TH THREAT HUNTER RESEARCH

2026 SPECIAL THREAT REPORT · PUBLIC RELEASE EDITION

Off-Network Fraud Evolution: From Forged Demand Letters to Auto-Recall Scams

Between January and November 2026, tightened telecom filtering and MIIT Order No. 74 shut down bulk SMS channels. Rather than retreating, fake debt-collection networks upgraded into forged legal demand letters, shifted outreach through OS-native iOS IP messaging and QR-free, link-only express mailers, and reused modular multi-scam infrastructure to spill rapidly into nationwide vehicle-recall scams affecting consumer-finance borrowers.

STAGE 01 · TELECOM CRACKDOWN

SMS Gateways Close

MIIT Order No. 74 collapses legacy bulk-SMS collection campaigns.

STAGE 02 · TWO-HOP BYPASS

iOS IP Msg → Link-Only Mail

Stamped demand letters + printed short URLs bypass telecom & QR checks.

STAGE 03 · INDUSTRY SPILLOVER

Shared Base → 800k+ Recall

Pre-staged domains convert recall panic into concealed consumer-finance NPLs.

Threat Hunter Research Team · Complete English Edition Monitoring Window: Jan–Nov 2026 · www.threathunter.com

Research Scope & Monitoring Window: Between January and November 2026, tightened telecom filtering and the enforcement of Ministry of Industry and Information Technology (MIIT) Order No. 74 shut down bulk SMS channels. Rather than retreating, fake debt-collection rings completed a full off-network transition: upgrading phone scripts into convincing forged legal demand letters, migrating outreach in two hops—from SMS to OS-native IP messaging on iOS devices and then to QR-free, link-only door-to-door mailers—and reusing shared multi-scam infrastructure to spill rapidly into real public events such as nationwide vehicle recalls. Based on Threat Hunter's year-round monitoring, this report reconstructs that evolution and provides early-warning intelligence for consumer-finance institutions, express logistics providers, automakers, and the public.

Executive Summary: The 2026 Off-Network Generational Shift

In 2026, fake debt-collection operations completed a generational shift off traditional telecom networks. As major domestic carriers tightened link and contact-detail filtering and MIIT Order No. 74 took effect on May 1, low-cost bulk SMS collection scams quickly collapsed. Threat Hunter's monitoring from January through November shows that cybercriminal groups did not shrink; around June, they overhauled their channels, scripts, and underlying infrastructure—shifting online outreach to OS-native IP messaging on iOS devices carrying high-fidelity forged legal demand letters, while moving offline outreach onto legitimate express couriers that put printed notices directly into victims' hands.

An even sharper tactical adaptation emerged after late October. Following police raids on illicit print-and-mail hubs and stricter courier checks on letters containing QR codes, fraud rings rapidly rolled out **"QR-free, link-only + paid call-ahead door-to-door mailers."** By stripping out QR codes and printing a short URL for recipients to type manually into their phone's native browser, attackers simultaneously bypassed courier QR inspections and the built-in anti-fraud warning screens of major chat and payment apps. Infrastructure tracing further reveals that fake debt collection is not a standalone scheme—it runs as an add-on campaign atop modular cybercrime infrastructure combining device-level lead screening, reusable mobile web-page templates, and two-year domain pools pre-registered roughly three months in advance. The November vehicle-recall scams targeting car owners demonstrate how fast these same assets can be reskinned around real public news.

Online Channel Surge Peak (June)

32,112 records

Monthly underground activity around iOS native IP messaging surged as SMS script recruitment plunged from a May peak of 3,418.

QR-Free Link-Only Mailers (Nov 1–22)

~5x MoM surge

Jumped from 23 listings when first spotted in October to 114 in the first 22 days of November, bypassing courier and QR defenses.

Pre-Staged Domain Inventory (July 29)

42 domains / 50 min

Two-year domains for fake debt collection and auto-recall scams were registered in interleaved bursts, then held dormant for 88–102 days.

Infrastructure Takedown Agility

3 gens in 6 days

One origin server hosted 5+ fraud categories; after takedowns, spoofed sites rotated domains in 5 days and moved offshore.

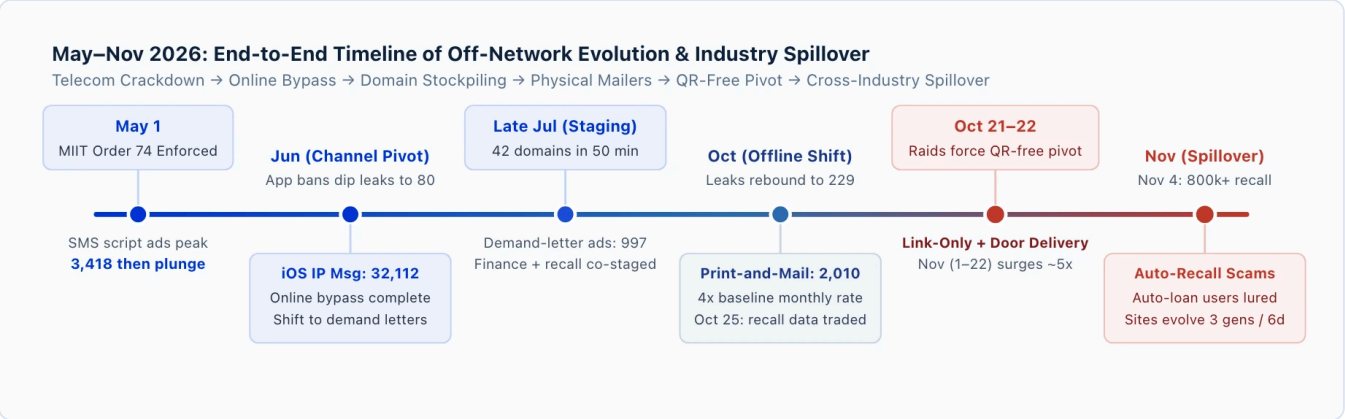


Figure 1. End-to-end timeline of off-network fraud evolution and cross-industry spillover, May–November 2026. · Source: Threat Hunter Research Team

Four Core Assessments

1. **Higher verification threshold:** The scam moved from live phone or SMS persuasion to an automated, document-led workflow, raising the recipient's burden from spotting an unfamiliar number to authenticating a formal legal demand letter.
2. **Physical off-network shift and QR-free evasion:** Outreach progressed through four stages—SMS, iOS native IP messaging, QR-coded mailers, and QR-free, link-only door-to-door mailers—creating blind spots in both telecom filtering and QR-only screening.
3. **Modular shared infrastructure:** The June dip in upstream consumer-finance data leaks reflected channel migration after mass bans on an encrypted messaging app rather than falling supply (rebounding to 229 incidents in October). Because fake collection is merely one bolt-on campaign running atop multi-scam infrastructure, taking down front-end pages alone delivers limited impact.
4. **Spillover onto real public events:** The auto-recall scam shows that mature cybercriminal groups do not lack technical capacity—they wait for real public news that compels clicks, then steer auto-loan customers into legitimate borrowing flows that turn into concealed non-performing loans (NPLs) for lenders.

Part 1. Under Regulatory Pressure: Why Fake Debt Collection Survived the SMS Crackdown

June 2026 marked a clear structural inflection point. Before June, fake debt-collection operators relied mainly on phone calls and text messages impersonating loan collectors. From June onward, operations shifted decisively toward delivering realistic forged legal demand letters that direct recipients to spoofed portals to "repay" or "verify funds."

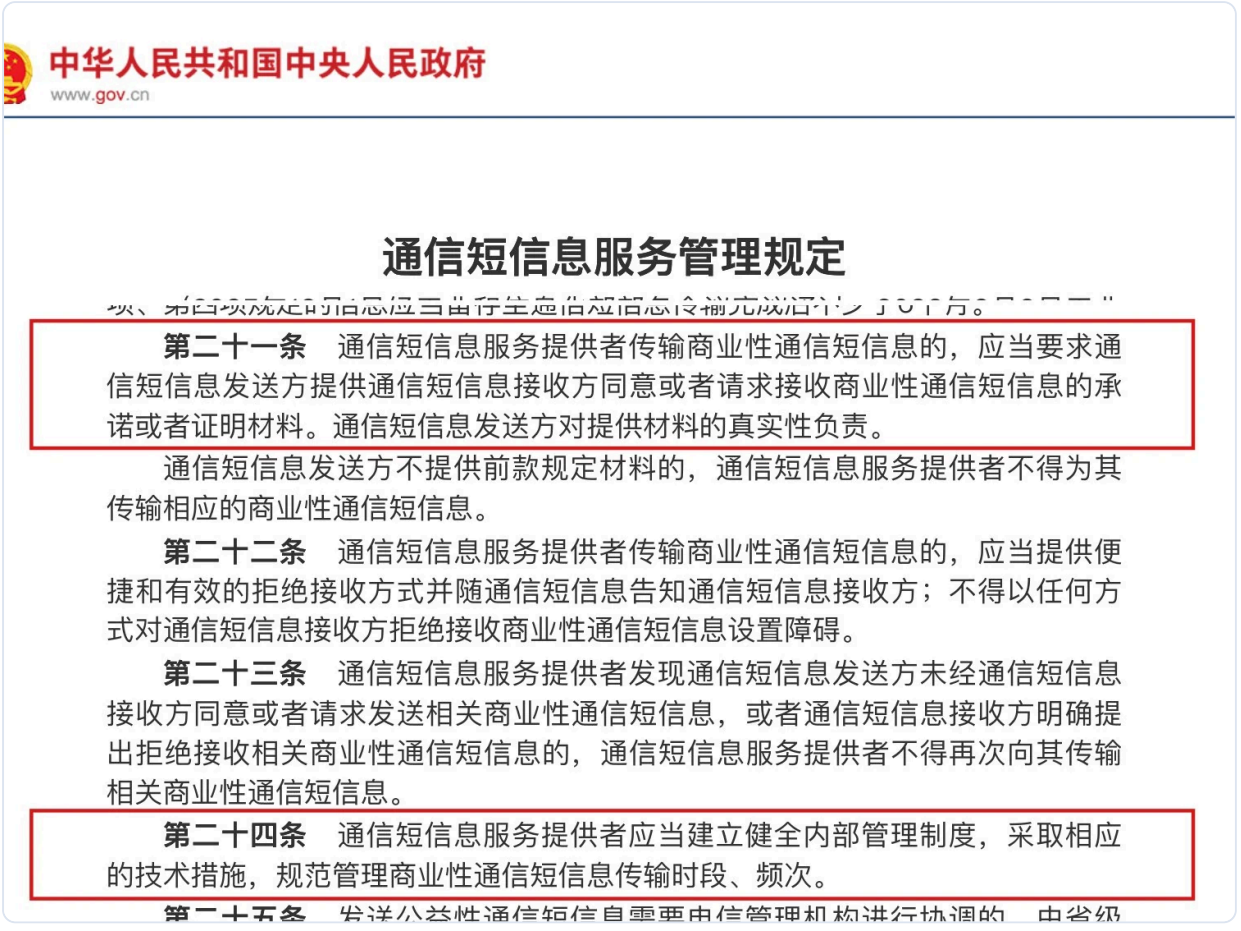
1.1 Dual Regulatory and Carrier Squeeze Collapses Bulk SMS Economics

Bulk SMS was once the widest-reach, lowest-cost outreach channel for collection scams. Between the second half of 2025 and the first half of 2026, however, carrier filtering and formal regulation closed the channel—culminating in the **Provisions on the Administration of Short Message Services (MIIT Order No. 74)**, which took effect on **May 1, 2026**.

Date	Authority / Operator	Control Measure
2025-05-20	Major domestic carrier A	Messages containing URLs, IP addresses, or contact details face high probability of interception
2025-07	Major domestic carrier B	Messages containing contact details require prior filing and review
During 2025	Major domestic carrier C	Progressive rollout of lead-generation SMS filtering blocking URLs and contact details
2026-05-01	**Ministry of Industry and Information Technology (MIIT)**	**Order No. 74 takes effect**: real-name sender verification, ban on mixing service and commercial SMS short codes, mandatory recipient opt-in proof, and regulated sending windows and frequency

The sharpest blow came from **Article 21** of Order No. 74: service providers transmitting commercial short messages must require senders to supply verifiable proof of recipient consent or request, with senders legally responsible for authenticity; without such proof, transmission is prohibited. Because targets of fake collection messages never opted in, fraudsters could no longer access legitimate commercial SMS gateways.

At the same time, **Article 18** barred mixing commercial messages with operational or service-notification short codes, **Article 19** mandated traceable real-name sender identification—closing gray workarounds such as piggybacking on service channels or spoofing sender signatures—and **Article 24** required operators to regulate transmission windows and frequency.


中华人民共和国中央人民政府
www.gov.cn

通信短信息服务管理规定

第二十一条 通信短信息服务提供者传输商业性通信短信息的，应当要求通信短信息发送方提供通信短信息接收方同意或者请求接收商业性通信短信息的承诺或者证明材料。通信短信息发送方对提供材料的真实性负责。

通信短信息发送方不提供前款规定材料的，通信短信息服务提供者不得为其传输相应的商业性通信短信息。

第二十二条 通信短信息服务提供者传输商业性通信短信息的，应当提供便捷和有效的拒绝接收方式并随通信短信息告知通信短信息接收方；不得以任何方式对通信短信息接收方拒绝接收商业性通信短信息设置障碍。

第二十三条 通信短信息服务提供者发现通信短信息发送方未经通信短信息接收方同意或者请求发送相关商业性通信短信息，或者通信短信息接收方明确提出拒绝接收相关商业性通信短信息的，通信短信息服务提供者不得再次向其传输相关商业性通信短信息。

第二十四条 通信短信息服务提供者应当建立健全内部管理制度，采取相应的技术措施，规范管理商业性通信短信息传输时段、频次。

Figure 2. Excerpt of MIIT Order No. 74 highlighting Articles 21 and 24 on mandatory consent proof and transmission controls (Chinese original). · Source: State Council Gazette, gov.cn

Two market dynamics compounded regulatory pressure: **declining credibility**, as consumers had grown broadly skeptical of overdue alerts from unknown numbers; and **rising delivery costs**, as gateway restrictions drove up per-message prices and forced constant number rotation. Together, regulation, skepticism, and cost collapsed the return on bulk SMS.

1.2 Script Upgrade: From Phone Pressure to Forged Demand-Letter Workflows

Threat Hunter continuously monitors two underground recruitment categories: "collection scripts / fake collection" and "legal demand letters." Monthly volume from January to November 2026 captures the direct handoff between legacy and upgraded tactics:

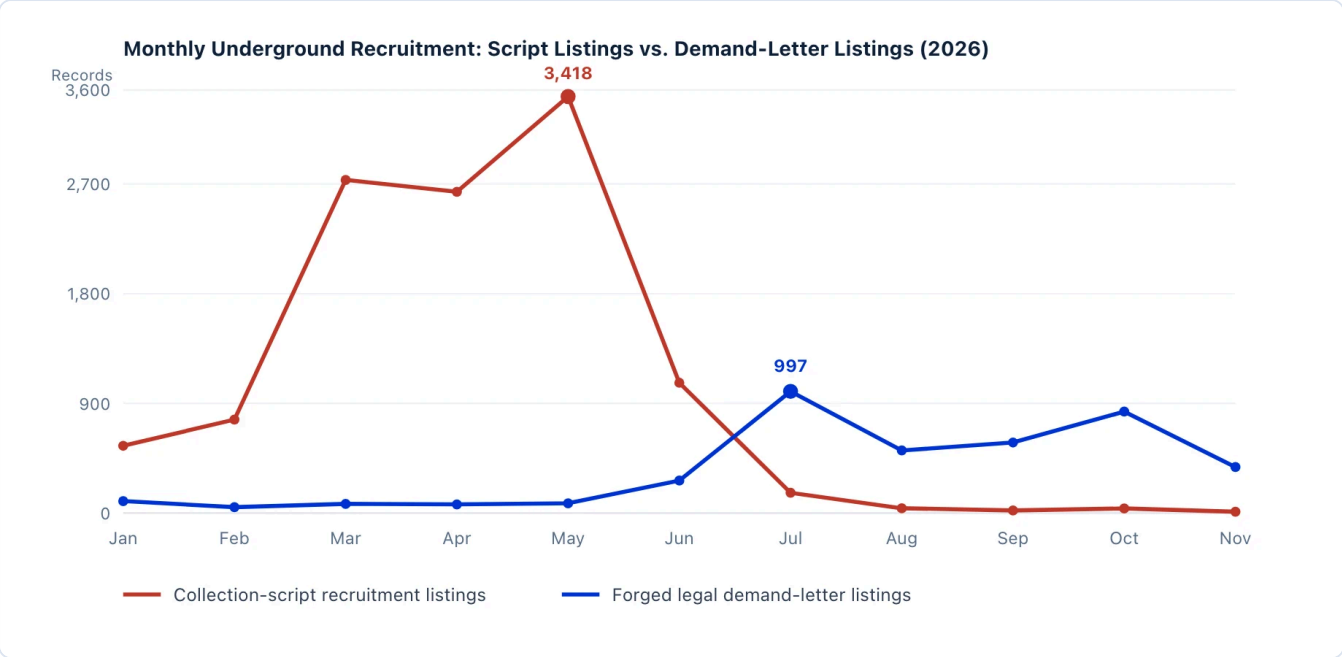


Figure 3. Monthly underground recruitment volume: collection-script listings vs. forged legal demand-letter listings, January–November 2026. · Source: Threat Hunter Research Team

Between March and May 2026, collection-script recruitment listings reached their annual peak at 2,734, 2,636, and 3,418 records per month. Just one month after Order No. 74 took effect on May 1, volume dropped sharply to 1,068 in June, fell to 166 in July, and lingered in the low dozens from August onward. Conversely, forged demand-letter recruitment started the year below 100 per month, surged to a peak of 997 in July, and remained elevated in the hundreds throughout the autumn.

> **Core Insight:** SMS collection tested whether a recipient trusted an unfamiliar number; a stamped legal demand letter with a case number shifts the burden to authenticating a formal legal document—turning social engineering from live phone persuasion into a zero-call guided workflow.

Most consumers can dismiss an overdue text from an unknown number using everyday common sense. When confronted with a clean letterhead, a law-firm seal, a case reference number, and named counsel, however, ordinary recipients rarely know how to verify authenticity and are far more likely to comply under stress.

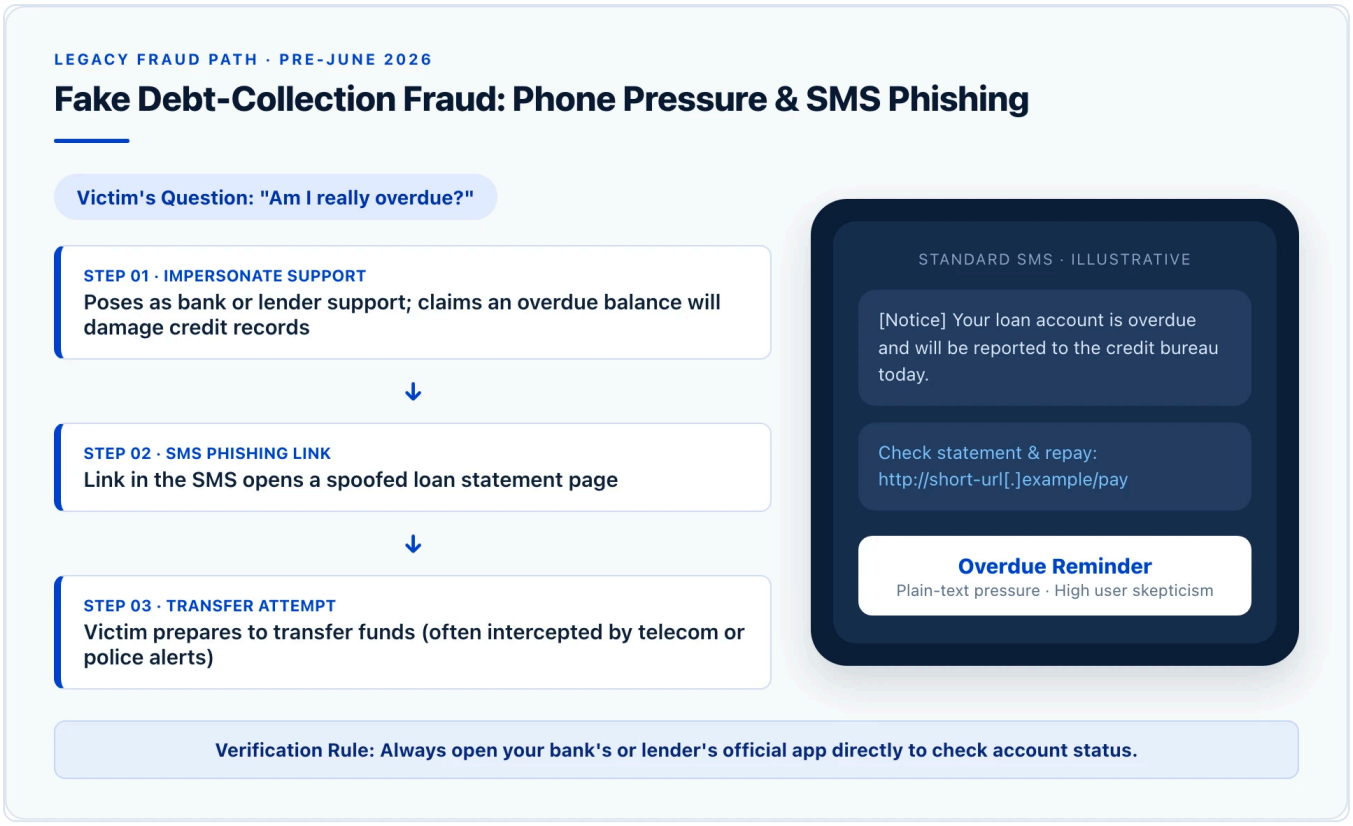


Figure 4. Legacy SMS collection fraud path: impersonated support pressure leading to a spoofed billing link. · Source: Threat Hunter Research Team

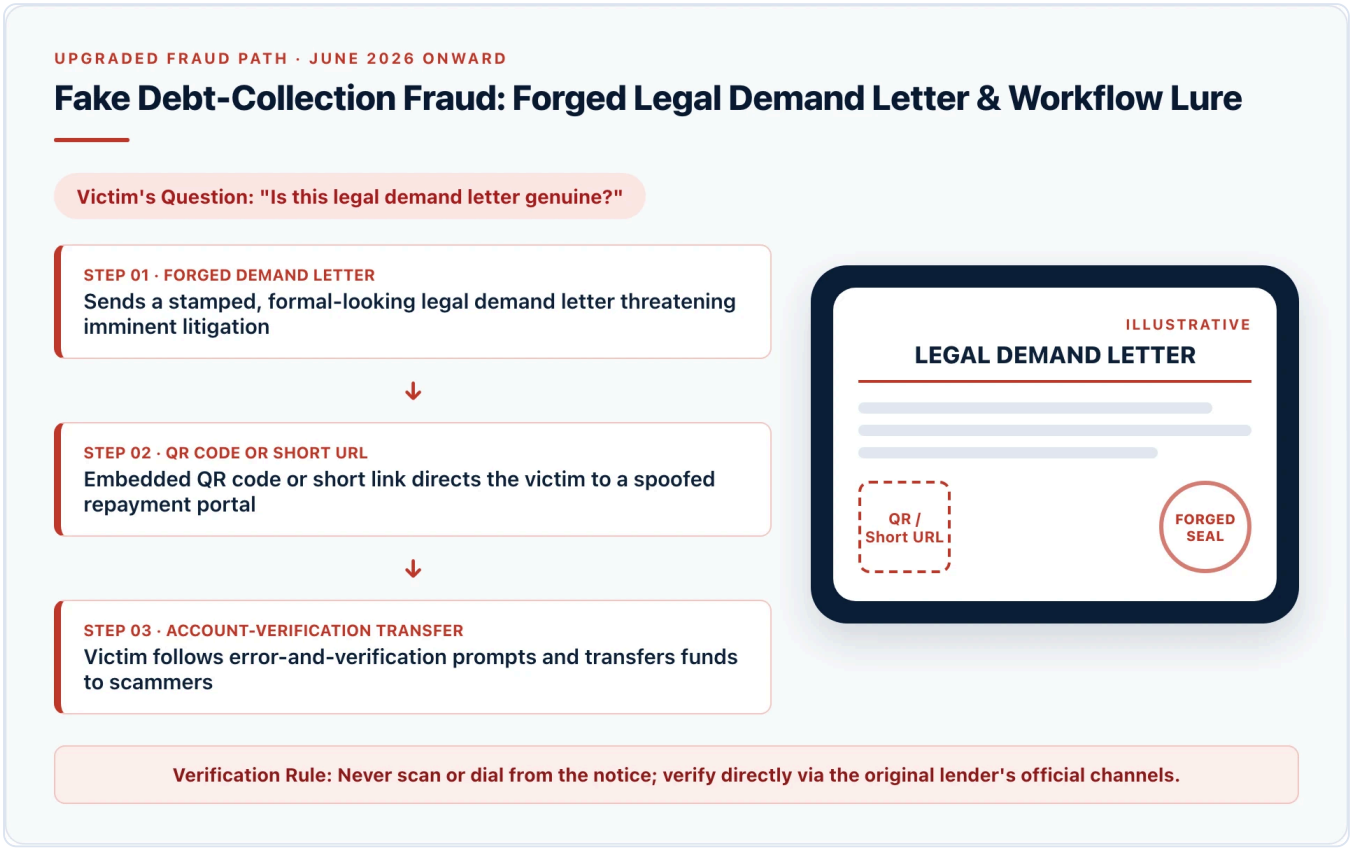


Figure 5. Upgraded forged demand-letter fraud path: formal document delivery leading to off-channel "account-verification" transfers. · Source: Threat Hunter Research Team

A representative case disclosed by Beijing police in late March 2026 (showing early incidents before June's mass scale-up) illustrates the mechanics: a victim received a forged legal demand-letter image bearing a law-

firm seal via iOS native IP messaging, claiming an overdue balance of CNY 40,000. Once the victim scanned the code into a spoofed repayment portal and entered bank card details, attackers extracted funds in three steps:

- **Step 1 (Manufactured error):** The page displayed "Transfer missing name memo—please retry," convincing the victim that the first repayment had failed.
- **Step 2 (Induced account verification):** The page demanded a larger "bank account-verification transfer" to prove the account was active.
- **Step 3 (False refund promise):** After the transfer cleared, the portal claimed the funds would be refunded automatically, while the money was siphoned away immediately.

The entire sequence ran with **zero phone calls and no live confrontation**. Operators no longer needed to persuade victims live over the phone—they simply guided them through an orderly online flow, following up hours later with pressure messages threatening an in-person home visit if the recipient did not respond.



Figure 6. Beijing police alert reporting 12 fake demand-letter cases via iOS native IP messaging totaling over CNY 260,000 within one month (Chinese original). · Source: Public police and media reports



Figure 7. Forged legal demand-letter image and follow-up pressure message received by a victim (Chinese, redacted). · Source: Threat Hunter Research Team

1.3 Forensic Breakdown: Template Reuse, Last-Digit Credit-Code Tampering, and Mobile Web Funneling

Structural comparison of multiple forged letters by Threat Hunter's Digital Risk Protection (DRP) intelligence team uncovered two industrialized traits:

Mass template reuse with duplicated reference numbers. Demand letters sent to different victims months apart repeatedly carried the exact same document reference number—violating standard sequential law-firm numbering. Operators clearly maintain ready-made templates impersonating firms in major cities such as Beijing and Shanghai, batch-swapping only recipient names and alleged debt amounts.

Subtle tampering with the final character of the Unified Social Credit Code. In verified samples, the law firm's name, reference number, and named attorney mapped to real entities, but the final character of the Unified Social Credit Code was altered—**replacing a real digit with a visually similar letter (such as changing `5` to `S`)**. Barely noticeable to the naked eye, this single-character substitution causes official registry lookups copied from the letter to fail.

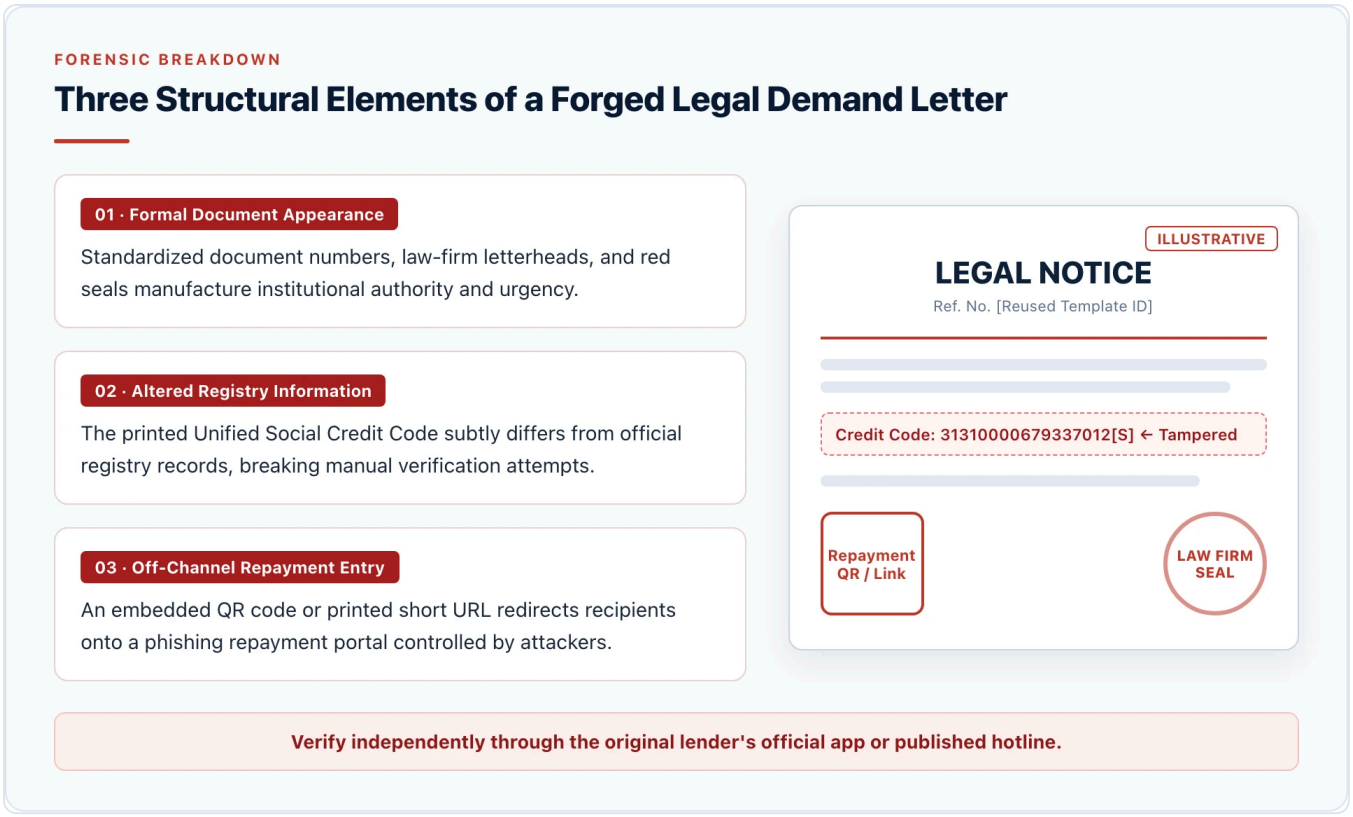


Figure 8. Three core elements of a forged legal demand letter: formal appearance, tampered registration details, and off-channel repayment link. · Source: Threat Hunter Research Team

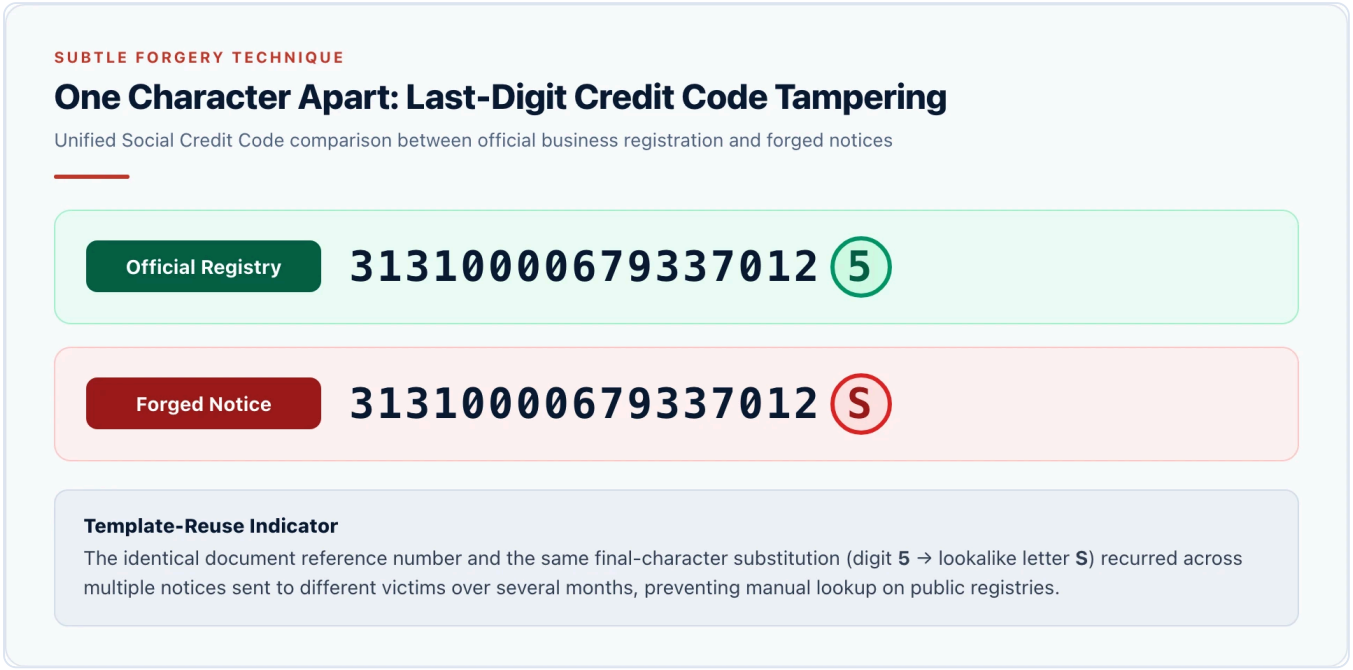


Figure 9. Unified Social Credit Code comparison: official digit 5 tampered to lookalike letter S to break manual registry lookup. · Source: Threat Hunter Research Team

Meanwhile, the spoofed landing pages upgraded in lockstep. Early cases used crude redirect pages, whereas sites observed later in the monitoring period evolved into polished mobile web apps (HTML5) impersonating consumer-installment login screens ("Enter your mobile number to check your bill"). This delivers a dual payoff: realistic UX lowers suspicion, and **phone-number entry acts as a live lead-cleansing funnel**, filtering leaked lists into active, high-conversion targets.



Figure 10. Upgraded spoofed landing page: a polished consumer-installment mobile web login screen used to verify active phone numbers (Chinese, brand redacted). · Source: Threat Hunter Research Team

Part 2. Two-Hop Channel Escape: From iOS IP Messaging to QR-Free Door-to-Door Mailers

Once SMS gateways closed, outreach migrated in two hops: first bypassing carrier SMS gateways via OS-native IP messaging on iOS devices, and next bypassing the entire telecom network via physical express couriers. Following late-October police raids and courier QR-code screening, physical mailers mutated yet again.

2.1 Hop One (Online Bypass): Rich Media on iOS IP Messaging Makes "Blue-Bubble Screening" Standard

Under strict SMS link filtering, OS-native IP messaging on iOS devices became the primary online substitute. Beyond bypassing carrier SMS gateways entirely, **it supports direct delivery of high-resolution images**—allowing collection scripts to be packaged as stamped legal demand letters with far greater visual credibility. That mutual reinforcement explains why channel migration and script upgrades happened simultaneously in June.

CHANNEL SHIFT · ONLINE BYPASS

Standard SMS vs. iOS Native IP Messaging in Fake Collection Scams

Dimension	Standard SMS	iOS Native IP Messaging
Transport Channel	Carrier SMS gateways (subject to strict filtering)	Wi-Fi or cellular data (bypasses carrier SMS gateways)
Media Format	Plain text only	Rich text, high-resolution images, and PDF attachments
Fraud Presentation	Short text warning about alleged overdue debt	Stamped, letterhead legal-notice images mimicking formal documents
Cost & Reach	Per-message gateway fees; shrinking delivery rate under Order 74	Data-based transport; reaches pre-screened active iOS devices ("blue-bubble" verified)

Figure 11. Core differences between standard SMS and iOS native IP messaging in transport, format, visual credibility, and reach. · Source: Threat Hunter Research Team

Monitoring curves capture the surge directly: **in June 2026, underground activity tied to iOS native IP messaging jumped to 32,112 records in a single month**, stayed above 24,000 per month from July through October, and eased to roughly 17,800 in November. In parallel, demand for offline print-and-mail courier services gathered momentum in autumn and spiked to **2,010 records in October**—roughly four times its pre-surge monthly average.

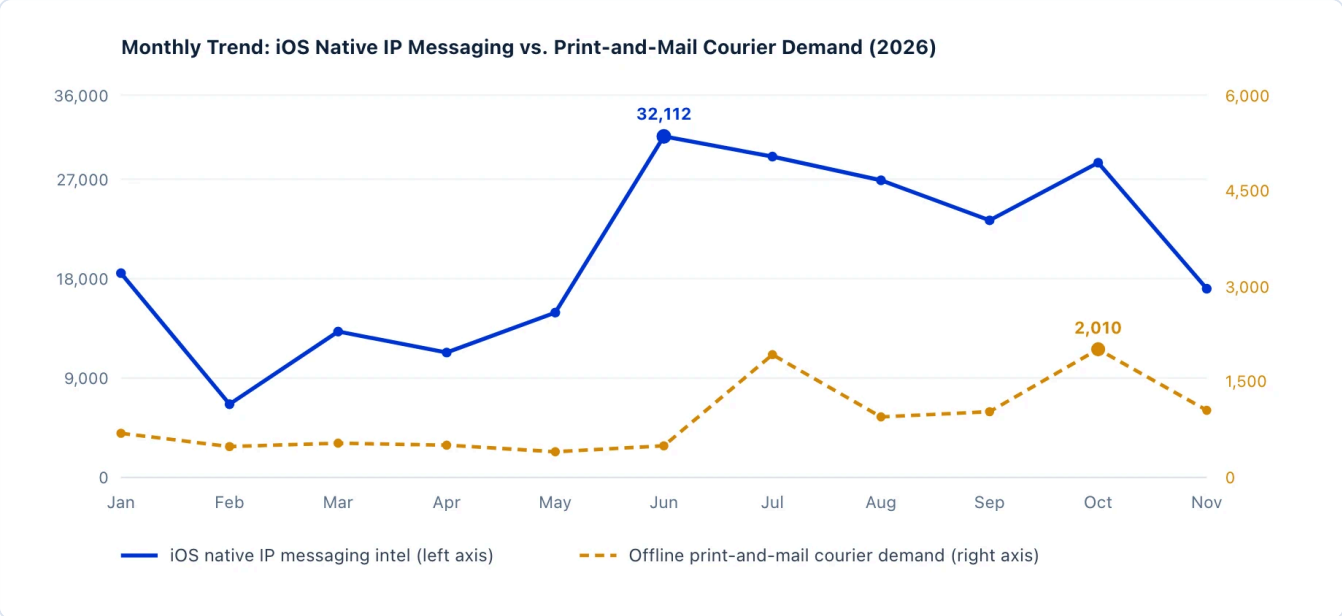


Figure 12. Monthly volume of iOS native IP messaging activity (left axis) vs. offline print-and-mail courier demand (right axis), January–November 2026. · Source: Threat Hunter Research Team

Downstream channel shifts immediately reshaped midstream data markets. Because OS-native iOS IP messaging reaches only active iOS devices, device-type filtering—previously an optional add-on—became a standard cross-scenario specification in 2026 across fake collection, refund, and vehicle-recall campaigns. In an October listing for secondhand collection leads, the seller explicitly marketed **"iOS blue-bubble screening**

with zero error," displaying 42,393 verified iOS records broken down by month from May to December 2025. Adding a screening step increases acquisition cost per lead; buyers' willingness to pay that premium confirms the high conversion economics of forged demand letters sent via iOS IP messaging.

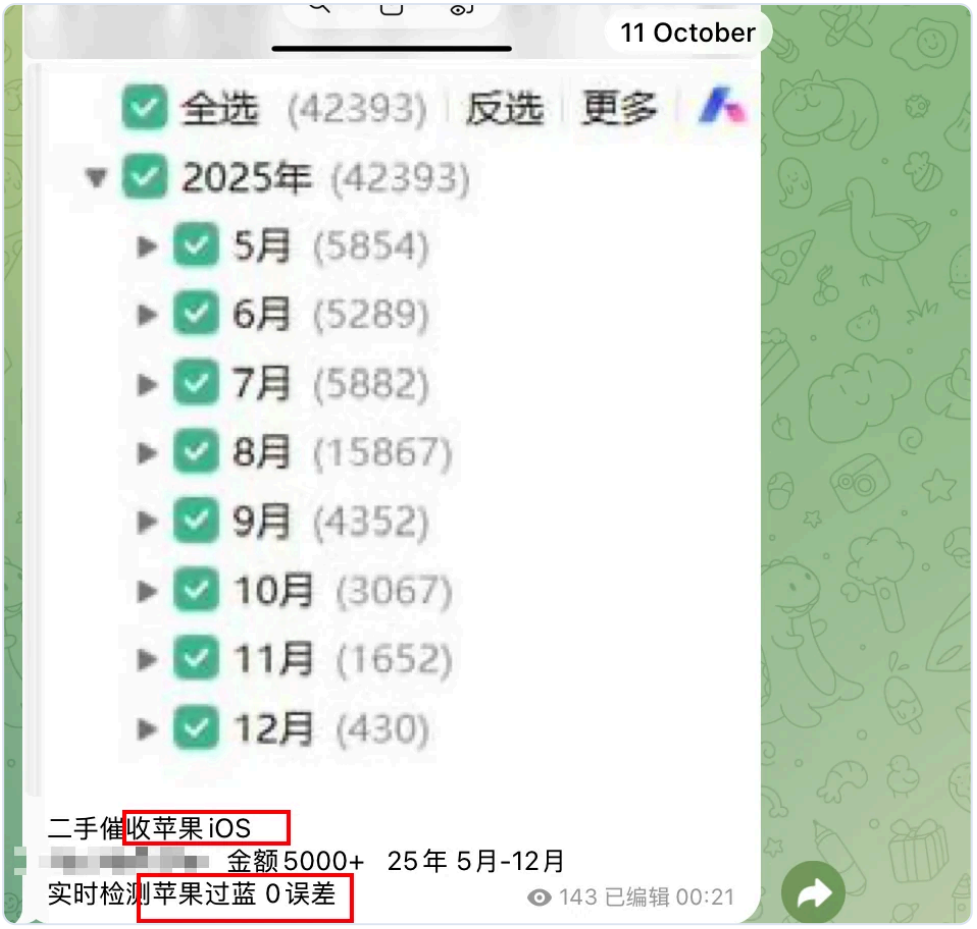


Figure 13. Midstream data-market adaptation: underground sellers market "zero-error iOS blue-bubble screening" as a standard delivery specification (Chinese, redacted). · Source: Threat Hunter Research Team

2.2 Hop Two (Physical Off-Network Shift): Print-and-Mail Couriers Borrow Logistics Credibility

Any online channel still operates inside internet and telecom monitoring boundaries. To escape telecom interception altogether, physical delivery became the final hop. By October 2026, underground recruitment for offline print-and-mail services surged to 2,010 records.

Monitored advertisements are blunt: operators now offer turnkey **"typesetting + data supply + printing and stuffing + express dispatch"** services that abuse legitimate direct-operated express couriers, national postal express services, and major parcel networks along with brand-specific document envelopes—explicitly listing "legal demand letters" as a supported category and advertising daily guarantees of 5,000 to 10,000+ mailings.



Figure 14. Underground print-and-mail recruitment explicitly accepting "legal demand letters" across major express networks (Chinese original). · Source: Threat Hunter Research Team



Figure 15. Stockpiled multi-brand courier document envelopes used to lend legitimacy to forged paper notices (Chinese original). · Source: Threat Hunter Research Team

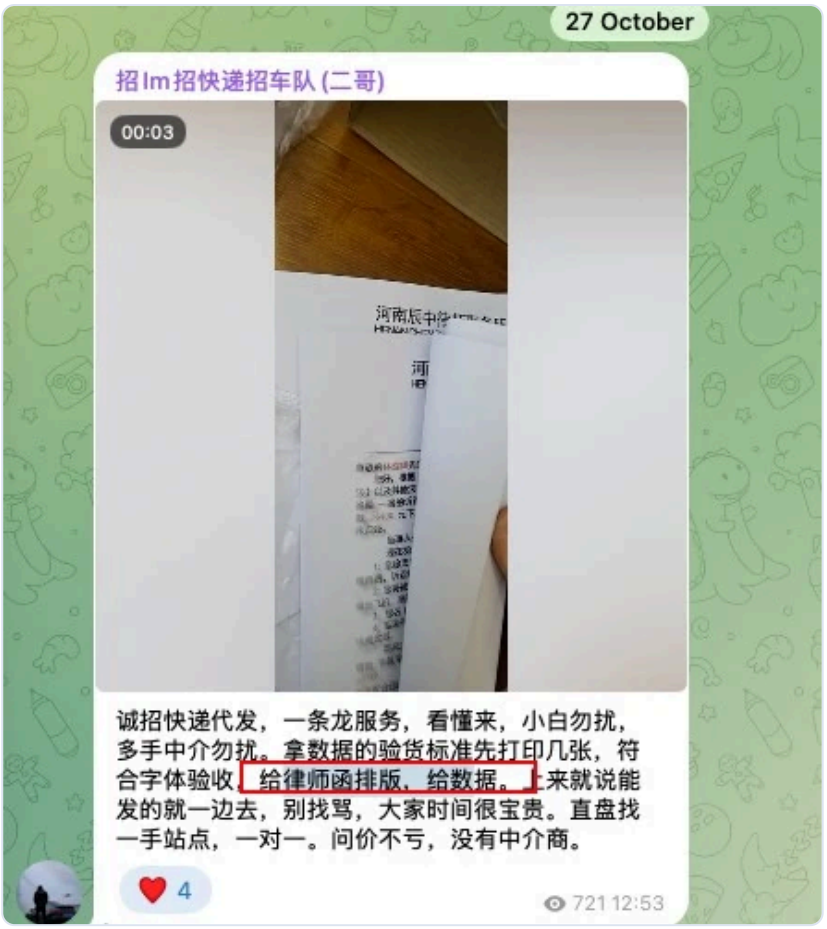


Figure 16. Turnkey underground offer bundling demand-letter typesetting, victim data, and sample-print verification (Chinese original). · Source: Threat Hunter Research Team

The core hazard lies not in mailing paper itself, but in **institutional trust transfer**: authentic shipping labels, real-time tracking records, and formal delivery signatures lend strong credibility to the forged letter inside, sharply lowering recipient defenses. Because the entire delivery path sits outside telecom networks, SMS filters, caller-ID warnings, and network URL blockers have zero visibility.

2.3 Late-October Counter-Adaptation: Dropping QR Codes for Short URLs and Paid Door Delivery

Starting in late October 2026, domestic law enforcement cracked down on illicit printing-and-mailing hubs—including an October 22 Shanghai police raid on a ring that printed and shipped over 3,000 QR-coded fake demand letters—while express depots tightened inspections on "single A4 sheet + QR code" envelopes. Within weeks, offline delivery mutated sharply: **paper notices removed QR codes altogether in favor of a "QR-free, link-only" format.**

> **Critical Inflection:** Removing QR codes from paper notices is not a step backward—it is a targeted double bypass that simultaneously evades courier QR inspections and the built-in anti-fraud warning screens triggered when scanning codes in major chat and payment apps.

In the "QR-free, link-only" model, forged paper demand letters contain no QR code at all; instead, a short URL is printed directly in the body text, prompting recipients to open their phone's native browser and type the address manually. This single design change breaches two established defensive layers at once:

- **Layer 1 (Logistics intake and sorting):** Without a printed QR code, visual checks, automated sorting flags, and depot penalties calibrated for "QR-coded scam letters" fail to fire.
- **Layer 2 (Messaging and payment app scanning):** Manual entry in a phone's native browser sidesteps the high-risk URL blocks and anti-fraud warning pages embedded in the QR scanners of major chat and payment apps.

Monitoring data reveals how quickly this variant spread: courier collection listings explicitly requiring **"no QR code / link-only"** were near zero from January through September, **first appeared on October 21 (23 listings in October), and jumped to 114 listings in the first 22 days of November—nearly a fivefold month-over-month surge**.

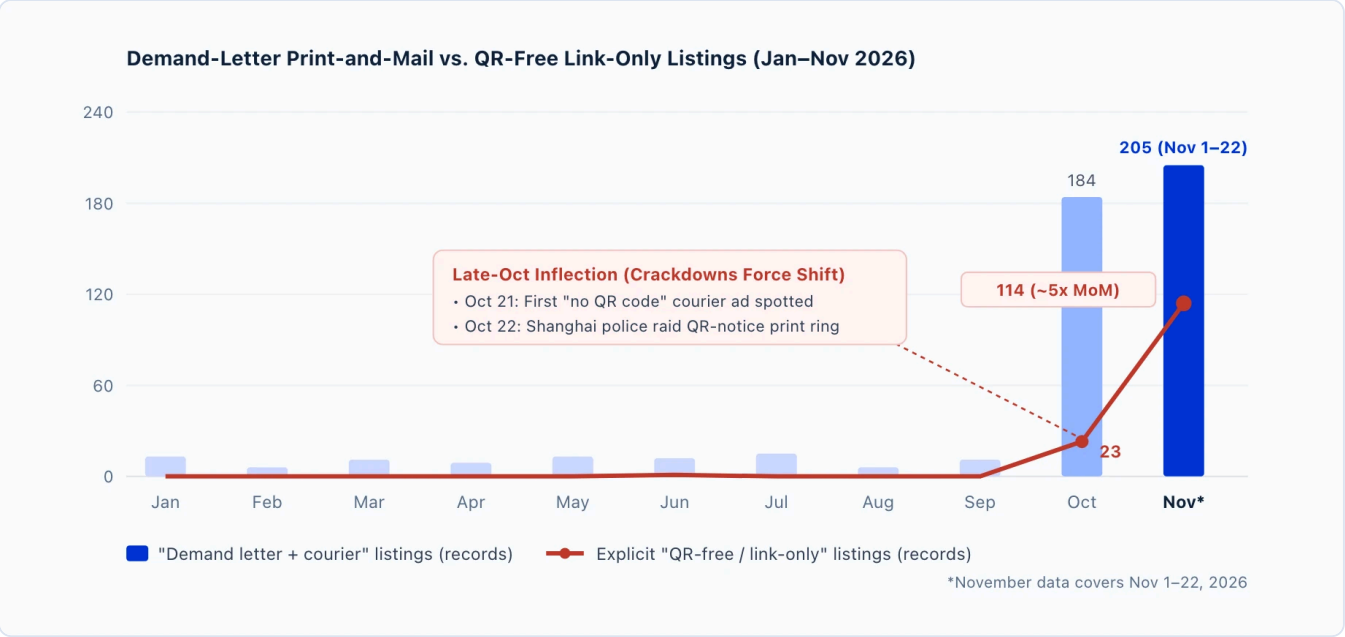


Figure 17. Monthly volume of demand-letter courier print-and-mail listings vs. explicit "QR-free / link-only" requirements (November covers Nov 1–22, nearly 5x month-over-month growth). · Source: Threat Hunter Research Team

Alongside removing QR codes, downstream operators became highly selective about shipping tiers and dispatch outlets. To prevent cheap standard parcels from sitting unopened in parcel lockers or pickup stations, recruiters willingly paid higher unit costs to **mandate premium direct-operated express services, national postal express, and paid call-ahead door-to-door delivery tiers**, paired with matching branded document envelopes so a courier's personal phone call and hand-delivery amplify psychological pressure. Settlement rules even specify "paid upon signature or refusal, unpaid only if intercepted by courier inspection," driving active recruitment of lax dispatch stations.

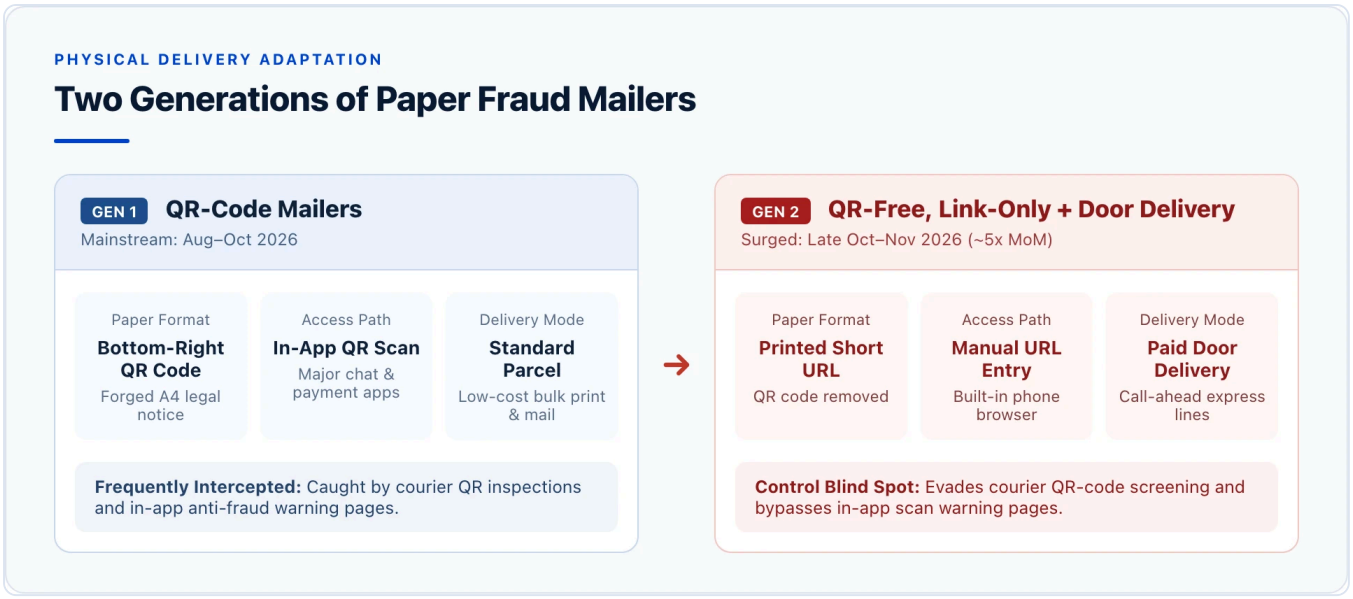


Figure 18. Comparison of two paper fraud-mailer generations: legacy QR-code parcels vs. QR-free, link-only door-to-door mailers. · Source: Threat Hunter Research Team

Part 3. Behind the Scenes: Nine Specialized Roles and Shared Multi-Scam Infrastructure

Focusing solely on a forged notice or a single spoofed website dramatically underestimates the adversary's scale. By tracing front-end and back-end artifacts, Threat Hunter found that fake debt collection is no longer run by ad hoc crews—it operates atop a specialized, modular cybercrime infrastructure shared across multiple scam campaigns.

3.1 Full Supply Chain: Nine Specialized Roles and the Attribution Gradient

Deconstructed by production and trade function, the ecosystem spans **nine specialized roles**: upstream supply covers (1) data suppliers, (2) script and creative kits, and (3) document templates; midstream production covers (4) site builders and (5) domain pools; downstream delivery covers (6) online dispatch (iOS messaging farms and dialers) and (7) physical print-and-mail dispatch; and cross-cutting support comprises **(8) escrow and guarantee layers** (holding deposits, issuing vouchers, mediating disputes) and **(9) brokers and assemblers** (bundling capabilities for cross-scenario reuse). The presence of escrow and brokerage roles confirms full industrialization.

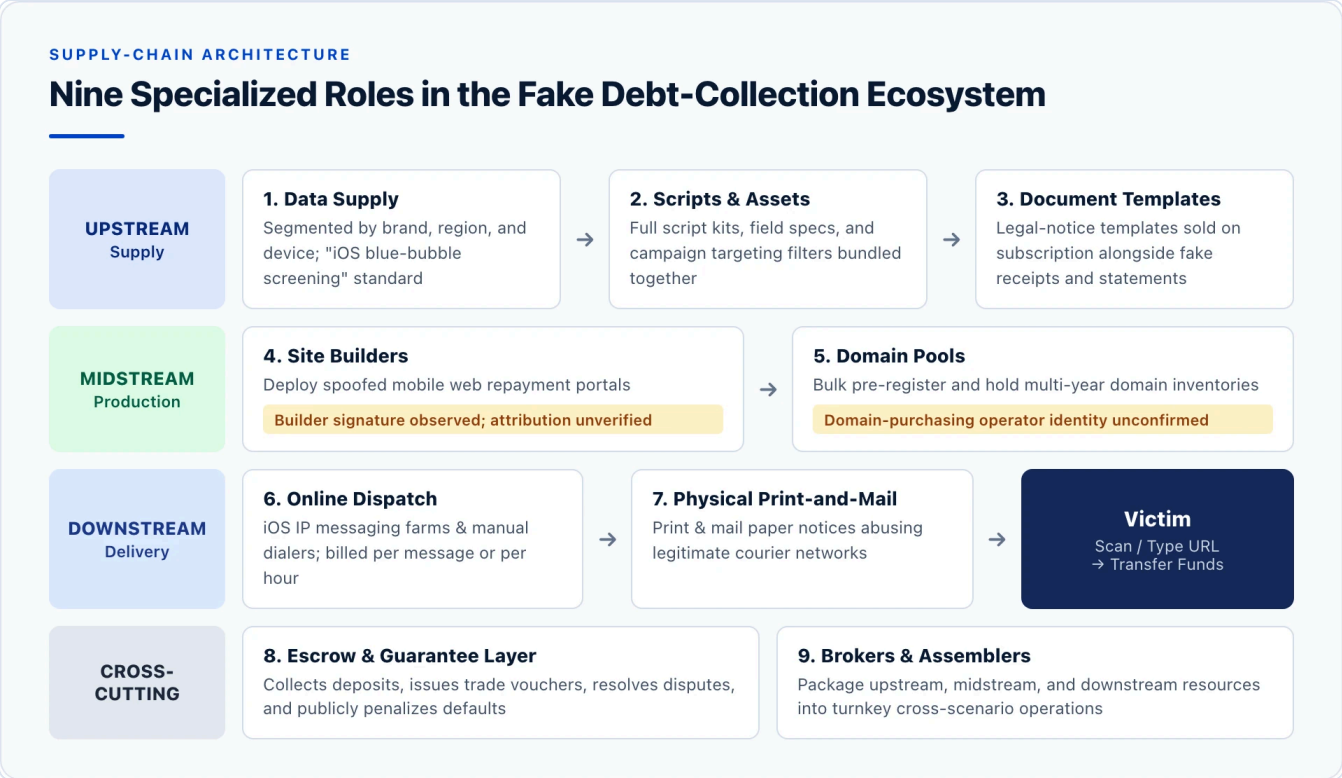


Figure 19. Overview of the nine specialized roles across the fake debt-collection cybercrime supply chain. · Source: Threat Hunter Research Team

Attribution tracing across these layers exposes a practical rule for defenders: **technical-supply layers leave the clearest objective artifacts, whereas operators closest to fund collection stay the cleanest.** Layers (4) site builders and (5) domain pools are the highest-leverage pivot points: involved servers revealed a reusable interactive mobile web-page builder and developer attribution strings shared across numerous fraud portals (redacted in this public edition because front-end title attributions can be spoofed and require law-enforcement verification), while domain registration logs preserve exact bulk-staging timestamps and activation rhythms.

Infrastructure Layer	Current Attribution Status	Key Evidence & Operational Assessment
Site-Builder System	Reusable template identified	Across 200+ sites hosted on involved servers, multiple portals shared default titles and sales showcase pages from the same interactive mobile web-page builder, confirming industrialized tool supply (actual authorship and intent require verification)
Origin Servers & Filings	Origin hosts located	Two core origin servers remained active throughout monitoring; associated ICP website filings belonged to two deregistered shell companies, offering no real operator lead
Domain Resource Pool	Staging rhythm mapped	Bulk registration timestamps, multi-year validity choices, and dormant-to-active cycles are highly distinct—making this the most actionable layer for proactive disruption and early warning
Front-End Operators	Highly concealed	Early landing pages used minimal redirects with no business logic, separating payment collection from front-end hosts so page artifacts alone rarely expose fund controllers

3.2 Upstream Supply Reality: June's Dip Was Channel Migration, Not Exhaustion

At first glance, monthly consumer-finance data-leak incidents from January to October 2026 present a tempting illusion: excluding February's seasonal holiday dip (75 incidents), **June logged a non-holiday low of 80 incidents**. Did upstream data supply dry up?

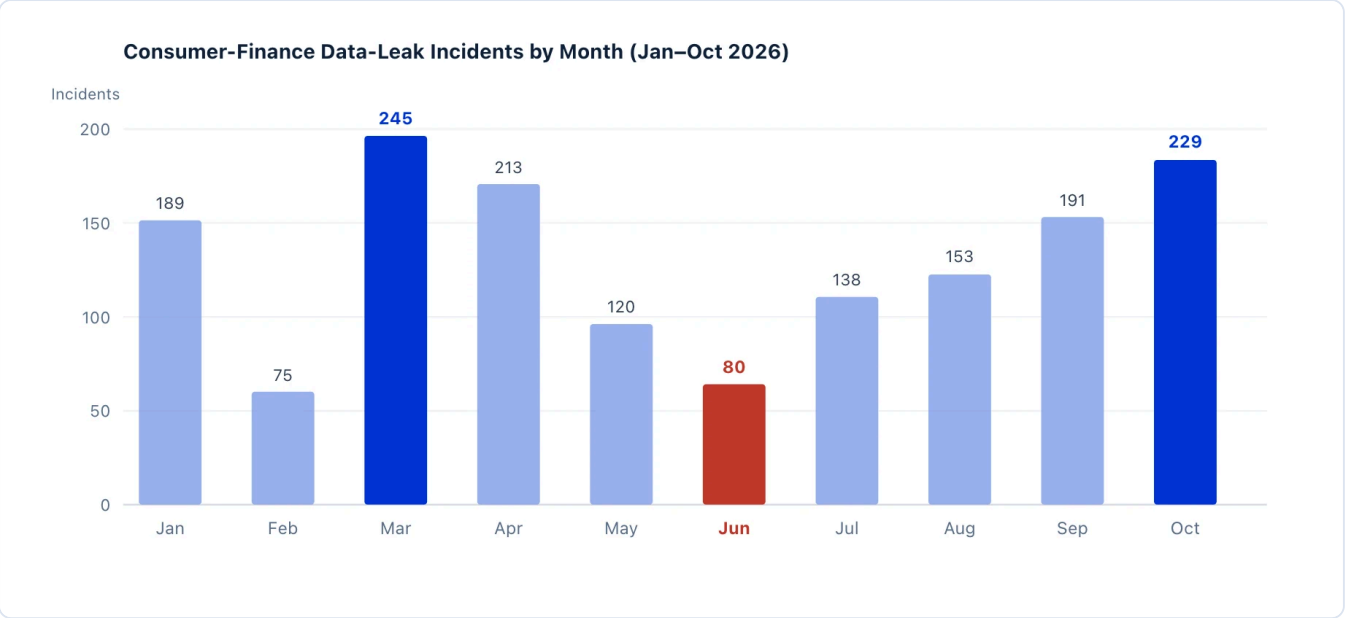


Figure 20. Monthly consumer-finance data-leak incidents (January–October 2026), showing a twin-peak pattern rebounding to 229 in October. · Source: Threat Hunter Research Team

The reality is the exact opposite. Timeline correlation and field intelligence confirm that **June's drop coincided directly with mass bans of cybercrime channels and groups on a major encrypted messaging app in May–June 2026**. Tracking the top ten data-trading groups from May showed every single one contracted sharply in June—six dropped by more than 70%, including three that fell to zero—yet within the very same month, newly formed groups rapidly scaled from single digits to over a hundred incidents, absorbing the displaced traffic.

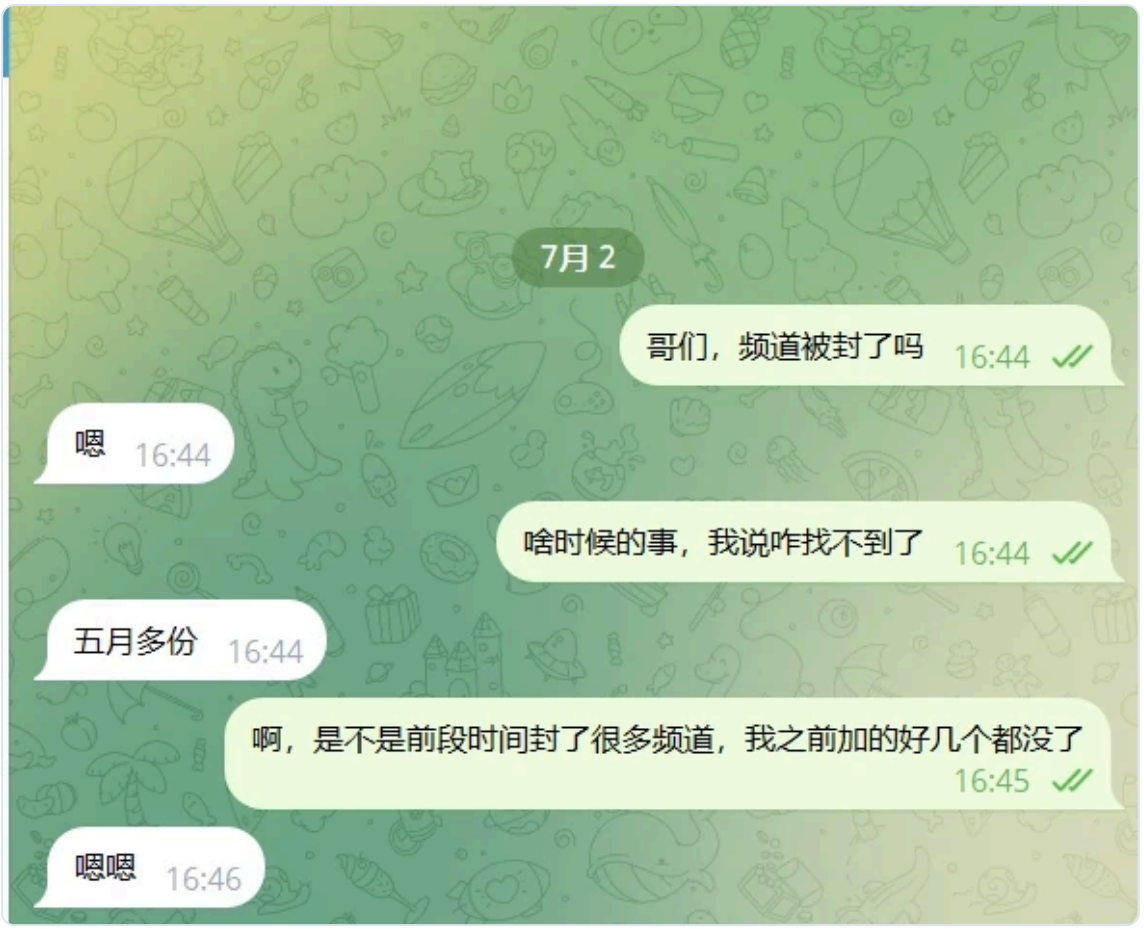


Figure 21. Underground chat confirming that prior data-trading channels were removed during May–June platform bans (Chinese original). · Source: Threat Hunter Research Team

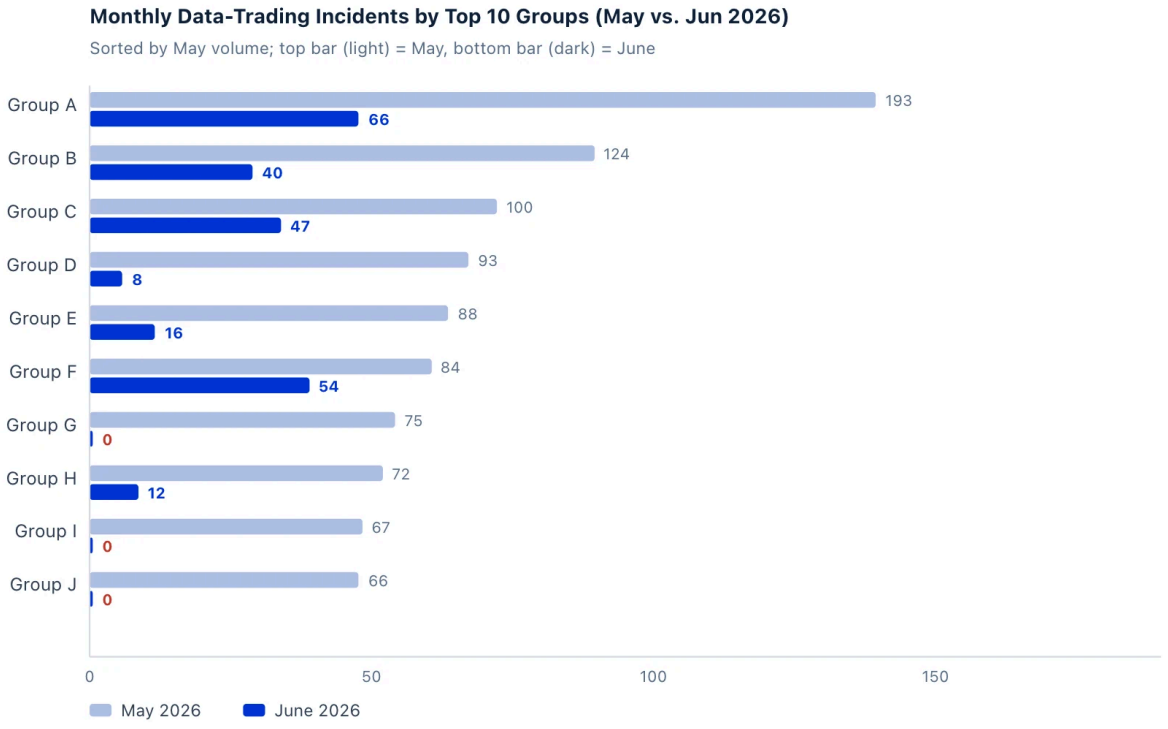


Figure 22. Top ten data-trading groups from May 2026 all contracted sharply in June following mass channel bans. · Source: Threat Hunter Research Team

Simultaneous collapse of legacy channels and rapid rise of replacements point to three conclusions: first, the June dip was a brief rebuilding vacuum rather than declining supply; second, continuous enforcement pushed markets into a "launch–ban–relaunch" cycle while shifting deals from public price boards toward **private one-on-one negotiations**; third, **monthly leak incidents recovered steadily from July onward, reaching 229 in October**—nearly matching March's 245 peak and confirming that upstream supply remains robust and expanding.

3.3 Shared Resource Layer: Five Fraud Campaigns Running on One Origin Server

Because the site-builder stack is a reusable commercial-grade tool, its underlying hosts support far more than fake debt collection. Tracing back from involved domains to origin servers revealed a single host resolving **287 domains** (multiple domains can map to one site), with **12 populated sites spanning five completely distinct suspected fraud categories**: advance-fee "national asset release" and fake poverty-relief schemes, multi-level "Global IoT" pyramid recruitment, bogus "new infrastructure" subsidies, healthcare-sector investment scams, and the fake debt-collection portal in this case.



Figure 23. Shared cybercrime hosting: one origin server resolving 287 domains and 12 configured sites across five suspected fraud categories. · Source: Threat Hunter Research Team

One counterintuitive detail stands out: in early-November snapshots of that server, the fake debt-collection page was actually the crudest site on the box (a bare iframe redirect that was not upgraded into a full mobile web login page until November 20). That indicates **fake debt collection was not the host operator's sole core business, but rather a bolt-on campaign mounted onto mature multi-scam infrastructure**—reinforcing why disrupting a single front-end operation rarely dents the shared base.

3.4 Domain Pools & Takedown Agility: Late-July Stockpiling and 6-Day Evolution

Domain-pool rhythms offer the clearest window into long-term organizational planning. Registration logs reveal a deliberate **"bulk pre-registration + extended dormancy + on-demand activation"** playbook:

Campaign Scenario	Registration Window	First Observed Activation	Dormant Staging Period
Consumer-finance fake collection	2026-07-29, 06:14–07:04	2026-11-08	Approx. 102 days
Auto-recall scam	2026-07-29 (same batch)	Around 2026-10-25	Approx. 88 days
Spoofed installment platform	Ad hoc during campaign	4–11 days post-registration	4–11 days (tactical top-up)

Even more telling are the exact timestamps and registration terms: **within a 50-minute window from 06:14 to 07:04 on July 29, 2026, operators registered 42 domains across two registrars, interleaving consumer-finance collection domains and auto-recall domains second by second**—proving both campaigns share the same procurement team or channel. Crucially, **every pre-staged domain was purchased for a two-year validity term, whereas tactical domains registered during live incidents carried one-year terms**. Fly-by-night crews do not pay extra for two-year domain registrations; this points directly to sustained, corporate-style operations.

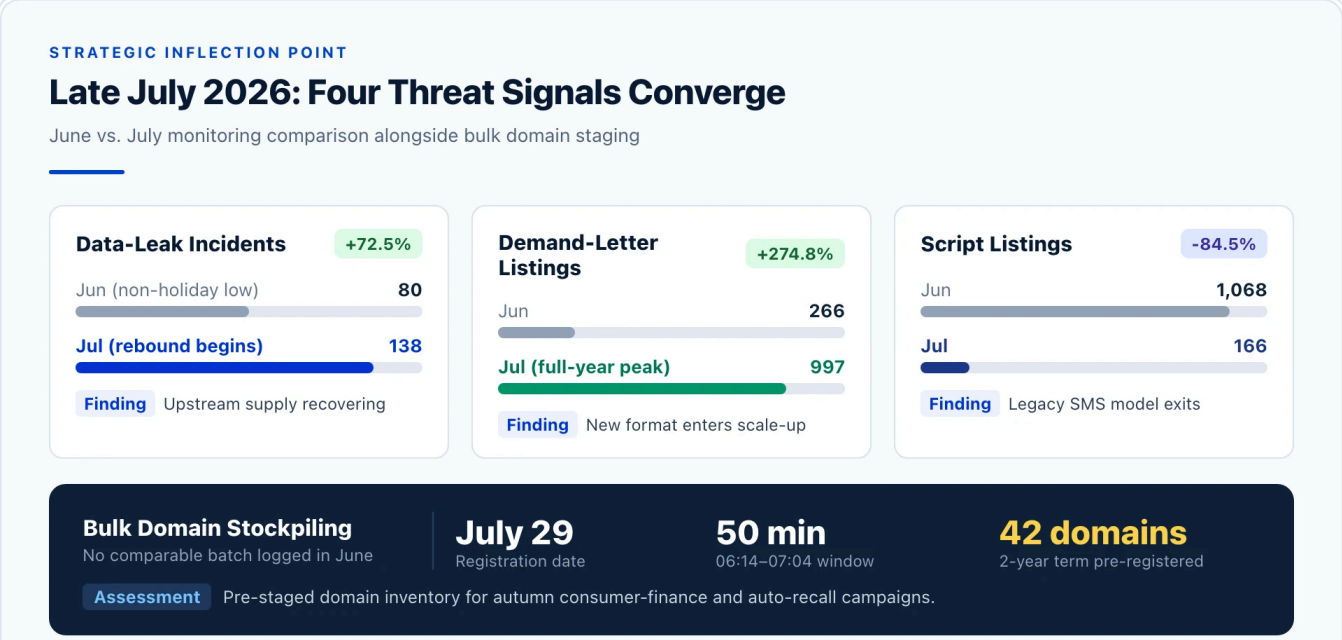


Figure 24. Late-July 2026 strategic convergence: upstream supply rebound, demand-letter scale-up, SMS exit, and bulk domain stockpiling. · Source: Threat Hunter Research Team

> **Strategic Assessment:** Late July was not a quiet period—it was the handoff where legacy tactics exited and next-generation infrastructure was stockpiled in bulk. In hindsight, June's low was merely a brief pause during retooling, not a retreat in threat activity.

Pivoting outward from the favicon fingerprint of a single spoofed site rapidly expanded into a large linked cluster: **84 full domains, 35 root domains, and 39 hosting IPs** sharing uniform titles, technical stacks, and script hashes—expanding to over 1,000 content-linked records.

A single week of tracking from November 8 to 15 demonstrated striking takedown resilience: after two legacy domains entered mitigation on November 8, operators **replaced them within 5 days** (registering two new domains two seconds apart on November 13 and adding another on November 15), **pushed three site generations in 6 days** (Gen 1 basic launch → Gen 2 brand-configurable templates → Gen 3 slider CAPTCHA to defeat automated scanners), and **migrated hosting entirely from domestic cloud nodes to overseas servers**.

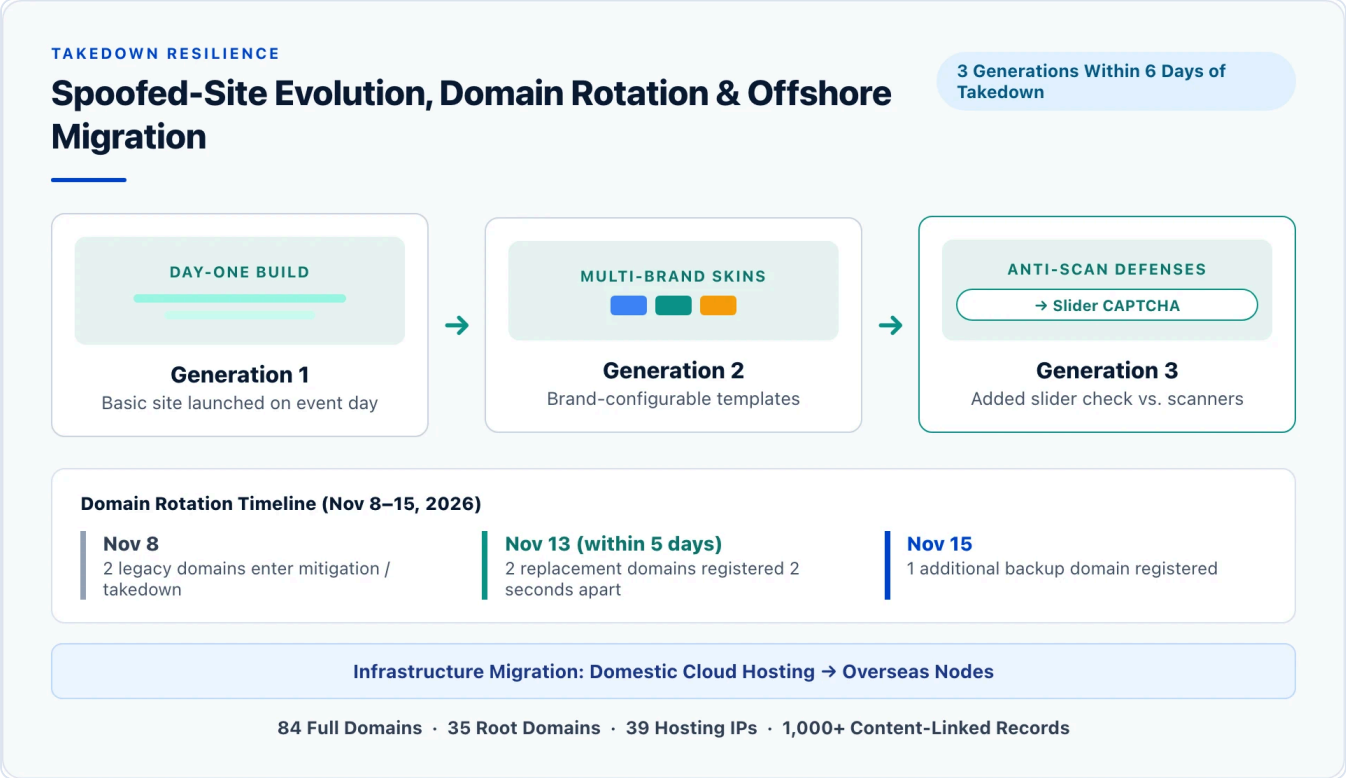


Figure 25. Six-day three-generation site evolution, five-day domain rotation, and offshore hosting migration (November 8–15, 2026). · Source: Threat Hunter Research Team

Part 4. Cross-Industry Spillover Alert: When the Same Stack Hits an 800,000-Vehicle Recall

Starting in late October 2026, monitoring detected a new campaign ostensibly targeting the automotive sector that ultimately rebounded onto consumer-finance lenders: "auto-recall" scams delivered via iOS native IP messaging. What makes it dangerous is not technical novelty, but how effortlessly cybercriminal groups reskinned existing fraud infrastructure onto a major real-world public event.

4.1 Premeditation Ahead of the News: July Domain Staging and Late-October Data Splits

Public and media warnings about auto-recall messaging scams surfaced widely in mid-November 2026, yet Threat Hunter intelligence shows preparation began well before public attention peaked: beyond interleaving recall domains with fake collection domains on July 29, **underground markets began actively trading "auto-recall" car-owner data packages on October 25, recruited rich-media dispatch farms on October 29, and delivered segmented owner batches by region, gender, and vehicle brand by October 30**.

Date	Monitored Underground Intel (Translated & Redacted)	Supply-Chain Role
2026-10-25	"CNY 38,000 batch · Guangdong · bank transfer · **auto-recall leads**"	Data trade
2026-10-26	"CNY 20,000 batch · Guangdong · postal-bank transfer · **auto-recall leads**"	Data trade
2026-10-29	"**Auto-recall rich-media** at CNY 1.3/msg; launching tomorrow, reserve slots now"	Dispatch recruitment
2026-10-29	"**Auto-recall iOS IP messaging**—capable farms reach out, top rates, escrow group filing available"	Dispatch recruitment
2026-10-29	"Custom debt-collection, **auto-recall**, and education rich-media—known farms contact me directly"	Cross-scenario dispatch
2026-10-30	Batch files: `1030-[Brand]-Owners-IM-5001/5002`, `1030-Guangdong-Female-IM-1001`	Data delivery
2026-10-30	"**Car-owner iOS messaging just started—get in early**"	Promotion pitch

Underground Jargon Quick Reference:

- **Leads ("liaozi"):** Packaged sets of personal victim records segmented by scenario and attributes for resale.
- **Blue-bubble screening ("shai IM / guolan"):** Checking whether phone numbers are active on iOS native IP messaging so rich media can be delivered directly.
- **Dispatch farm ("jifang"):** Underground operator controlling bulk device and account clusters to execute mass-messaging jobs.
- **Escrow group / filing ("gongqun / baobei"):** Underground trading groups backed by third-party security deposits to enforce settlement across buyers and sellers.



Figure 26. Batch delivery of car-owner iOS messaging data packages segmented by region and gender, October 30–31, 2026 (Chinese, redacted). · Source: Threat Hunter Research Team

> **Nature of the Spillover:** "Auto recall" was never an improvised script—it is a standing category in underground data markets. For modular cybercrime groups, the scarce resource is not attack capability, but a genuine public event that motivates victims to click.

4.2 Why Penetration Is So High: Real Public News + Real Plate Data + Fake Defect Reason

Compared with debt collection, auto-recall scams enjoy a decisive structural advantage: **they piggyback on a real, headline-making public event**. On November 4, 2026, the Defective Product Recall Center (DPAC) of China's State Administration for Market Regulation (SAMR) published a cluster of recall notices across multiple mainstream automakers covering **more than 800,000 vehicles**. In the days immediately following, large numbers of owners were actively checking whether their vehicles were affected, creating a natural window of high attention.



Figure 27. Public vehicle recall notices published on the SAMR Government Service Platform in November 2026—exploited by scammers as a real-world lure window (Chinese original). · Source: State Administration for Market Regulation (SAMR)

Attackers fused real recall news with accurate leaked owner data to send fabricated notifications such as the following example cited in a police warning (automaker name anonymized):

> [Impersonated Automaker] (Urgent Recall Notice) Dear owner: Your vehicle (Plate: Guangdong-XXXXXX) is affected by an airbag recall in which inflator fragments may eject during deployment... Recall began October 1, 2026. For your family's safety, please log in to the official website immediately to verify. — Representative fraudulent message disclosed by Shenzhen Anti-Fraud Center and Shenzhen Telecom on November 14, 2026 (impersonating a legitimate automaker).

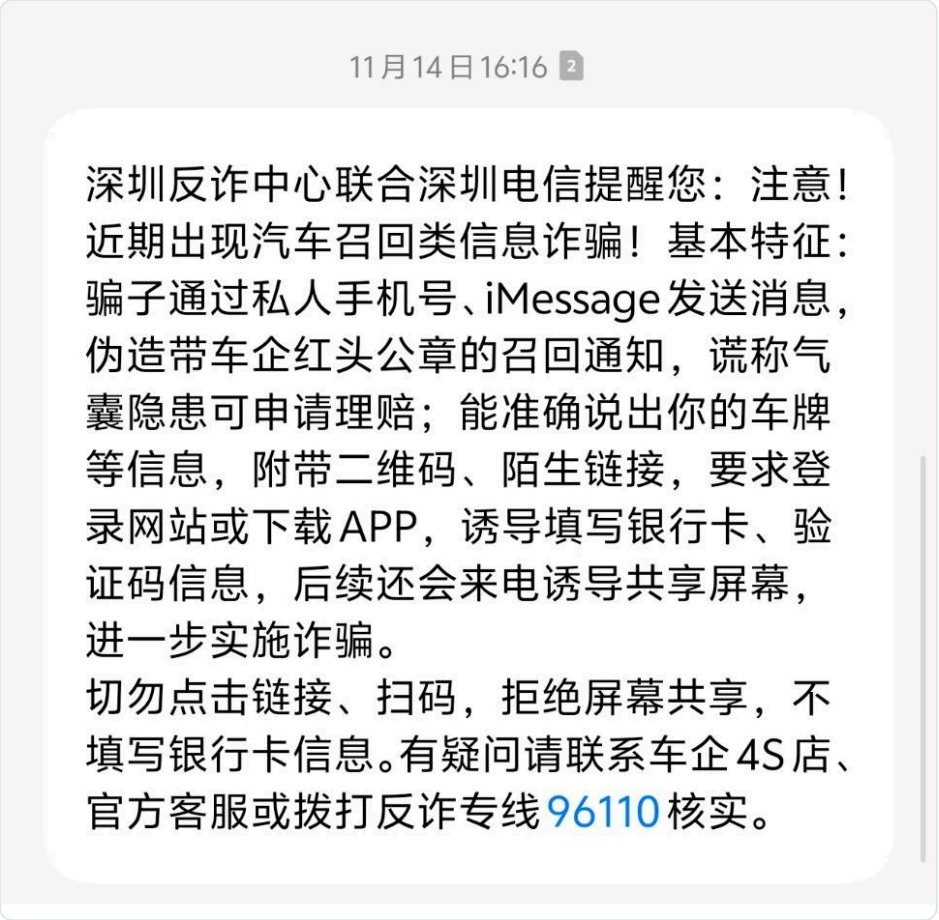


Figure 28. Auto-recall messaging scam alert issued jointly by Shenzhen Anti-Fraud Center and Shenzhen Telecom on November 14, 2026 (Chinese original). · Source: Shenzhen Anti-Fraud Center & Shenzhen Telecom

Close inspection reveals clear flaws: none of the 800,000+ recalls announced on November 4 involved airbags (they concerned steering, fuel, braking, and fastener components), the sender used a non-standard corporate name, and the claimed "October 1" start date predated the official announcement. Yet the psychological reality is unforgiving: **the moment a victim sees their exact vehicle model and license plate alongside genuine national recall news, the primary "is this event real?" filter collapses**, and very few verify technical defect details line by line.

4.3 Hidden Credit Risk: Overlapping Auto-Loan Customers Turn Legitimate Borrowing Into Bad Debt

Why does a scam dressed in automotive branding hit consumer-finance lenders so hard? Because **auto financing is a core pillar of consumer credit, and recalled vehicle owners overlap heavily with lenders' active borrower base**—a car owner on a recall list is very likely an existing prime customer of a financial institution.

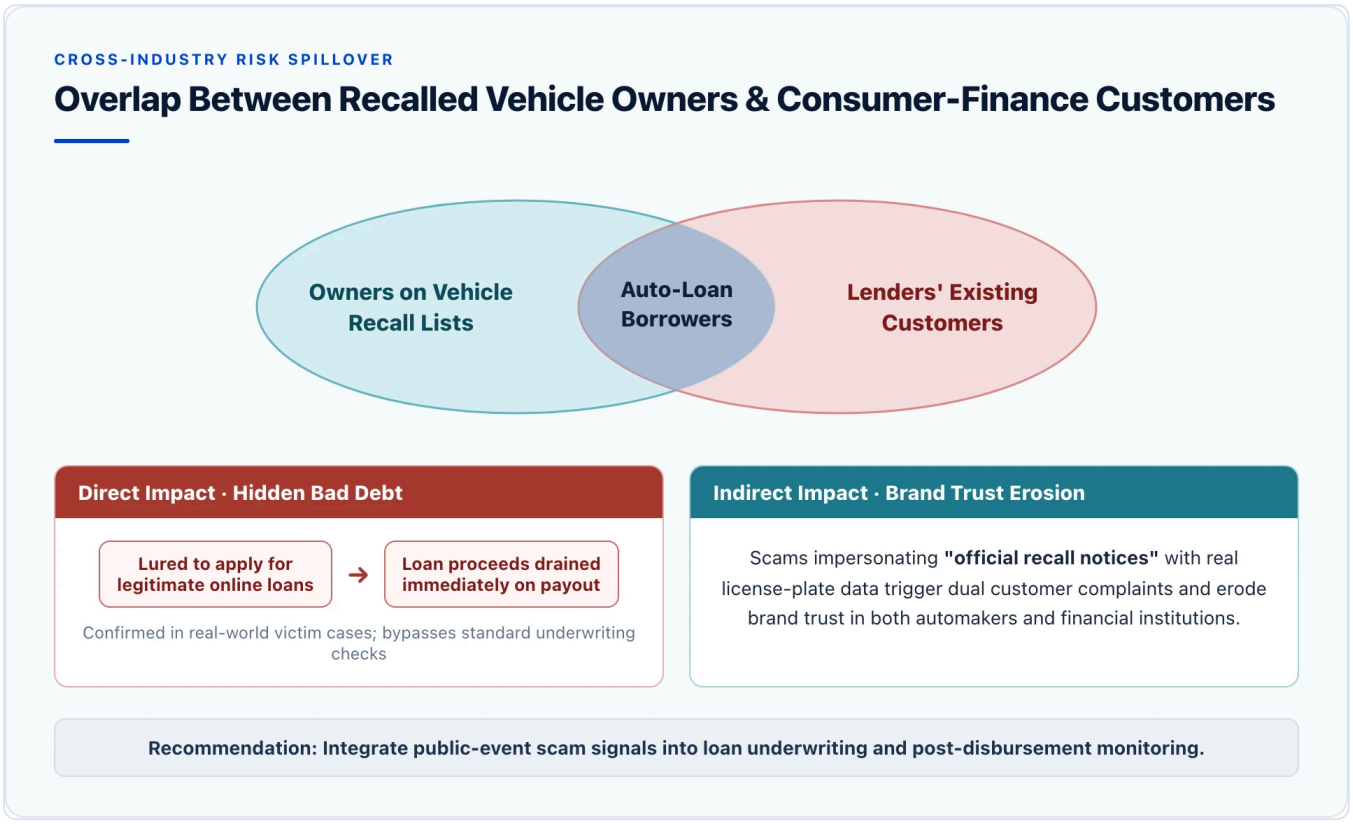


Figure 29. Cross-industry risk overlap between recalled vehicle owners and consumer-finance auto-loan customers. · Source: Threat Hunter Research Team

That overlap transmits losses to financial institutions through two concealed channels:

- **Direct credit loss (concealed non-performing loans):** Real-world cases confirm that victims guided through fake "official recall, compensation, or subsidy" flows are induced to apply personally for loans on legitimate consumer-finance or online lending platforms, only to transfer the disbursed funds immediately to scammers. Because the borrower is genuine, creditworthy, and passes identity verification cleanly, **anomalies appear only after disbursement—leaving conventional credit-underwriting fraud models largely blind** and leaving lenders holding fresh bad debt.
- **Indirect reputational damage:** Because forged "official notices" cite exact license plates and models, both the impersonated automaker and the affected financial institution absorb customer complaints and trust erosion when victims suffer losses.

The broader warning extends across industries: today this turnkey stack ("blue-bubble screened leads + iOS IP messaging or QR-free door-to-door mailers + pre-staged domain pools + polished mobile web templates") targets vehicle recalls; tomorrow, whenever a new public trigger emerges—social-security refunds, insurance claims, flight disruptions, or education refunds—operators can reskin and strike another high-value customer segment within days.

Research Statement & Compliance Notice: This report was compiled by Threat Hunter from continuous public threat intelligence monitoring between January and November 2026 covering cybercrime countermeasures and representative fraudulent infrastructure, and is published openly for partners in consumer finance, logistics, automotive, and the general public. Self-reported volumes and pricing cited from underground listings reflect raw intelligence monitoring and are unverified. Legitimate express services, official recall notices, and real law-firm names referenced in underlying cases were impersonated or abused by threat actors and have no affiliation with the fraud. Personal data, non-essential brand identifiers, and unverified technical attribution strings have been redacted in accordance with public-release compliance standards.