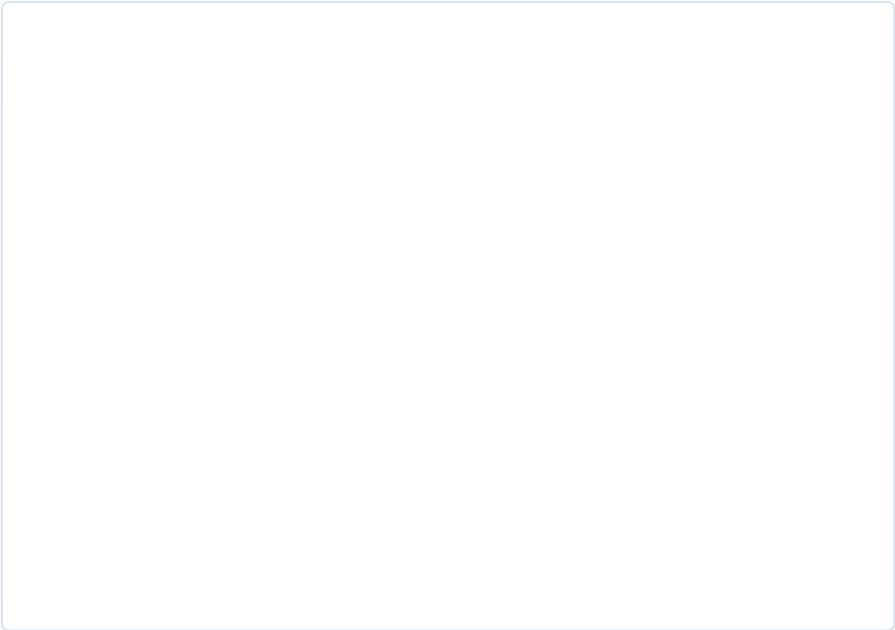


FIGURE CONTEXT
Picture 21

Original DOCX, near paragraph 60

2.4 Enterprises should bring third-party supply chains into the core scope of lending data breach governance

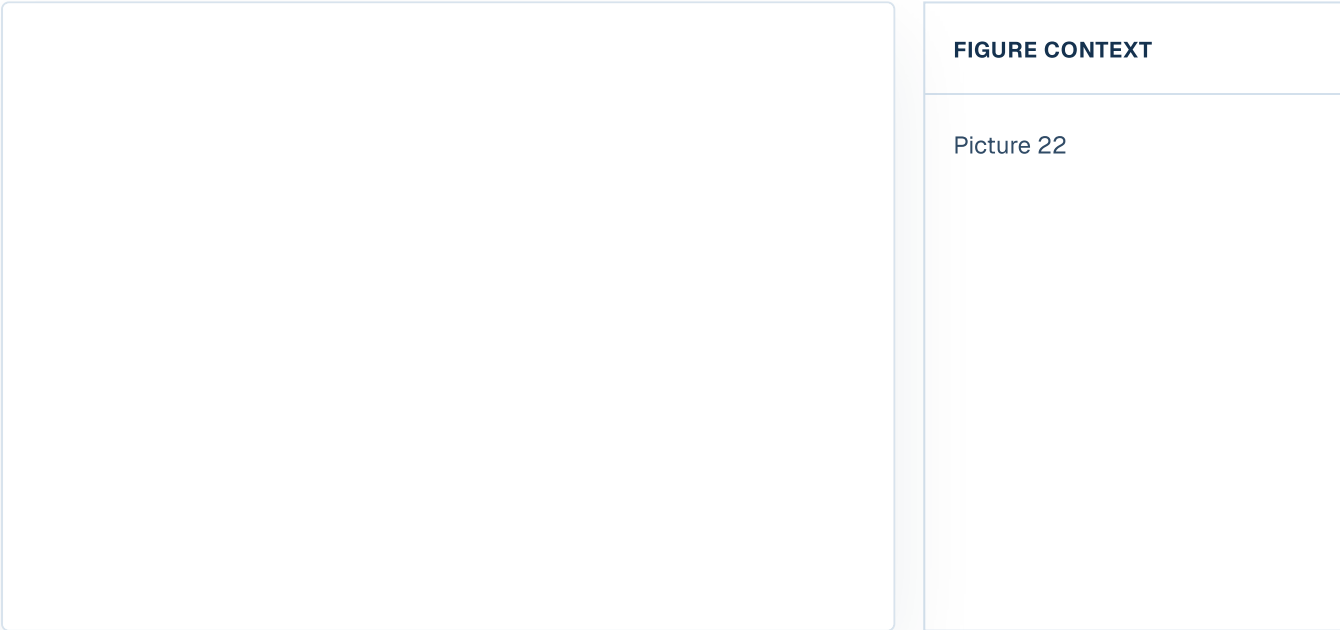
Lending businesses depend on multiple external service nodes—risk control, credit reporting, loan facilitation, SMS, and collections. Once data enters third-party processing chains, institutions’ visibility into data flows, sub-delegation relationships, API calls, and historical retention declines. Some data may continue to secondary and tertiary vendors, ultimately leaking at supply-chain ends that the original institution can barely audit directly.

Moreover, multiple financial institutions may share the same service provider. Once an external node is compromised, many enterprises may be affected at once. An absence of detectable intrusion inside an institution’s own systems does not mean related data has not leaked along external chains. Lending data governance must extend from protecting owned systems to third-party supply-chain management.

跳到主要内容
Hard to control mainly because supplier chains are opaque, internal systems may show no clear alerts, and discovery often lags. Enterprises may first find

Therefore, lending institutions’ governance focus should expand from protecting owned systems to supply-chain management and external risk monitoring. Enterprises need stronger vendor onboarding and ongoing assessment, clearer requirements on sub-delegation and data retention, monitoring of anomalous API calls and bulk extraction, and continuous attention to brand, product, field, and sample signals in underground channels—followed by timely authenticity validation and incident attribution.

These measures mainly help reduce new leaks and supply-chain control loss; they cannot eliminate the stock of data already in underground markets. Exfiltrated data may still be retained long-term, repeatedly traded, and continue to cause harm across downstream scenarios.



Original DOCX, near paragraph 66

2.5 Continued exploitation after data leaves: outbound fraud, fake collections, and
document in parallel
跳到主要内容

calls, fake collections, precision marketing, and personal-information enrichment. Outbound fraud and fake collections most readily cause direct user losses; record-check and similar enrichment services further deepen and amplify the harm of the original leak.

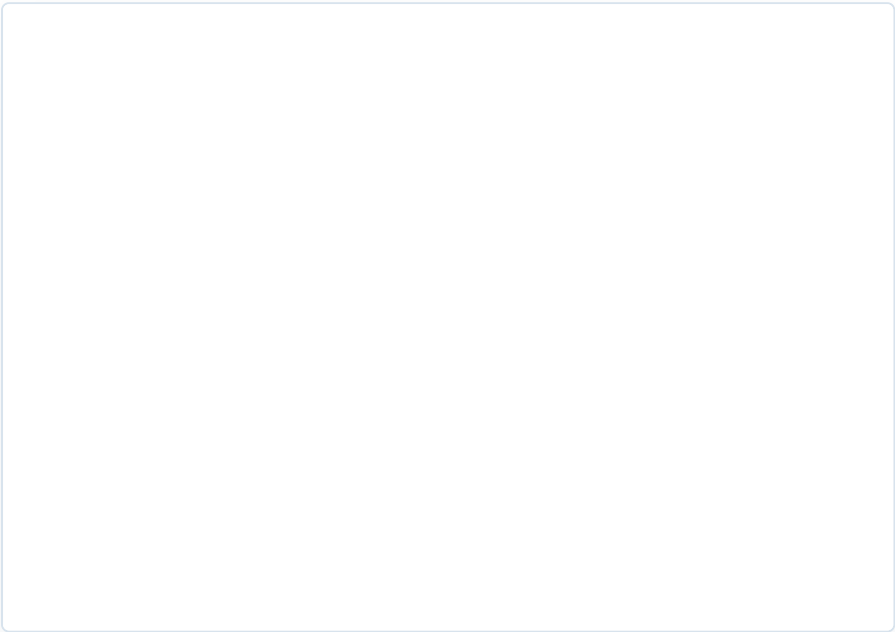


FIGURE CONTEXT

Picture 23

Original DOCX, near paragraph 68

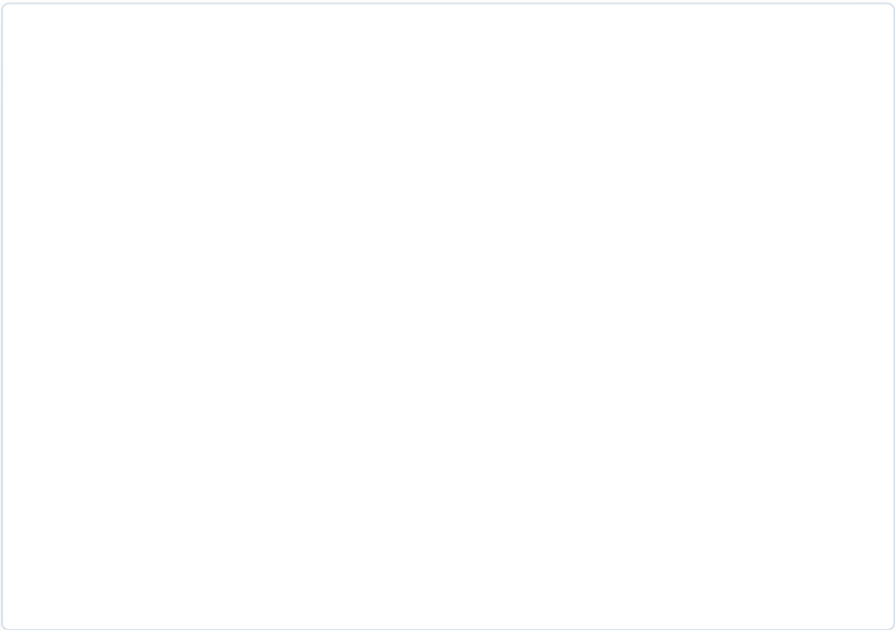


FIGURE CONTEXT

Picture 24

跳到主要内容 r paragraph 68

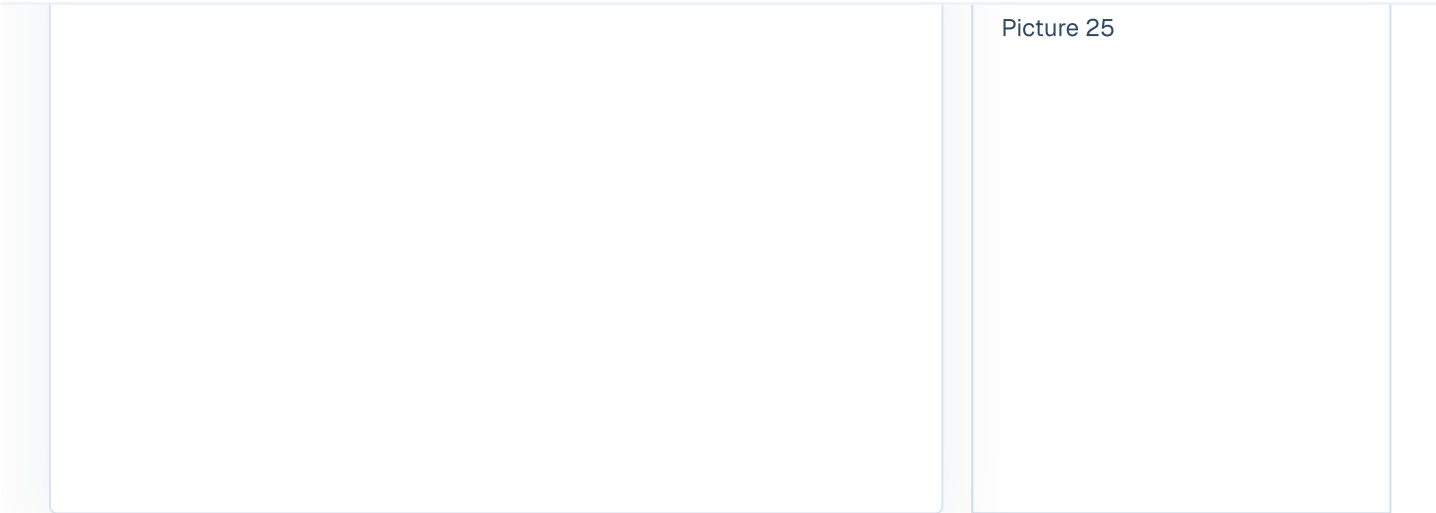
Lists of users who have just applied and are still awaiting approval or disbursement may be rapidly loaded into autodial systems. Fraud groups contact users ahead of legitimate platforms, impersonating customer service or loan reviewers and inducing transfers with claims such as “account anomaly,” “credit freeze,” or “processing fees.” Because the fraud timing closely coincides with the user’s real loan application, such scripts more readily win trust.

(2) Secondary collections and fake collections

After collection, overdue, and disbursement data leak, underground actors can impersonate collectors using lender name, loan amount, disbursement time, overdue status, and bound card numbers—pressuring users via fake collection SMS/calls or high-fidelity repayment pages to induce transfers.

For example, in March 2026 the Beijing financial regulator issued a consumer risk alert on “loan collection” SMS fraud. Public reports described typical tactics including impersonating legitimate financial institutions to send collection SMS, directing users to high-fidelity websites, coercing transfers with claims such as “overdue penalties doubling” or “being placed on a credit blacklist,” and harvesting sensitive information under pretexts such as “identity verification” or “confirming repayment intent.”

[跳到主要内容](#)



Original DOCX, near paragraph 73

(3) Repeated resale and cross-scenario reuse

Lending data risk does not end when the original leak source is cut off. Once data enters the underground market, it may be copied, cleaned, reclassified, and repackaged, then repeatedly resold across groups and channels. Even after an enterprise has patched vulnerabilities, handled accounts, or remediated vendors, already-exfiltrated data may continue to fuel outbound fraud, fake collections, precision marketing, and other downstream scenarios.

If the post-loan stage sees a concentrated wave of anomalous customer complaints in which callers accurately cite lender, loan amount, disbursement time, overdue status, or bound card numbers, enterprises should consider the possibility that historically leaked data is being reused. Such anomalies do not necessarily mean a new recent leak; they may stem from continued circulation and secondary monetization of earlier exfiltrated data in the underground market.

Typical case:

跳到主要内容
bserved that a lending platform received a large volume of user
ite 2025 alleging harassment by “fake collectors.” Investigation found

underground and used for collection fraud and secondary monetization. In underground markets, so-called “first-hand overdue data” containing overdue timing, loan amounts, and contact details has long-standing trading demand. This case shows that data breach response cannot end solely when “the leak source is cut off.” When assessing impact, enterprises must also factor in the subsequent trading and exploitation cycle of exfiltrated data. A concentrated wave of fake-collection complaints that accurately cite loan details is itself a leak signal worth retrospective investigation.

(4) Record-check enrichment and expansion of financial profiles

Fields in lending data—mobile numbers, ID numbers, bank card numbers, and similar—can become query entry points for further record checks. Underground actors may then enrich linked bank cards, account balances, bank statements, credit reports, and payment transactions, inferring account holdings, asset status, fund activity, and repayment capacity. Data that originally reflected a single lending event is thereby expanded into a fuller personal financial profile, used to raise fraud-script credibility, enable fake collections, or continue resale.

Record checks are a critical link in the chain of “clue verification → field enrichment → profile expansion → remonetization.” They are not a separate risk disconnected from lending data, but an important way leaked data is further exploited downstream. Part III builds on this to analyze the market structure of illegal record checks, with a focus on data security and regulatory risks from abused bank and payment query privileges.

Beyond repeated resale and direct abuse, fields such as mobile numbers, ID numbers, and bank card numbers in lending data can also become entry points for further personal-information queries, allowing original data to be enriched and expanded checks.

[跳到主要内容](#)

Record checks are an underground trading mode of querying personal information on a per-person basis. Buyers provide clues such as mobile numbers, ID numbers, or bank card numbers; sellers return financial, household registration, telecom, travel, and other information per query. Data from different sources can also be cross-stitched to gradually reconstruct identity, assets, and activity trails. According to Threat Hunter monitoring, there were about 2,800 related incidents over the past year, forming a stable trading market. The following focuses on financial record checks, using high-risk query items such as bank accounts, balances, and statements as examples.

Over the past one to two years, cases of illegally obtaining and trading citizens' personal information have been repeatedly disclosed publicly, and national crackdowns on crimes infringing citizens' personal information have continued. Yet according to Threat Hunter monitoring, the record-check underground has not disappeared: the share of judicial/public-security style checks among record-check incidents rose from 5.3% in H2 2025 to 12.5% in H1 2026. Persistent demand, plus supply that relies on dispersed internal privileges and data interfaces across industries and cannot be eradicated in one stroke—these are the roots of its resilience.

3.1 Record-check market structure: specialized proxy checks dominate; financial queries rank first

3.1.1 Trading modes: clear division between specialized proxy checks and social-engineering databases

By trading form, record checks mainly fall into specialized proxy checks and social-engineering database (SE database) queries. Specialized proxy checks account for about 84%; SE database queries about 16%.

跳到主要内容 xy checks are also known underground as “manual callbacks.” Sellers typically return information directed by the buyer's query clues. Ads often promote

external service APIs, or other illicit acquisition channels.

SE database queries mainly rely on historical leak datasets and automated bots for retrieval, often attracting users with “free, instant, self-serve” offers. Some groups first use SE databases to provide low-cost or free basic information, then sell more timely, deeper financial, telecom, and household-registration specialized proxy checks as paid items.

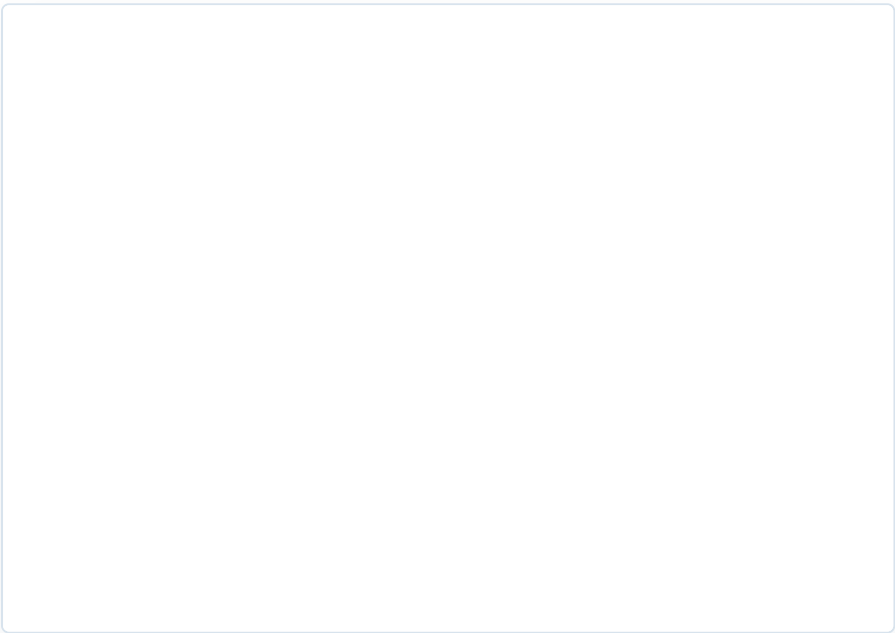


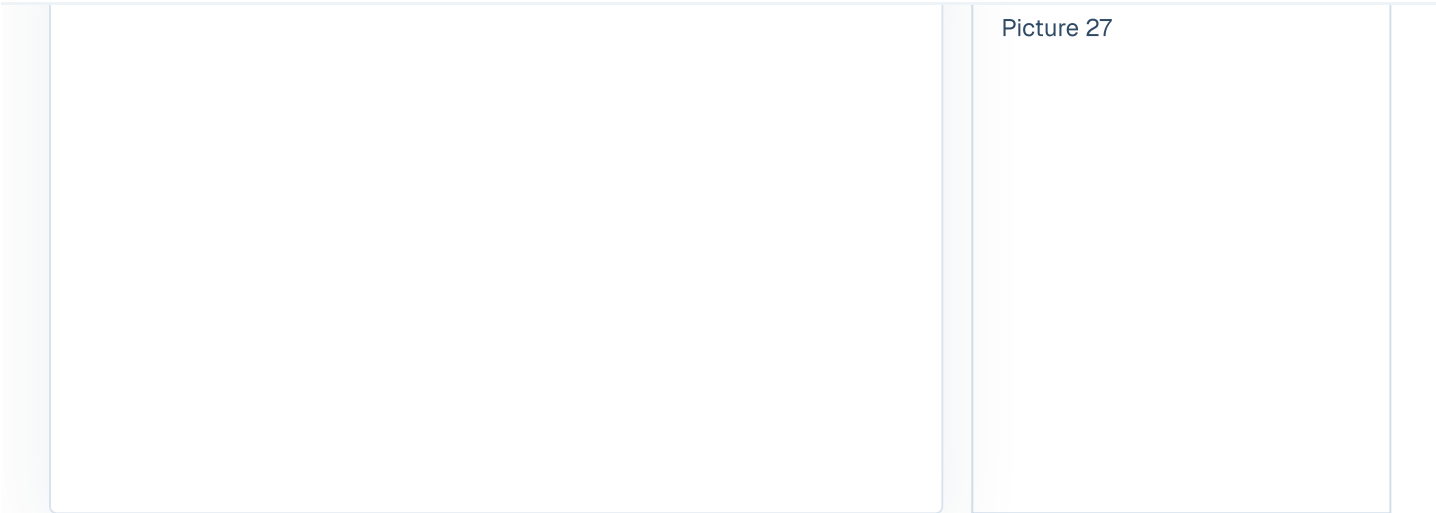
FIGURE CONTEXT

Picture 26

Original DOCX, near paragraph 90

Left: specialized proxy-check ads offering per-person queries with language such as “manual callback” and “forced login to banking apps.” Right: SE-database bots using free or low-cost automated search as a funnel.

跳到主要内容



Picture 27

Original DOCX, near paragraph 91

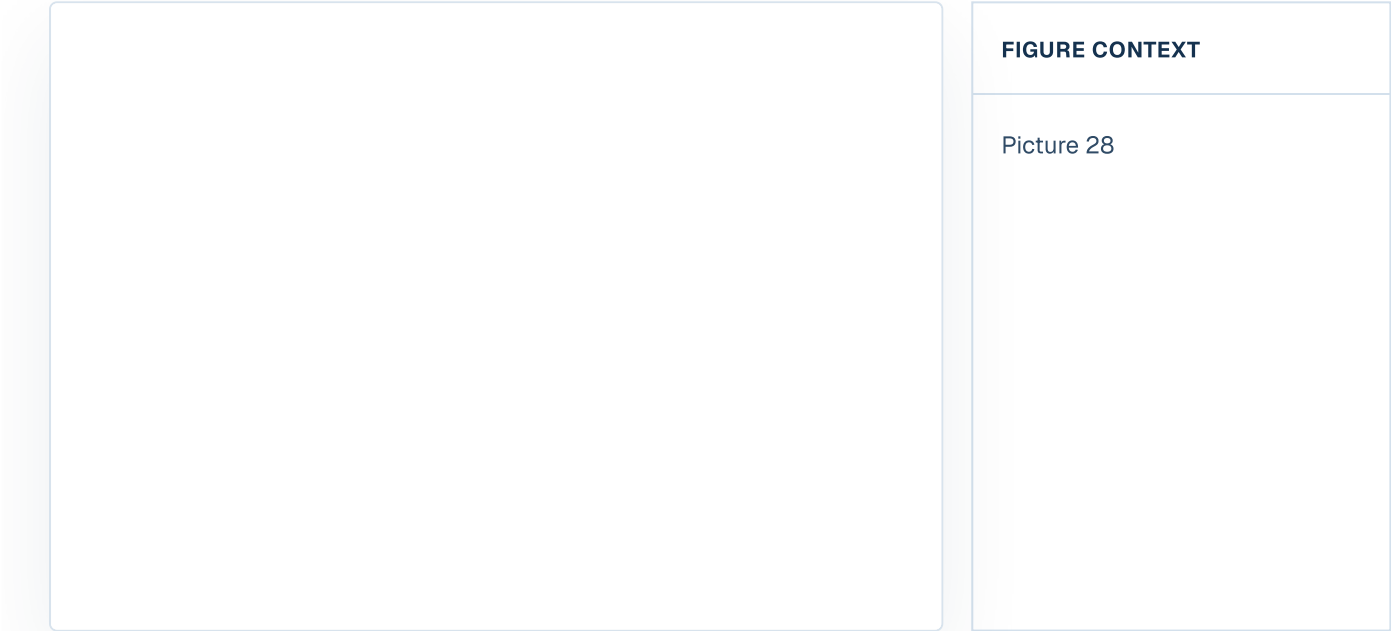


FIGURE CONTEXT

Picture 28

Original DOCX, near paragraph 91

3.1.2 Query content: financial categories highest; record checks span multiple industries

By query content, financial, parcel/e-commerce/logistics, and identity/household registration categories were elevated. Financial accounted for about 23.4%—highest
跳到主要内容 check targets; parcel/e-commerce/logistics about 21.3%;
old registration about 18.2%.

These fields can not only verify identity but also reflect account holdings, asset status, fund activity, and repayment capacity—and are readily used for precision fraud, fake collections, debt pressure, extortion, and secondary resale.



Original DOCX, near paragraph 94

3.2 Commoditization of bank information queries: single queries packaged as tiered priced services

Bank accounts, account balances, bank statements, account-opening information, and corporate accounts are high-risk content within financial record checks. The underground market often packages such queries as per-query paid services using language such as “counter,” “card-opening hotline,” and “internal direct pull.”

Unlike selling historical data packages, the core of this trade is not a one-time sale of fixed data, but continuously charging for the ability to query information per person. Buyers can start from mobile numbers, ID numbers, or bank card numbers and .. ing account relationships, fund activity, and asset information.

跳到主要内容

balance items are often used for quick localization; bank statements are usually priced by lookback window; corporate accounts and cross-institution / cross-domain combo queries command higher prices.



Original DOCX, near paragraph 98

Sample public quotes for underground bank-statement queries:



跳到主要内容

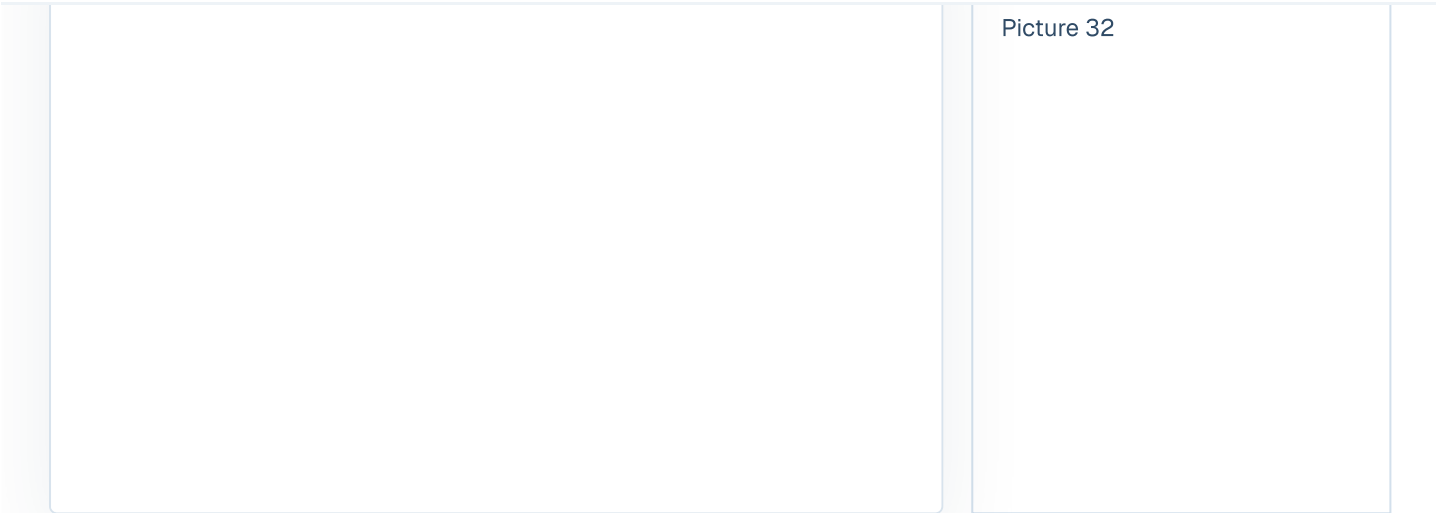
Original DOCX, near paragraph 99

The main difference between financial record checks and ordinary historical data-package resale is that sellers claim they can continuously return query results on a per-person, per-query basis. Paths to this capability are not singular: they may involve personnel with legitimate privileges making unauthorized queries; employee, privileged, or service accounts taken over via credential leaks or session theft; or uncontrolled outsourced accounts, partner accounts, or query APIs.

Underground ad language such as “real-time,” “internal direct pull,” “counter,” and “callback available” reflects attempts to convert query privileges meant for normal business into continuously charged underground services. For accounts with privileges to query customer information, export results, or call APIs, once privilege abuse or account takeover occurs, risk may expand from a single compromised account into ongoing query and bulk outward sale of data.

Threat Hunter’s ATO monitoring watches externally leaked accounts, passwords, and related identity markers, and secondarily matches them against employee emails, mobile numbers, UIDs, login behavior, and high-value account tags to identify accounts with realistic takeover potential. If a matched account also has privileges for customer-information queries, data export, or API calls, harm may expand from a single account compromise to abuse of high-privilege query capability.

[跳到主要内容](#)



Original DOCX, near paragraph 103

3.4 Data security accountability further extends to business, technology, and operations personnel

Underground financial record checks reflect the risk that query privileges and sensitive information may be exploited externally. Recent data security enforcement cases further show that banks’ and payment institutions’ data security accountability is borne not only by the institution, but also further assigned to relevant business, technology, and operations responsible persons.

Note: the enforcement cases below do not necessarily map directly to illegal record-check incidents, but their themes—data security management, privilege control, third-party risk, and accountability of responsible persons—are closely related to governance issues exposed by financial record checks.

Since 2026, the banking sector has seen multiple regulatory penalty cases involving data security and personal information protection; some fines directly involved insufficient third-party cooperative data security risk controls, privilege management, and data governance mechanisms.

[跳到主要内容](#)

retail finance and operations/maintenance were each fined RMB 140,000. The case shows data security accountability is borne not only by the institution, but also further assigned to business units and technology/operations roles.

Payment institution data security responsible-person penalty case — A payment institution was penalized for violations in account management, clearing management, and data security management; related technology responsible persons were also penalized for liability in data security violations. The case shows payment institutions' data security accountability may likewise reach technology and systems management roles.

Overall, illegal record checks are expanding from single-item information queries toward multi-field stitching and personal financial profiles—especially bank cards, balances, statements, credit reports, and payment transactions, which combine high sensitivity, direct monetizability, and lasting harm. Related enforcement cases also indicate that financial data security accountability has extended from the institutional level further to relevant business, technology, and operations responsible persons.

IV. Conclusion

In H1 2026, the underground data trading market remained elevated; the dark web's share of data circulation channels rose markedly; third-party supply chains became a major source of lending data leaks; and finance-related data remained a priority underground commodity.

Risk after lending data leaves no longer stops at a single leak: data may be repeatedly resold and, through record checks, enriched with account, asset, and transaction information to gradually form personal financial profiles. The per-person, per-query ~~delivery mode~~ in financial record checks also shows underground actors extending [跳到主要内容](#) tic data packages to selling query capability—potentially involving privileged-access abuse, account takeover, or uncontrolled APIs. Related regulatory

responsible persons.

Translation note: This English edition translates the full body text of Threat Hunter's H1 2026 China Data Breach Risk Trends Report and includes English recreations or annotated versions of all figures from the Chinese original. Institution and product names follow common English usage where established (e.g., Threat Hunter, LockBit).

Complete report

Download the English PDF

The English PDF is stored. Internal preview does not count as a public download.

PDF available (preview)

Related research

Continue reading

Return to research



跳到主要内容

Half are gone in 30 days. Three in ten return after 90. Threat Hunter monitored 48,222 SMS-receiving numbers in July 2026: 56% appear once or span 30 days or less, and 32.7% are seen again after 90 days. These numbers are shelf inventory, so judge them on last-seen.

machine from a person?

8 devices, 75,000+ events, 9 dimensions: a robotic arm can look human on one signal; combinations of contact area, trajectory, and pressure are harder to fake.