TrendAI™ Research



The Market for Trust

How Cybercriminals Recruit Corporate Insiders

Mayra Rosario Fuentes
Senior Threat Researcher, TrendAI™ Research

Stephen Hilt
Principal Threat Researcher, TrendAI™ Research

David Sancho
Senior Threat Researcher, TrendAI™ Research

Table of Contents

4

Key Takeaways

9

The trust problem

13

Public sector: Access-as-a-service fueled by insiders

16

Government: The scarcest commodity with the highest stakes

20

Healthcare: Patient records for the right price

24

Social media: The trust marketplace

31

Telecom: Hijacking the signal

37

Finance: The high price of a banker's access

44

Industrial and energy: Skimming at the pump

49

Shipping and logistics: Tracking numbers for hire

54

Retail: Refunds without limits

58

Reviews and reputations: Five stars on demand

61

Building the inside job

66

Conclusion

68

Recommendations

1

Key Takeaways

1. **Insider recruitment is now part of a structured underground economy.**

Insider recruitment now runs through brokers, guarantors, escrow services, and recurring partnerships on forums such as XSS, Exploit, and BlackHat World, alongside dedicated Telegram channels. Both supply-driven posts (employees offering their own access) and demand-driven posts (criminals soliciting hires at named target companies) operate openly through the same channels.

Why this matters	Risk implications
Insider access is no longer an occasional opportunity. It is a maturing market with pricing, intermediaries, and professional norms that lower the barrier to entry for any criminal willing to pay.	• Higher baseline likelihood of insider compromise across every sector • Greater difficulty distinguishing malicious activity from legitimate work • Insider events that move faster and recur more often as relationships persist • Compromise of authentication, monitoring, and approval workflows from the inside

2. **Social media platforms are a high-demand insider target.**

Underground forums covering Meta (specifically its platforms Facebook and Instagram), TikTok, X, and Google show consistent demand for insiders. Sought-after actions include safelisting ads, taking over accounts, unbanning accounts, pushing verifications, and surfacing competitor ad data. Per-account unban prices range from US$1,000 to more than US$7,000, and recruiters openly offer a 50/50 profit split to platform insiders.

Why this matters	Risk implications
Account status manipulation directly enables fraud, influence operations, and competitive sabotage at scale. A single insider can monetize access across thousands of accounts.	• Fraudulent ads reaching platform users with insider-granted approval • Reinstatement of accounts previously removed for abuse or policy violations • Exposure of advertiser data and competitive intelligence • Platform trust and safety controls undermined from within

3. **Telecommunications insiders power SIM swap and account takeover.**

Demand for telecom at carriers in the U.S., the European Union, Australia, Brazil, and Canada centers on SIM swaps and account changes. Recruiters offer recurring payment relationships in exchange for repeated swaps, with pricing structured by carrier and geography.

Why this matters	Risk implications
A single SIM swap can defeat SMS-based multifactor authentication (MFA) and unlock bank, brokerage, crypto, and email accounts in minutes. Telecom insiders sit at the chokepoint of consumer identity.	• Account takeover of customer banking, brokerage, and crypto wallets • Bypass of SMS-based MFA across the consumer economy • Regulatory and class-action exposure for carriers • Erosion of consumer trust in phone-based identity verification

4. **Shipping and logistics insiders enable marketplace and refund fraud.**

Forums show recurring demand for insiders at UPS, FedEx, DHL, and USPS. These are individuals who are in a position to generate shipping labels (often with fake delivery scans), reroute or stall in-transit shipments, and confirm bogus proof of delivery. Pricing ranges from per-scan service fees to retainers of roughly US$1,000 per day for ongoing access.

Why this matters	Risk implications
Tracking and delivery systems are the trust anchor for marketplace payouts, refund decisions, and chargeback adjudication. Insider scans turn that trust into a fraud primitive.	• Marketplace payouts released on goods never delivered • Refund and chargeback fraud against retailers and payment processors • Theft of high-value goods through rerouted or stalled shipments

5. **Financial and payment insiders monetize banking access and card data.**

Underground actors recruit insiders at banks and payment firms to initiate and approve transfers, run account lookups, and perform PIN jobs. They recruit cashiers, gas station staff, and retail staff to place card skimmers at the point of sale. Pay ranges from flat per-job fees to recurring revenue-share arrangements. In 2025, the U.S. Secret Service ran 22 nationwide operations against card skimming, inspecting nearly 60,000 terminals, gas pumps, and ATMs, and removing 411 devices.[1]

Why this matters	Risk implications
Payment systems are where insider access converts most directly to cash. An employee who can approve a transfer, expose a PIN, or seed a skimmer turns trusted financial infrastructure into a cash-out channel.	• Direct theft from customer bank, card, and brokerage accounts • Card-present fraud at fuel and retail terminals at national scale • Money-mule and PIN-job networks moving stolen funds • Regulatory, chargeback, and remediation exposure for financial institutions and merchants

6. **Data-for-sale insiders supply medical records and classified material.**

Insiders are recruited to extract and sell sensitive records that external attackers cannot easily reach, from patient medical files at healthcare providers to internal reports and classified documents inside government and defense organizations. Pricing ranges from low-cost bulk record dumps to premium intelligence work, with one buyer advertising a commission of more than US$2,000 for a successful insider introduction.

Why this matters	Risk implications
Some records cannot be obtained any other way, which makes the insider the only supplier. Medical and government data carry long-lived value for fraud, extortion, and espionage well after the breach.	• Exposure of patient medical records protected by law • Leakage of classified, controlled, or restricted government material • Long-tail identity fraud and extortion from durable personal data • National-security and regulatory consequences that outlast the initial sale

7. **Insiders manipulate trust and reputation signals.**

On platforms where reputation is the product, insiders are paid to delete negative reviews, inflate ratings, reinstate banned accounts, and approve fraudulent refunds. Review-removal listings run from US$30 to US$100 per review taken down, with “refunders” charging a percentage of each refund. However, the U.S. Federal Trade Commission (FTC) has since moved against such schemes and now authorizes civil penalties of up to US$53,088 per violation for trafficking in fake reviews.

Why this matters	Risk implications
When an insider can edit a rating, a review, or a refund decision, they are selling the platform's credibility itself. The manipulated signal is the very thing customers rely on to make decisions.	• Fraudulent refunds and chargebacks approved from inside the retailer • Fake or suppressed reviews distorting buyer and guest decisions • Reinstatement of accounts removed for abuse or policy violations • Regulatory exposure under fake-review and consumer-protection rules

8. **Insider access is sold as a turnkey commodity.**

Beyond selling data or single actions, insiders increasingly sell standing access to entire systems, collapsing a full intrusion into a single purchase. Listings range from a few hundred dollars for credentials to a government-linked platform, up to premium offers of administrator-level control inside large enterprises. These higher-tier offers are packaged with the persistence and tooling a buyer would otherwise have to build through a breach.

Why this matters	Risk implications
An insider who sells direct access removes every step of the traditional intrusion chain. The buyer skips reconnaissance, exploitation, and privilege escalation and starts with trusted control.	• Full enterprise compromise without an external breach • Single sign-on, admin, and persistence access sold as a package • Faster, harder-to-detect attacks that begin inside trusted boundaries • Exposure of customer data, funds, and downstream systems at once

2

The trust problem

Insider threat remains one of the most difficult problems in cybersecurity. An insider already possesses authenticated access, familiarity with internal systems, and the trust granted to legitimate employees—all things attackers must fabricate or work around. An insider does not need to breach the perimeter, bypass multifactor authentication (MFA), or evade endpoint protections as an outsider would. If they do things right, their actions will appear consistent with normal operations, and their malicious activity will remain indistinguishable from legitimate work.



Historically, insider incidents were framed around the disgruntled employee, the careless contractor, or the departing engineer copying sensitive files before leaving the company. That model still exists, but it now coexists with a more organized market. An active underground economy has emerged for insider access and services enabled by insiders. Cybercriminal groups, fraud operators, and ransomware groups increasingly recruit employees directly through underground forums and encrypted messaging platforms. Their offers often include fixed payments, profit-sharing agreements, referral bonuses, and ongoing partnerships in exchange for access, data, workflow manipulation, or direct assistance from inside targeted organizations.

Shifting cybercriminal ecosystems

When LockBit 2.0 relaunched in 2021, the group used victims' own compromised systems as a recruitment platform. Compromised machines displayed desktop wallpapers with offers that promised employees a share of ransom proceeds in exchange for credentials or execution of malware supplied by attackers.[2] Since then, underground recruitment activity has continued to mature and diversify.

In one forum post we have observed, a seller advertised three years of insider access within the accounts payable, accounts receivable, and payroll functions of a company. The company earned around US$25 million per year, and so the bidding for this access started at US$25,000.

We saw different examples in different industries. Carrier insiders advertise SIM swaps at Verizon, T-Mobile, and AT&T for tens of thousands of dollars plus a percentage of

downstream proceeds. One buyer offered US$1,000 per day for a FedEx employee capable of uploading tracking information into internal systems. Services backed by insiders on social media platforms openly advertise manual ad approvals, account reinstatements, and verification manipulation for Meta, TikTok, and other platforms.

These examples illustrate a broader shift within the cybercriminal ecosystem. Insider abuse is no longer limited to isolated opportunism or one-off recruitment efforts. Increasingly, it resembles a structured underground economy with brokers, recruiters, guarantors, recurring partnerships, and specialized services built around insider access.

What we examined

This research examines underground demand for insiders over the last two years. The source material includes recruitment posts, advertisements, and insider service listings collected from cybercriminal forums and Telegram channels.

We analyzed these materials to understand what threat actors are seeking, what kinds of access command the highest values, and how operations enabled by insiders are becoming integrated into the broader industrialization of cybercrime.

It is important to note that the validity of these forum posts could not be independently verified. Individual listings may represent genuine recruitment attempts, law enforcement honeypots, deliberate disinformation intended to mislead researchers, or fabricated posts intended to deceive other forum participants. Many listings provide little or no direct explanation for the requested access. However, the surrounding context consistently indicates criminal intent tied to fraud, account takeover, ransomware operations, business email compromise (BEC), or other illicit activity.

As long as a single bribed employee can do what would require a sophisticated external intrusion, insiders will remain a serious and frequently overlooked risk vector. The underground demand documented here is likely to grow rather than recede.

Supply and demand for betrayal

While it is uncommon for a person to join an organization with the intention of becoming an insider threat, human nature can be unpredictable. Over time, employees can be persuaded to act on behalf of a threat actor. This shift may be driven by changes in workplace culture, personal financial pressures, or a general dissatisfaction with their circumstances. This human vulnerability is precisely what the underground market for insider access is built to exploit.

Within this market, two distinct types of activity run in parallel. The first is supply-driven: existing employees advertise their own access for sale and approach criminal buyers directly. The second is demand-driven: criminals openly recruit employees they do not yet have, soliciting insiders to fill specific roles at named target companies.

The sections that follow trace this market across the industries where insider access is bought and sold, namely the public sector, healthcare, social media, telecommunications, finance, shipping, retail, and the reputation systems that sit behind online commerce. Each section examines who is recruited, what their access is worth, and how that access could convert to fraud, theft, compromise, or other forms of cyberattack.

3

Public sector: Access-as-a-service fueled by insiders

Insiders are selling ready-made access-as-a-service, collapsing the entire intrusion chain, including government-linked systems, into a single purchase that lets buyers skip the break-in altogether.

We identified multiple underground forums where threat actors actively advertise access-as-a-service using an insider. These actors often seek employees willing to provide access to systems and networks in exchange for payment. This access may include the reuse of passwords across personal and corporate devices, ignored MFA implementation, and unpatched vulnerabilities. Insiders help feed the credential and access market. Prices are often not advertised, as sellers ask buyers to negotiate through private message or Telegram.

In April 2026, an actor on Exploit advertised exclusive insider access to a “Tier 1 iGaming conglomerate.” The operation runs more than 100 active brands, with combined annual gross gaming revenue of roughly US$1.5 billion. The actor offers full “Master Admin” access to the back office, persistence into the enterprise Slack environment and Okta single sign-on, and real-time insider support for bypassing MFA. The post frames the access as suitable for full network ransomware deployment or systemic revenue diversion through the admin panel, and states that hardware fingerprints and session cookies are included so the buyer can impersonate trusted devices and sessions.

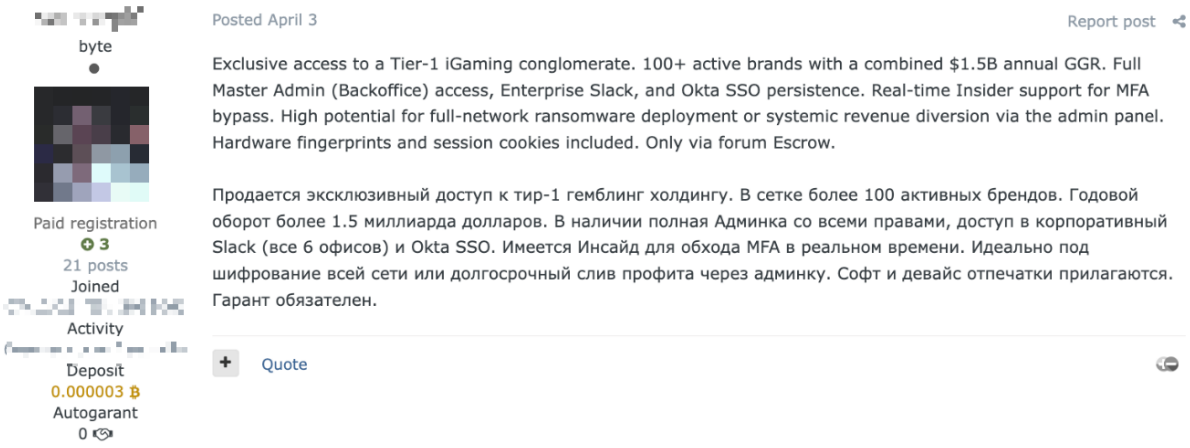
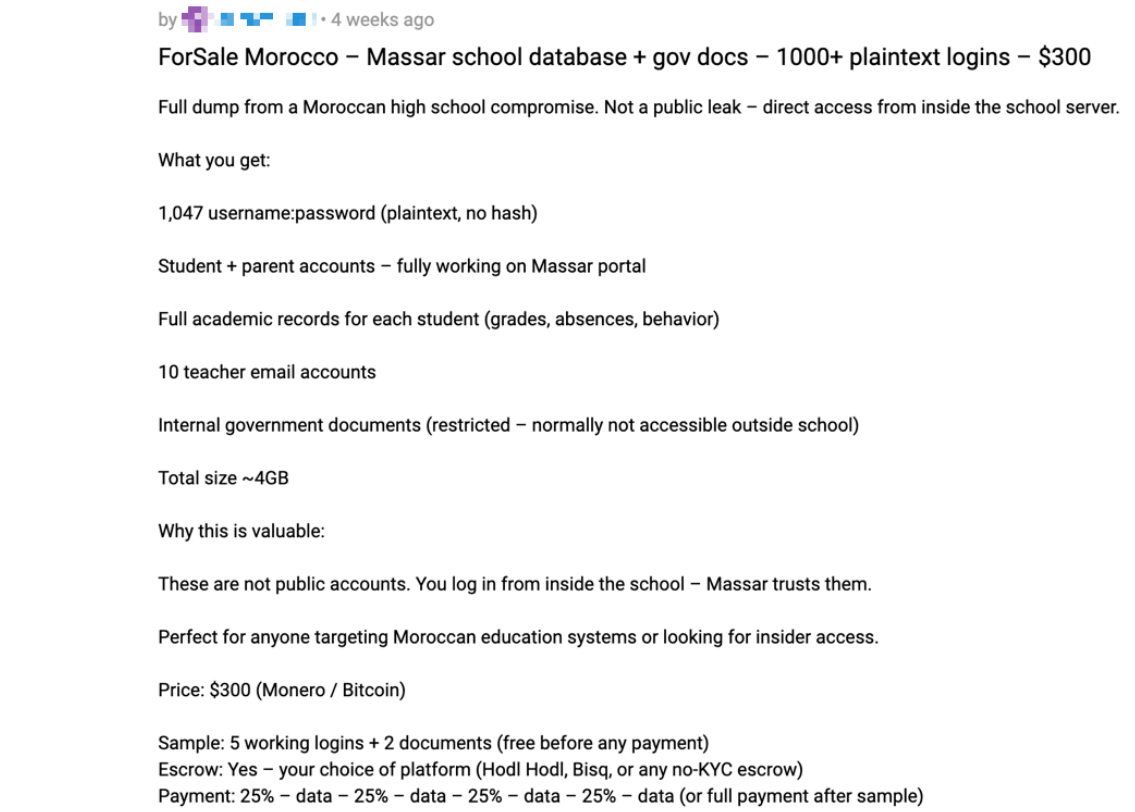


Figure 1. Access-as-a-service listing for an iGaming conglomerate

The listing illustrates how high-value insider access can compress an entire intrusion into a single purchase, combining administrative control, identity-provider persistence, and live insider assistance that bypasses the external defenses an outside attacker would normally have to defeat.

Another example, posted in May 2026, is an actor advertising a Moroccan high school dataset for sale at US$300, payable in monero or bitcoin. The actor stresses that the material is not a public leak, but rather direct access obtained from an insider of the school. Sample contents include, among other items, 1,047 plain-text username and password pairs, working student and parent accounts on the school’s education portal, and full academic records covering grades, absences, and behavior for each student.



by [redacted] • 4 weeks ago

ForSale Morocco – Massar school database + gov docs – 1000+ plaintext logins – $300

Full dump from a Moroccan high school compromise. Not a public leak – direct access from inside the school server.

What you get:

1,047 username:password (plaintext, no hash)

Student + parent accounts – fully working on Massar portal

Full academic records for each student (grades, absences, behavior)

10 teacher email accounts

Internal government documents (restricted – normally not accessible outside school)

Total size ~4GB

Why this is valuable:

These are not public accounts. You log in from inside the school – Massar trusts them.

Perfect for anyone targeting Moroccan education systems or looking for insider access.

Price: $300 (Monero / Bitcoin)

Sample: 5 working logins + 2 documents (free before any payment)
Escrow: Yes – your choice of platform (Hodl Hodl, Bisq, or any no-KYC escrow)
Payment: 25% – data – 25% – data – 25% – data – 25% – data (or full payment after sample)

Figure 2. Insider listing selling Moroccan school and government records

The listing demonstrates how insider access to a government-linked education platform is packaged and monetized. Trusted internal credentials and restricted official documents are offered as a turnkey path into systems that external attackers could not reach directly.

What these two listings have in common is that the insider collapses the entire intrusion chain into a single transaction. An external attacker normally must perform reconnaissance, breach the perimeter, escalate privileges, and establish persistence, and each of those stages is a chance to be detected and stopped. An insider sells all of it at once, delivering working credentials, administrative control, and identity-provider persistence from inside the trust boundary, and in some cases offering live assistance to defeat the controls that remain.

In this market the buyer is not paying to break in but paying to skip the break-in entirely, which makes insider-enabled access among the most efficient and most dangerous products documented in this report.

4

Government: The scarcest commodity with the highest stakes

Government insiders are the scarcest commodity in the underground market. Unlike the open volume we will show later for social media or retail, they appeared only occasionally in our research. This is likely because of credibility concerns, limited demand, or recruitment that moves to private channels. However, the few listings that do appear command premium prices and provide access to sensitive systems and nation-state intelligence.

We saw a BreachForums listing advertising persistent two-factor authentication (2FA) bypass and active employee credentials inside Brazil's Conselho Nacional de Justiça, the country's National Council of Justice. The advertisement mentions how such services are offered at a high price, but the exact amount was not disclosed in the posting.

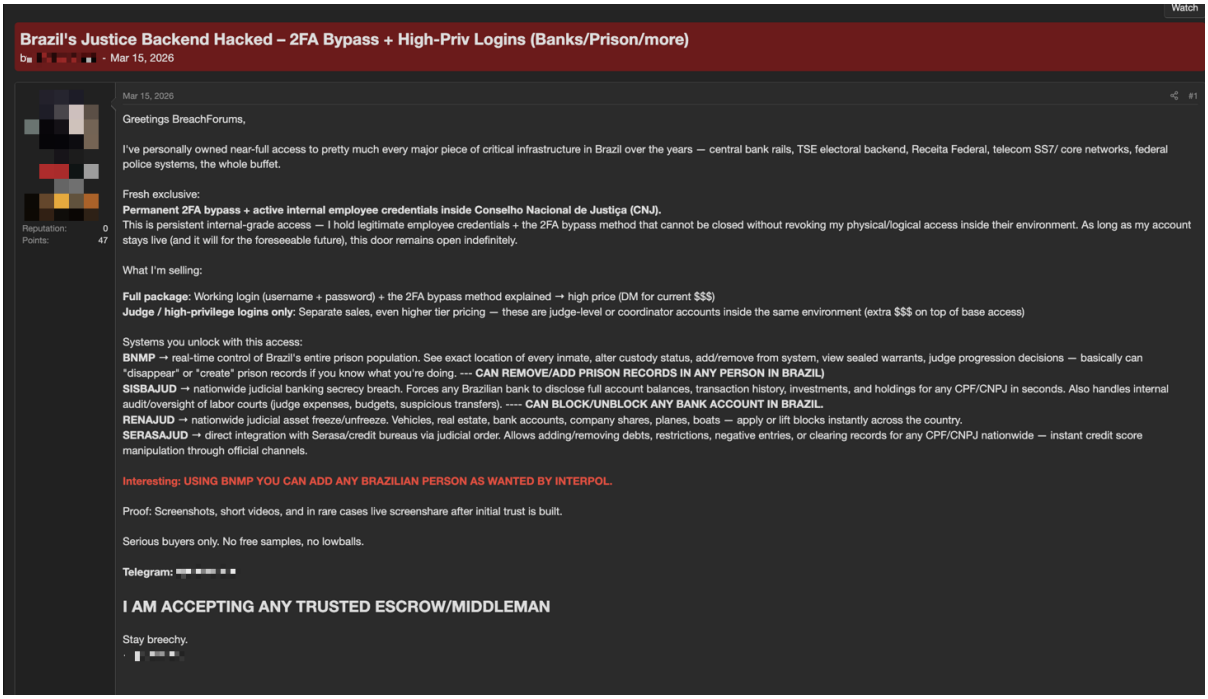


Figure 3. An active employee at Brazil's Conselho Nacional de Justiça offering their insider services

We found one listing posted in several forums written in Mandarin, openly advertising to buy internal government intelligence from a defined set of nation-states. These include the U.S., China, Japan, India, and Russia, and the actor offers to pay a premium for such material. The buyer specifies an interest in policy materials, internal reports, classified documents, and military intelligence.



Figure 4. Mandarin-language listing seeking a government insider

We found another post seeking classified documents tied to U.S. and NATO military, political, and technology programs, enumerating specific handling caveats and classification markings such as controlled unclassified information (CUI), for official

use only (FOUO), for internal use, NATO Restricted, EU Restricted, EU Secret, Official Sensitive, Distribution Statement C/D/F, Confidential, Rel to NATO, and Top Secret.

The level of detail in the post demonstrates familiarity with how such material is controlled. Critically, the buyer explicitly recruits current or former insiders from U.S. or NATO government, military, and defense contractor organizations. They offer a commission of more than US$2,000 for a successful introduction. The buyer supplies multiple contact channels such as a Jabber address, a Proton email, and a full Pretty Good Privacy (PGP) public key block to enable encrypted communication. The account's visible reputation and posting history lend the buyer credibility—cues these markets rely on.

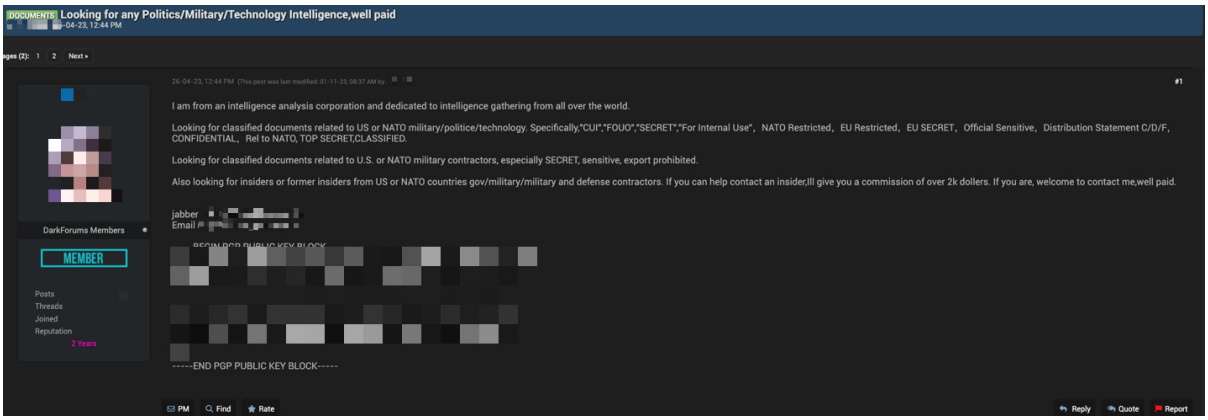


Figure 5. Listing seeking an insider for intelligence material

Another listing, posted in January 2026 and later modified in February, advertises insider access to economie.gouv.fr, specifically to TRACFIN. TRACFIN, the French Financial Intelligence Unit under the Ministry of Finance, is mandated to combat money laundering, tax fraud, and terrorist financing.

In exchange for the help of an insider, the actor offers full access to the government panel or the release of complete data on any person who holds a French bank account. Sample data includes customer identification details such as name, date of birth, address, and phone number; insurance contract details; transaction history related to suspicious operations; and the amounts, frequency, and origin of funds where available.

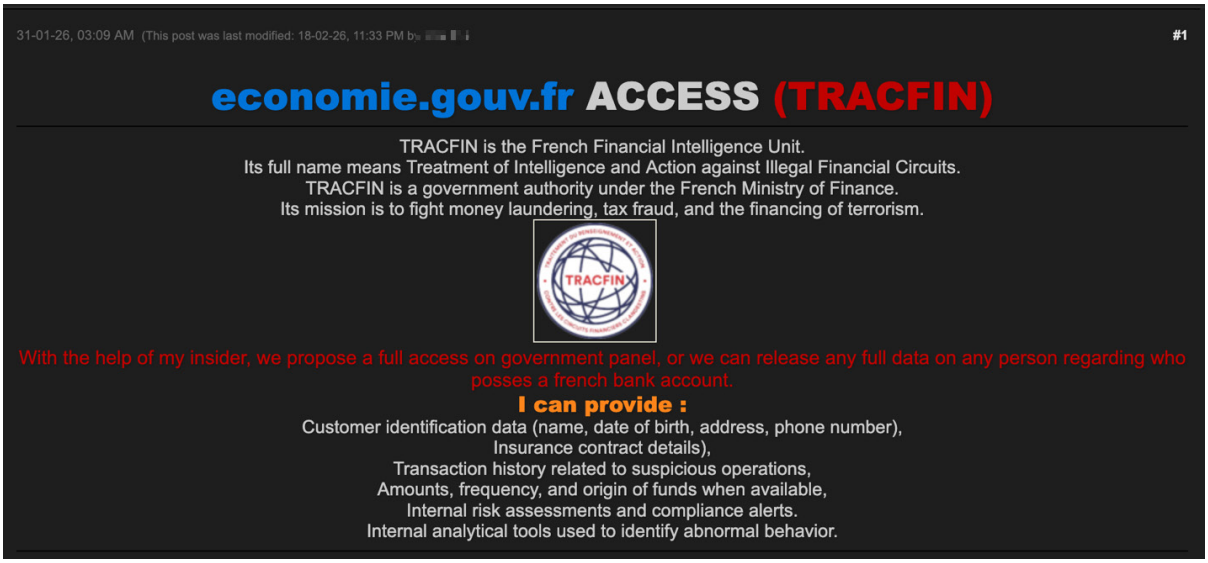


Figure 6. An offer to provide insider access to a French financial intelligence unit's data

As mentioned at the start of this section, government insiders are the rarest listings in this research. That scarcity is itself the finding. The buyers in this category are not fraud groups chasing a quick payout but actors seeking intelligence, classified documents, and standing access to state systems. The small number of advertisements reflects how carefully this trade is conducted rather than how little it matters.

A single recruited insider within a court system, a financial intelligence unit, or a defense program can expose far more than any individual bank account or retail refund. That makes the thinnest market documented in this report also the one with the highest stakes.

5

Healthcare: Patient records for the right price

Healthcare faces insider risk from two fronts. Employees steal and quietly alter permanent medical records that victims cannot reissue. Cybersecurity professionals hired to respond to ransomware attacks instead carry them out against U.S. companies.

Medical records are among the most durable commodities in the underground economy. A patient cannot cancel a diagnosis or reissue a date of birth the way a bank can replace a compromised card. That permanence makes healthcare insiders especially valuable. The betrayal documented here extends from clerks who handle records all the way to professionals hired to defend hospitals against attack.

We found several healthcare databases for sale on underground forums, with sellers explicitly stating that the data had been obtained through an insider. One listing on the Exploit forum advertised a healthcare company client database of more than 500,000 records. Drawn from 2024 through 2026 and priced at US$350,000, the database included Social Security numbers, dates of birth, addresses, and phone numbers. The seller also offered ongoing access to the underlying database.

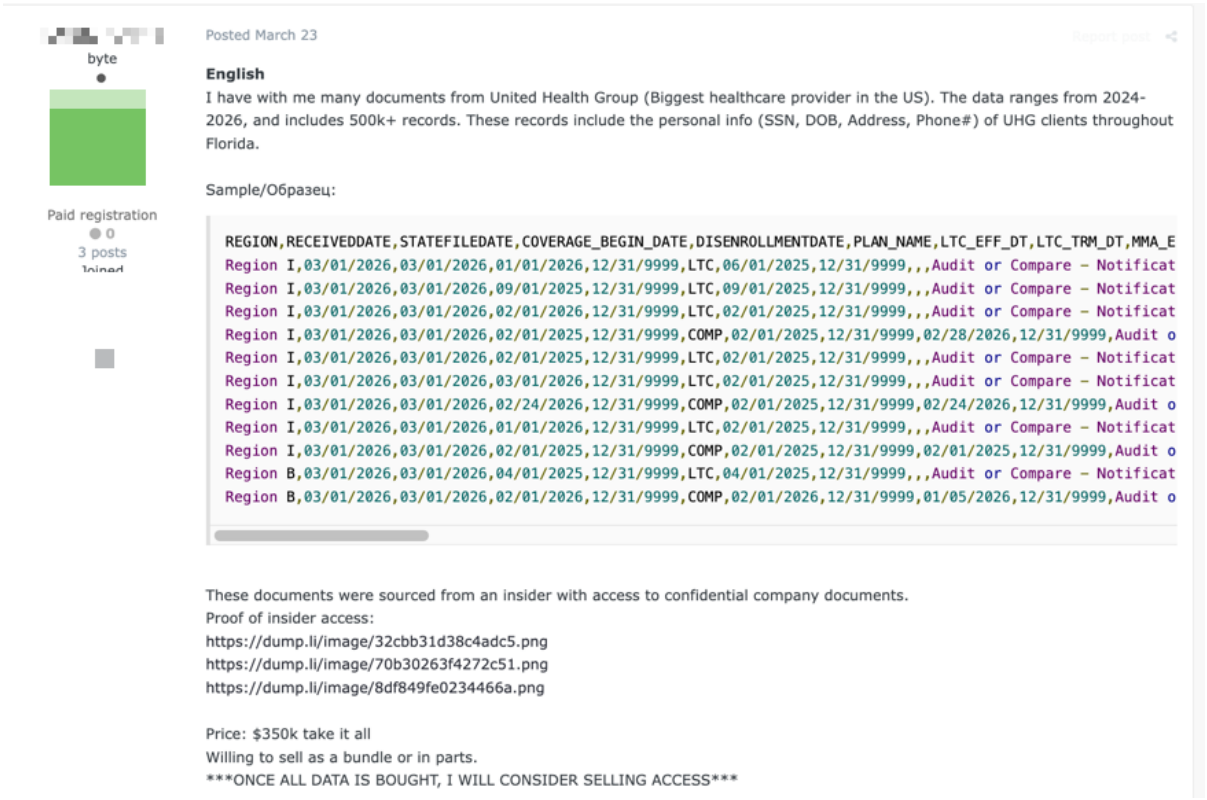


Figure 7. Listing offering U.S. healthcare company records obtained from an insider

Insiders are sought not only to steal records in bulk but also to quietly alter them. We identified one such request, in which a buyer sought an insider at a U.S. medical card service who could add “Hard of Hearing” status to medical cards, with contact directed to Telegram.

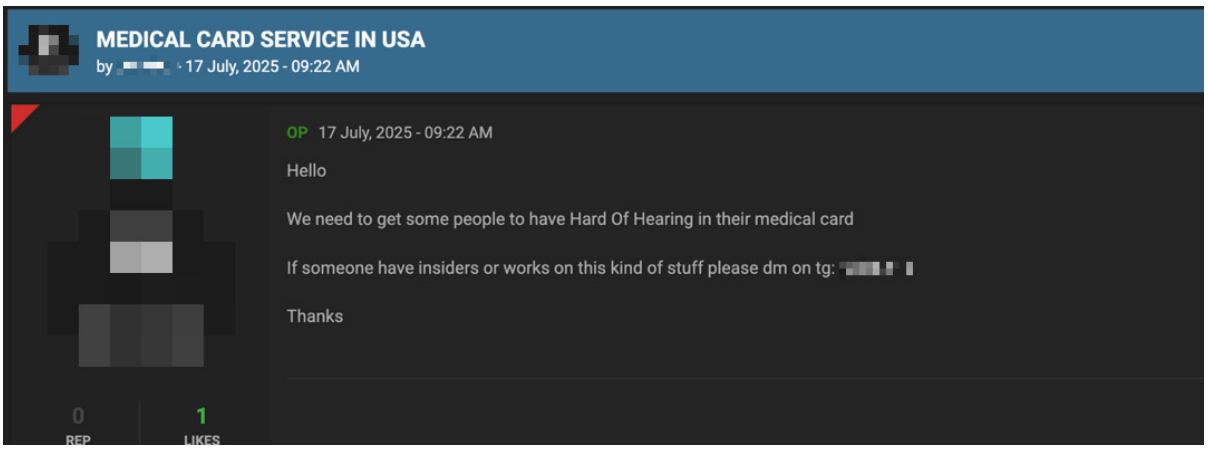


Figure 8. A post looking for an insider to modify medical cards

The intended use of this fraudulent status modification is unclear, but we can identify several plausible motives tied to the discounts and benefits available to deaf or hard-of-hearing individuals. For example, some state departments of motor vehicles issue disability license plates and driver's license endorsements designed to alert law enforcement and emergency responders that a driver is deaf or hard of hearing, and these can come with reduced fees. Several cell phone carriers also offer discounted service plans for deaf or hard-of-hearing customers. Most significantly, hard-of-hearing status that meets the Social Security Administration's Blue Book criteria can qualify an individual for Social Security disability income, which can pay more than US$1,000 per month.[3]

Insider risk in healthcare also extends to the very professionals retained to defend against ransomware. Investigations by the U.S. Department of Justice and the FBI found that several U.S.-based ransomware negotiators and cybersecurity professionals became affiliates of the BlackCat (ALPHV) ransomware group in 2023.[4]

These individuals used their positions at legitimate cybersecurity firms to act as double agents, conspiring with the ransomware actors to extort the companies they attacked and split the proceeds. The people hired to contain an attack were the same people engineering it, which inverts the most basic assumption a victim makes about the firm defending it.

They specifically targeted entities in the healthcare sector in May 2023. That year a spate of cyberattacks targeted healthcare entities within months of each other. A Florida medical device company was attacked and faced a US$10 million ransom demand.[5] The company ultimately paid approximately US$1.27 million. That month, a pharmaceutical company was also attacked. A few months later, in July 2023, a California doctor's office was hit with a US$5 million demand.[6]

Healthcare therefore faces insider risk from both directions, with employees stealing and altering records from the inside and defenders turning against their clients by engineering the very attacks they were paid to fight.

6

Social media: The trust marketplace

Social media insiders are recruited to approve fraudulent ads, reinstate banned accounts, and manipulate verification and takedowns. This turns platform trust into a standing, openly priced market that persists even after companies fire the insiders behind it.

Underground forums covering Meta (Facebook, Instagram, and WhatsApp) and TikTok show a consistent demand for social media insiders. We identified forum posts seeking two things in particular: ad approvals and visibility into competitors' ad campaigns.

Buyers want insiders who can safelist ads or pull information on rival advertisers. One service charges US$50 to US$100 per manually approved Facebook ad, with discounts for volume.

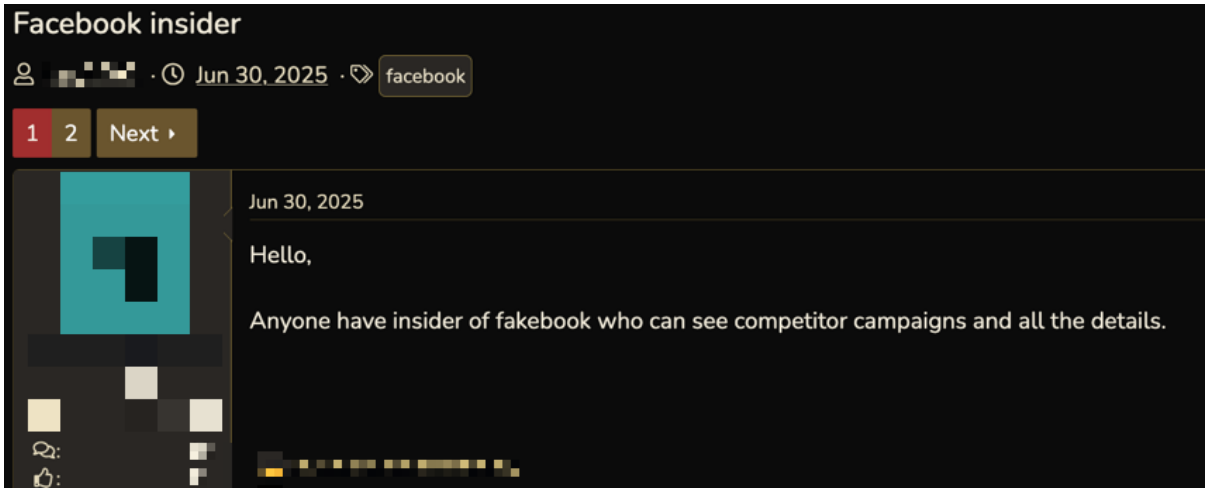


Figure 9. Post seeking a Facebook insider who can see competitor ad campaigns

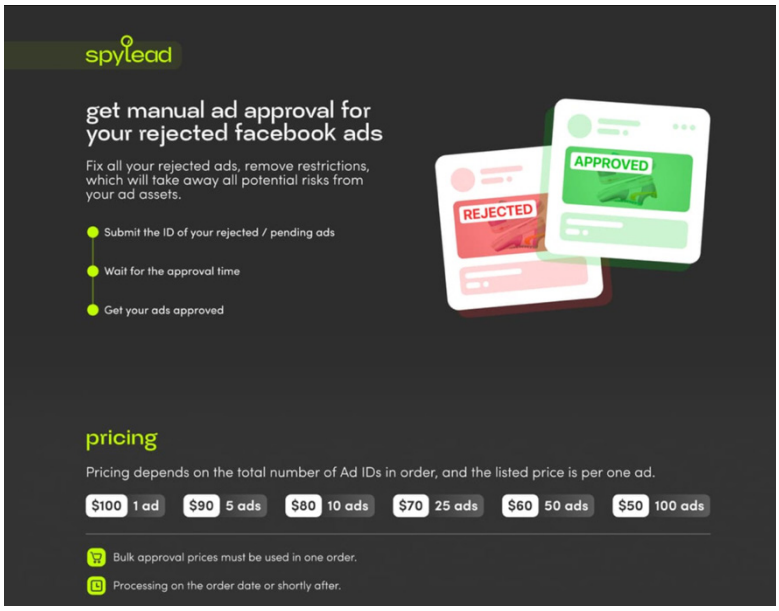


Figure 10. Advertisement offering manual approval of rejected ads

For ads, the business case for buyers is straightforward: An insider who can push a scam ad through review turns ad approval into a fraud pipeline.

Account reinstatements run higher, ranging from US$1,000 to more than US$7,000 per account. Pricing is driven by follower count, account age, and the reason for the ban, with high-profile accounts commanding the top of the range.

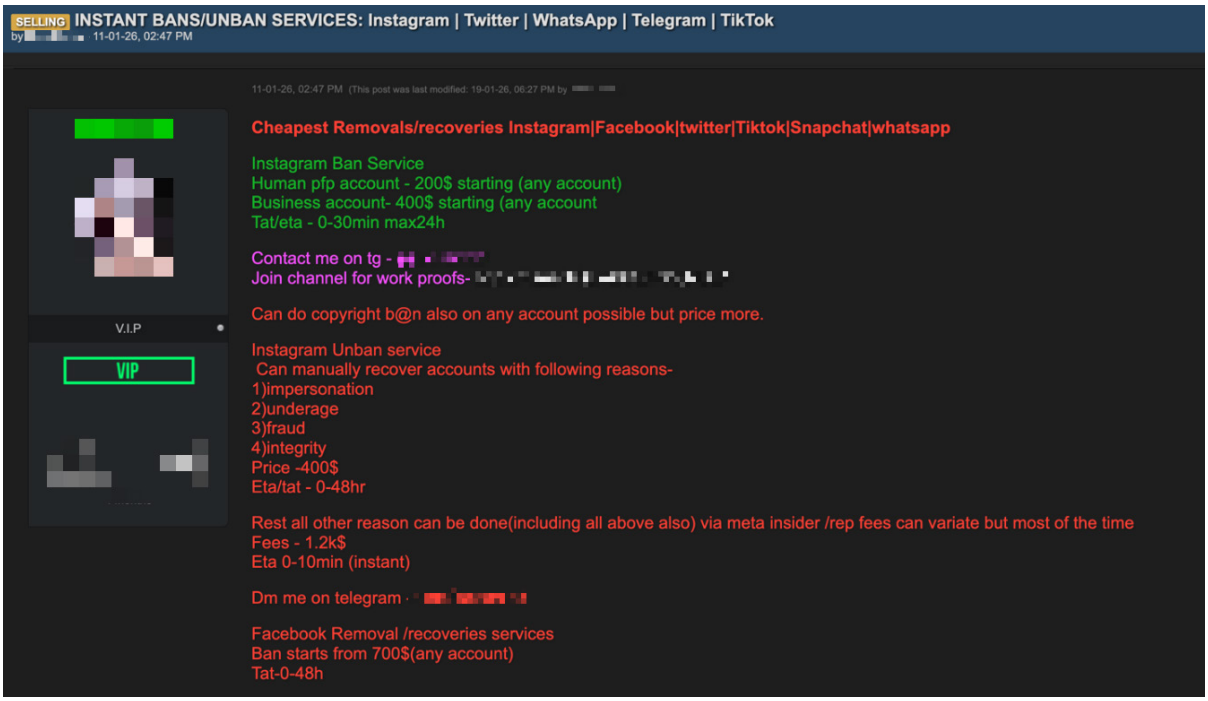


Figure 11. Sample of instant (within 10 minutes) ban and unban service being offered

We also saw multiple listings for account status manipulation, covering unbans, verification, and takedowns, where recruiters openly offer a 50/50 profit split to platform insiders at Meta, X, and Google. Among these listings, buyers also sought TikTok insiders to manually safelist ads. Sellers also used Telegram channels to offer social media unbans.

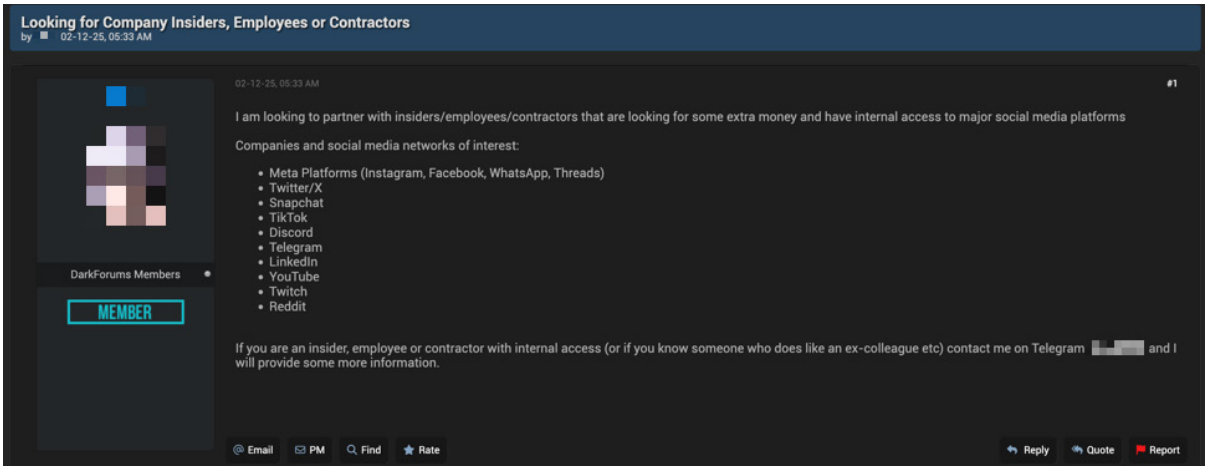


Figure 12. Post looking for social media insiders

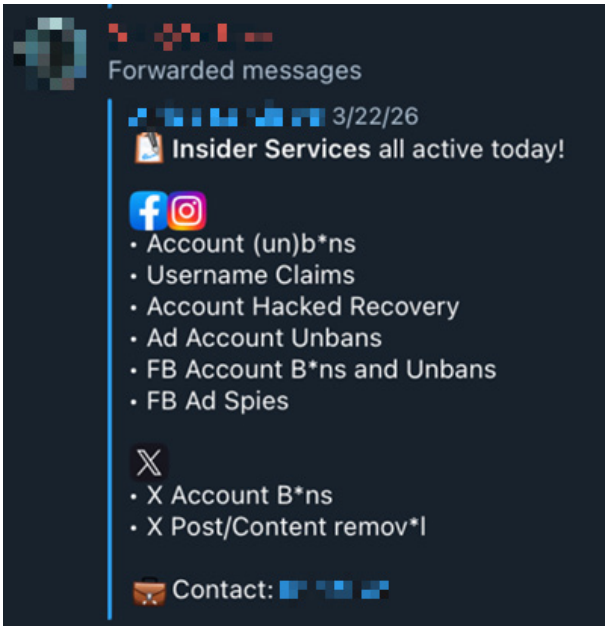


Figure 13. Telegram channel advertising spazzing and social media unbans

Meta's internal account recovery tool, Online Operations, known internally as "Oops," has been used by cybercriminals for abuse. Oops was originally built to let employees help locked-out colleagues, friends, family, and high-profile partners to regain access. Over time, access expanded to dozens of Meta employees, and even third-party Allied Universal security guards physically stationed at Meta offices. Insiders realized they could use Oops to recover any account, not just ones belonging to people they knew. Thus began the sale of this service to outsiders, brokers, and other malicious actors for bribes of up to US$7,000 per account restoration.

Such abuse has not gone unnoticed and has resulted in real consequences. In late 2022, Meta fired or disciplined more than two dozen employees and contractors for misusing Oops to take over user accounts, in some cases for thousands of dollars in bribes paid in bitcoin.[7] In March 2023 Meta sued alleged brokers in the Ontario Superior Court of Justice for orchestrating these reinstatements.[8]

Investigations have since found the underground trade in Oops access continuing years after the firings, which demonstrates that enforcement against individual insiders has not closed the market their access created.[9]

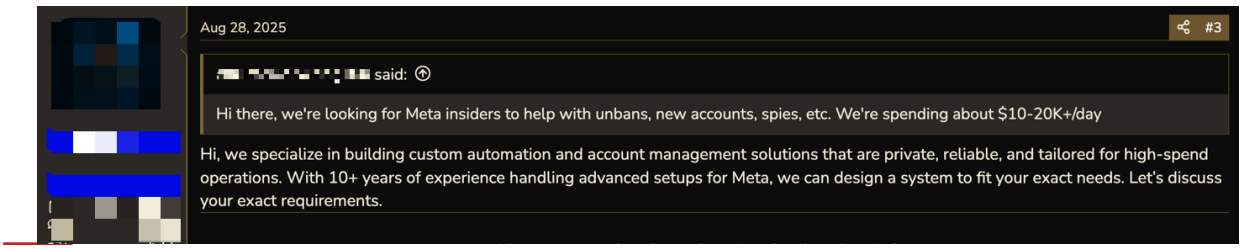


Figure 14. Response for Meta insiders

Underground forum users have also pointed buyers to SWAPD at swapd.co for social media insiders. SWAPD presents itself as a "digital rights marketplace"—a forum-based escrow platform where buyers and sellers trade digital assets, with the platform holding payment as the middleman until the deal closes.

The live listings on SWAPD as of April 2026 tell a different story. Alongside legitimate account trading, the platform openly hosts services that are possible only through insider access at Meta, TikTok, and other platforms. Representative listings include the following:

- Facebook ad account unbans via insider: One active listing advertises, "If your Facebook ad account has been disabled, I can unban it within 3-5 days. I do not need access to your Facebook account. This ban is being done via an insider. It is not a support ticket." The advertised price is US$1,950.
- Instagram account recovery, backed by verified Meta network: An Instagram recovery listing advertises a "$1,000 flat" service with "fast turnaround (often within minutes, guaranteed within 24 hours)" and explicitly states it is "backed by verified Meta network."

Each of these listings implies the existence of at least one insider behind the service, whether a current or former employee, a contractor, or someone else with access to the platform's internal systems.

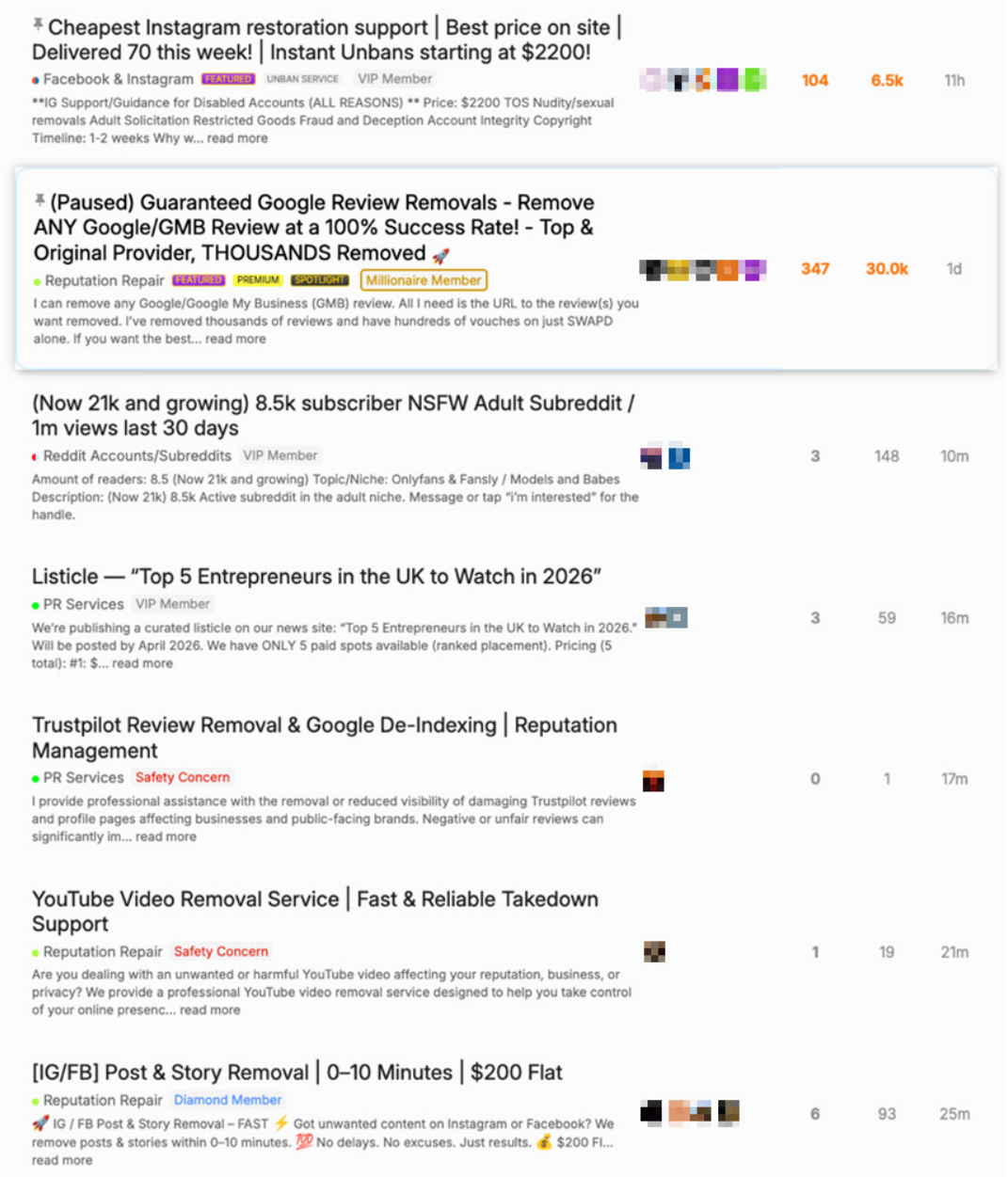


Figure 15. Snapshot of SWAPD on April 23, 2026

Table 1 shows the average prices for the services we found. Most providers advertise a standard turnaround of 72 hours or more, while instant unbans can cost twice as much or more. Copyright and intellectual property unbans carry additional fees because these cases are more complex. Reinstatement after a copyright or intellectual property ban on major platforms is generally difficult to achieve through the standard appeal process.

Platform	Service	Price
Instagram	Unban	From $400
Facebook	Unban	From $700
Twitter/X	Unban	From $500
WhatsApp	Unban	From $400
TikTok (non-US)	Unban	From $300
TikTok (USA)	Unban	From $500
Snapchat	Unban	From $600
WeChat	Unban	From $150
Facebook	Ad approval (manual)	$50 – $100/ad
Facebook	Ad account unban (insider)	From $1,500
Instagram	Account recovery (Meta network)	From $1,000
Most social media accounts	Instant unban	$1,500 – $3,500

Table 1. Average prices for offered social media services in U.S. dollars

These listings show that social media insider access is valuable for reasons that extend well beyond any single account. An insider who can approve ads turns platform review into a fraud distribution channel; an insider who can reinstate accounts converts a platform failure into a recurring paid service; and an insider who can manipulate verification or takedowns can launder reputation or silence competitors on demand. The price table represents a standing market in which platform trust itself is the commodity being sold.

7

Telecom: Hijacking the signal

Telecom insiders are among the most sought-after and highest-paid in the underground. A single bribed carrier employee can perform a SIM swap that defeats text-message 2FA and hands attackers a victim's email, banking, and cryptocurrency accounts.

Telecom carriers have access to customer identity, financial accounts, authentication systems, and sensitive communications infrastructure. Carrier employees, including retail store associates, call center agents, and back-office account managers, routinely touch all four. It is no surprise that SIM swapping is among the most dominant insider use cases at carriers.

A carrier employee with access to account management systems can transfer a victim's phone number to a SIM card controlled by a criminal, who then receives the victim's text-message authentication codes and takes over any account protected by SMS-based verification. Recruiters in underground forums openly advertise SIM swaps at Verizon, T-Mobile, and AT&T for US$20,000 plus 20%. MetroPCS was listed at a lower price of US$10,000 plus 20%.

Across these categories, two distinct attack patterns recur. In the first, an outsider impersonates an employee or customer and pressures the carrier's IT help desk into resetting credentials and bypassing 2FA. In the second, an actual carrier employee is caught accepting bribes in exchange for using their own legitimate access to bypass 2FA and reset accounts on behalf of criminals. The two patterns differ in who is sitting at the keyboard, but they exploit the same combination of help desk authority and lightly audited account management tooling.

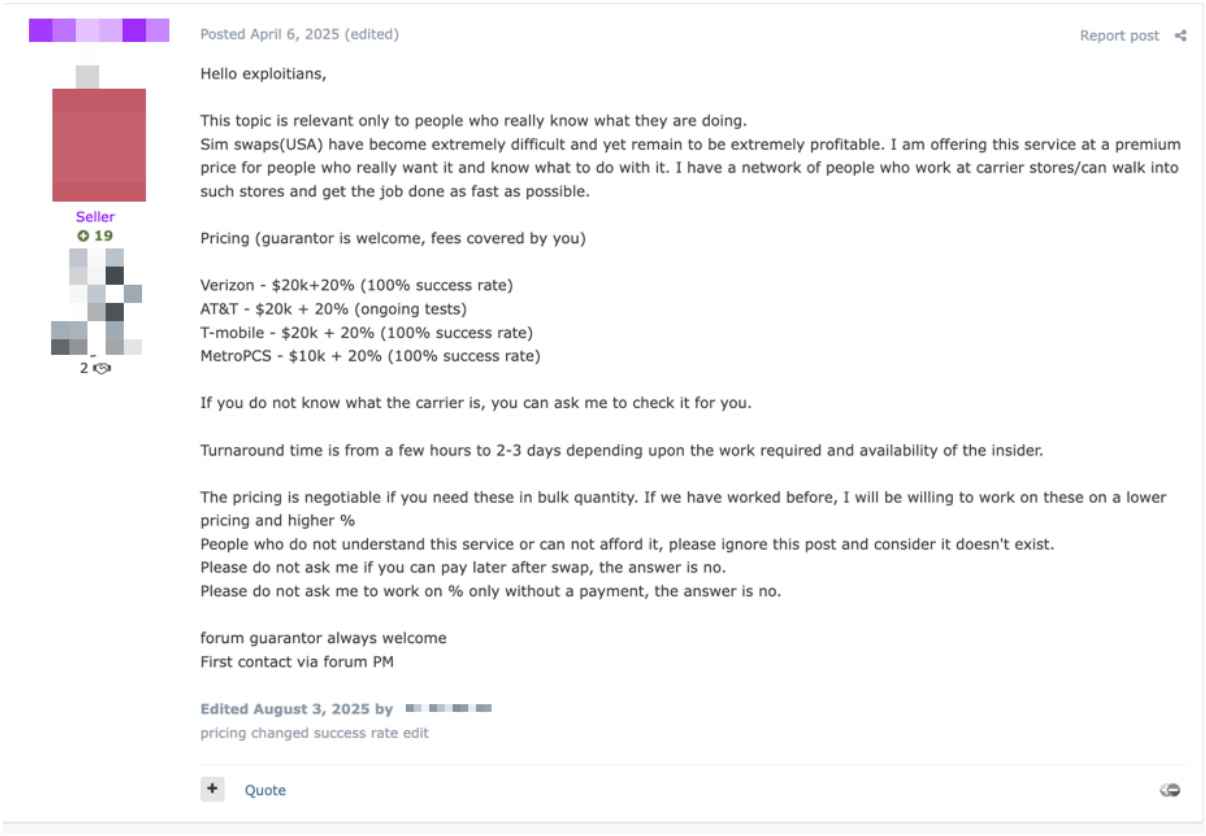


Figure 16. Forum listing offering SIM-swap services through a network of carrier insiders

On the supply side, one self-described T-Mobile USA insider advertised a full menu of services, including SIM swaps against an existing customer SIM, SIM swaps against a freshly generated eSIM that the buyer would activate by scanning a QR code, lookups of Social Security numbers (SSN), driver's license (DL) numbers, and dates of birth (DOB), retrieval of customer message and call history, and cell-tower location lookups.

The same seller declined to take on International Mobile Equipment Identity (IMEI)-unlock work, describing it as too labor-intensive for the payout. A separate post advertised SIM-swap services across nearly all U.S. carriers, requiring only the target's email address as input, priced at US$3,000 plus a share of any cryptocurrency proceeds, and promising a turnaround of 3 hours.

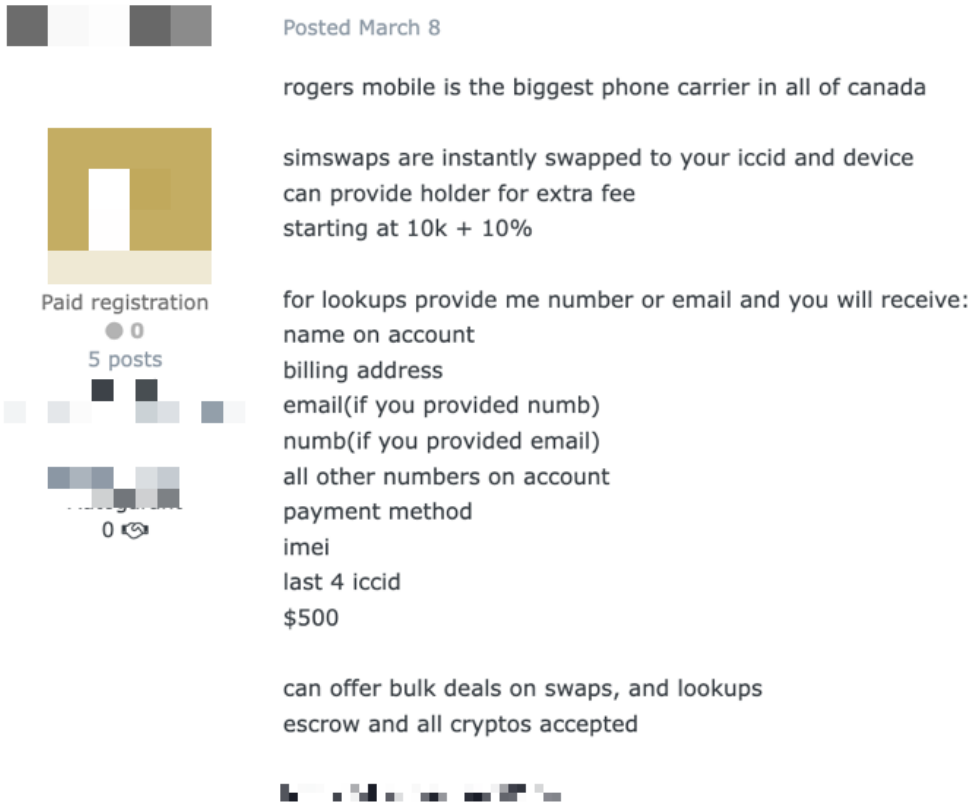


Figure 17. Insider services from US$500 and up for Rogers, a Canadian mobile carrier

A more elaborate listing offered SIM swaps against carriers in multiple markets as noted in Table 2. The seller stated the swaps were performed by insiders and store managers without any social engineering of the customer. Prices started at US$15,000 plus a 15% profit share, with turnaround times ranging from 30 minutes to 48 hours depending on the carrier.

Region/Country	Carriers
U.S.	Verizon AT&T T-Mobile
Poland	Orange Play Plus
Australia	Optus Vodafone Telstra
Brazil	Vivo Claro TIM Algar
Canada	Bell Rogers Telus

Table 2. Regions and carriers that were advertised in an elaborate listing

A separate Irish-market listing advertised SIM swaps against Eir, Vodafone Ireland, and Three, with the operator stating that insiders were already in place and that they were looking for collaborators.

On the demand side, we also identified buyers explicitly looking for SIM-swap services at AT&T, T-Mobile, and Verizon, offering a 50/50 profit split to any insider willing to perform the swap.

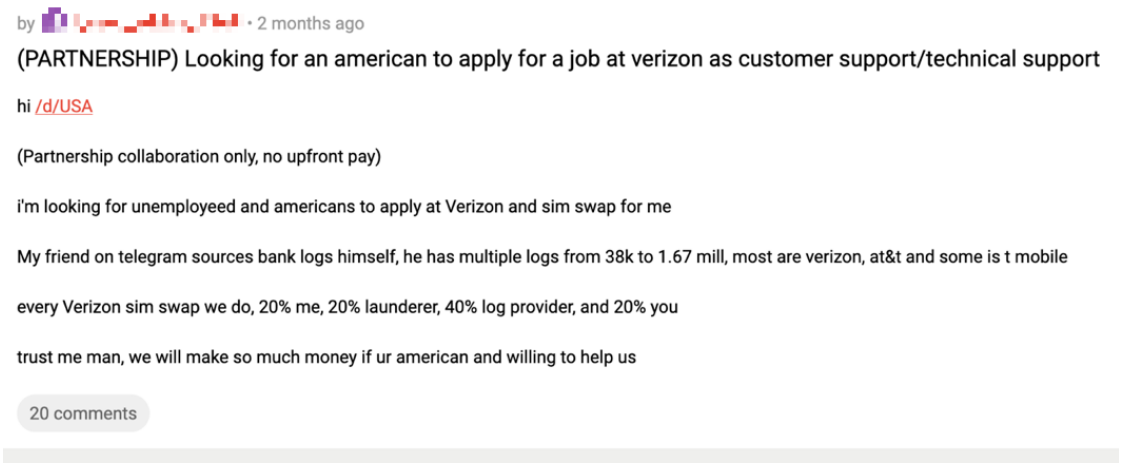


Figure 18. Forum advertisement offering a profit-sharing partnership to a current Verizon employee

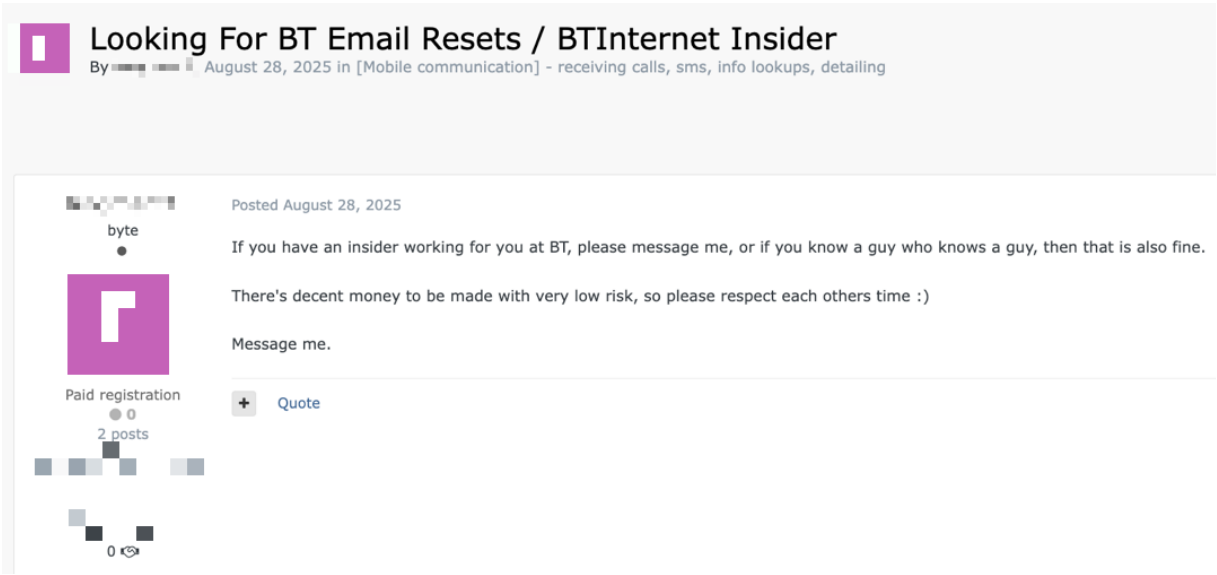


Figure 19. Forum post looking for a BT (British Telecom) insider

In May 2021, a manager at a telecom retail store in Marlton, New Jersey, used his managerial credentials to access customer accounts and transfer five victims' phone numbers to SIM cards controlled by a criminal associate. He received US$1,000 per swap, or US$5,000 in total, plus a percentage of profits paid in cryptocurrency. In March 2024, he pleaded guilty to conspiracy to gain unauthorized access to a protected computer.[10]

In November 2025, the Manhattan district attorney announced the indictment of an organized ring that allegedly stole US$435,000 from four Manhattan victims.[11] The alleged ringleaders directed the swaps and the movement of funds. A third conspirator recruited and paid four carrier employees to perform unauthorized SIM swaps using their inside access.[12]

Table 3 consolidates the telecom insider services and average prices observed across the forum listings and Telegram.

Carrier / Region	Service	Price
Verizon/T-Mobile/AT&T (US)	SIM swap bulk	$20,000 + 20% profit share
Verizon/T-Mobile/AT&T (US)	SIM swap individual	From $180 per phone
MetroPCS	SIM swap bulk	$10,000 + 20% profit share
All carriers	SIM swap quick 30-minute to 3-hour turnaround	From $3,000 per phone + profit share
US/EU/AU/BR/CA (multi-carrier)	SIM swap bulk	From $15,000 + 15% profit share

Carrier / Region	Service	Price
EE/Vodafone	SIM swap individual	From $150 per phone
Rogers (CA)	SIM swap individual	From $500 per phone
Most carriers	SSN/DL/DOB lookup	From $400 per phone number

Table 3. Average prices for offered telecom services in U.S. dollars

These findings show how the insider economy is operating in the open. That combination of high prices, wide geographic reach, and consistent demand is why SIM-swap recruitment remains one of the most durable insider markets we observed.

8

Finance: The high price of a banker's access

Financial insiders are the necessary link in large fraud schemes, recruited to approve payments, extract customer and transaction data, and disable the fraud controls that would stop a transaction. A parallel strand of insiders meanwhile handles the physical cash-out through ATM and point-of-sale (POS) skimming and fraudulent financing.

An insider at a bank, payment processor, or other financial services company is often the necessary link in a large fraudulent scheme. Underground actors recruit financial-sector insiders to approve payments and transfers, to extract customer profiles and transaction histories, and to disable or downgrade the fraud controls that would otherwise stop a transaction in flight.

The recruitment posts we observed targeted three overlapping populations, namely payment-processor staff with policy and risk authority, retail and back-office employees at traditional banks and neobanks, and customer-support and verification personnel at cryptocurrency exchanges. A separate strand of activity recruits insiders not for data or approvals but for the physical cash-out stage of fraud, including ATM withdrawals, POS skimming, and fraudulent vehicle financing.

A self-identified seven-year Stripe employee, since banned, hosted an open question and answer thread on a cybercriminal forum. The poster offered paid guidance on how to operate in high-risk merchant categories, on cloaking techniques used to disguise the true nature of a checkout flow during Stripe review, and on which limited-liability-company structures Stripe's onboarding systems treated as low-risk.

The post is notable because it monetized institutional knowledge about a specific risk-review process rather than a stolen account or a credential. This demonstrates that long-tenured, well-placed employees can themselves become the product on offer.

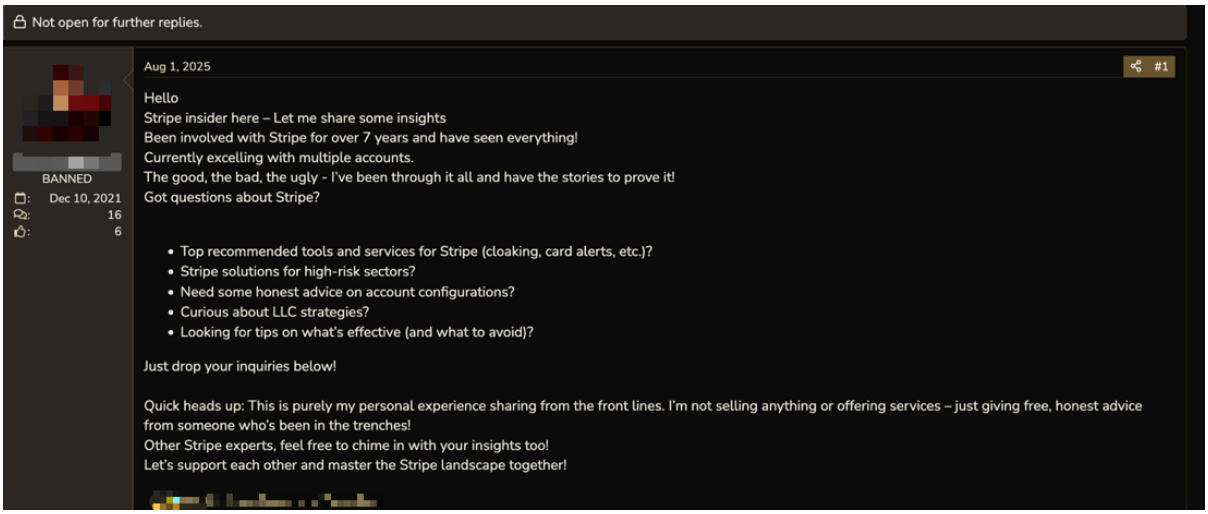


Figure 20. Stripe insider offering their services

We also found an active recruiter offering to pay open-source intelligence (OSINT) researchers up to US$5,000 per identified bribable employee at named cryptocurrency platforms (including CoinTracker, ZenLedger, Binance, CoinStats, CoinMarketCap, and Robinhood), or alternatively a 15% share of the proceeds from any successful job sourced from that lead.

The recruiter claimed that a prior team focused on CoinStats had earned eight figures from the resulting access. The post illustrates a two-tier insider economy, in which intermediaries are paid to identify and pre-qualify employees who can then be approached with a bribe.

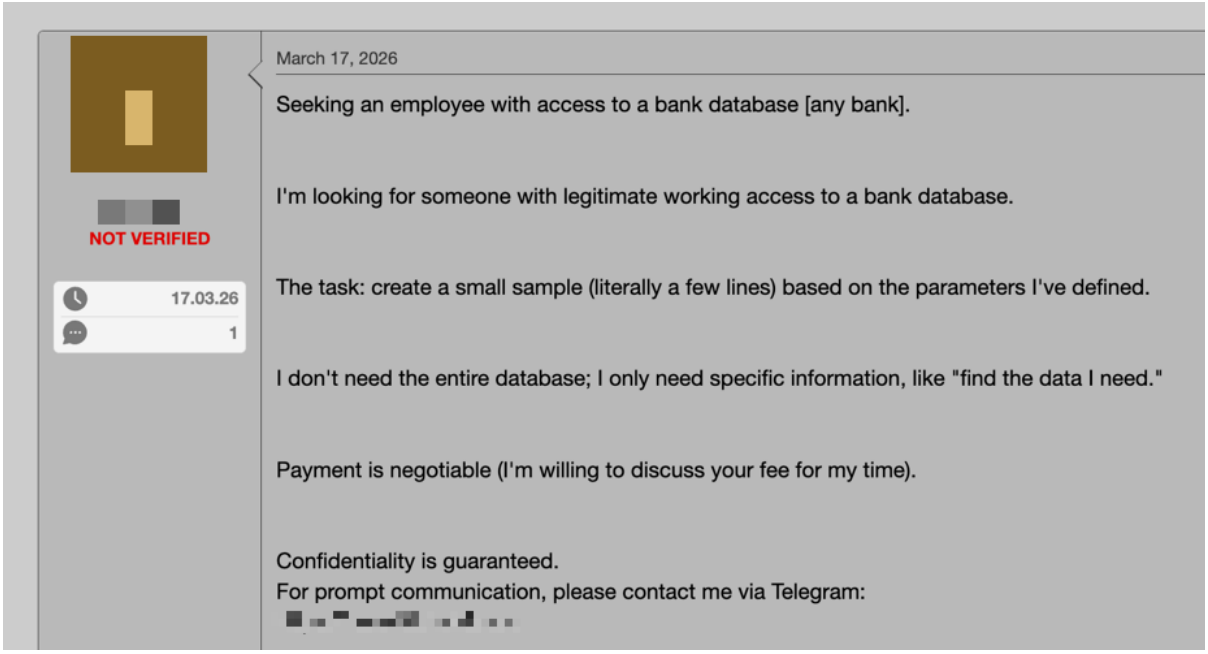


Figure 21. Post recruiting a banking insider with database access

The most detailed recruitment post we observed in the financial sector appeared on the Exploit forum and was directed at employees of European financial organizations.

The poster sought a long-term partnership with an employee who held access to an internal customer database or who interacted physically with customers at the branch or counter.

On the buyer's side, the post advertised custom private software, established phishing infrastructure, account takeover capabilities, and the operational ability to access cryptocurrency exchange accounts and withdraw funds. On the insider's side, the post described an interest in employees whose work routinely exposes them to customer data and who can extract that data securely, and it enumerated the specific roles of greatest interest.

At banks and neobanks, those roles included dedicated VIP account managers, fraud prevention specialists, database administrators, and IT staff with access to customer relationship management and support systems. At cryptocurrency exchanges, the post named verification, security, and customer support staff. At investment companies,

it named investor relations managers, analysts, and back-office staff. At fintech companies, it named specialists with access to full user profiles and transaction logs. The post explicitly stated that other positions could be considered as well.

Beyond data theft and payment approval, a distinct set of recruitment posts seeks insiders to help physically convert compromised funds into cash. We found a threat actor explicitly recruiting bank insiders to facilitate ATM fraud and promising high financial returns.

The actor is targeting specific high-tourism regions, including Australia, the Dominican Republic, Puerto Rico, the Middle East, New Zealand, Thailand, and small tourist island nations. These locations were likely chosen because of high foreign card usage, which maximizes skimming yield.

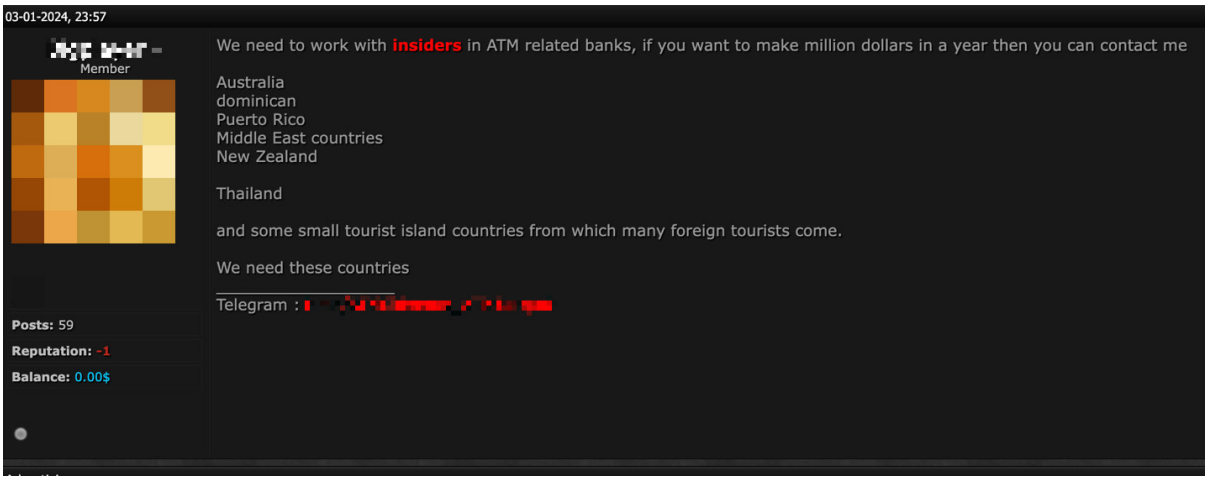


Figure 22. Forum post seeking insiders for specific tourist countries

Another example we saw was the recruitment of cashiers as possible money mules across Northern Virginia and Virginia Beach to perform “PIN jobs.” These mules were likely cashing out compromised card data at ATMs or point-of-sale terminals.

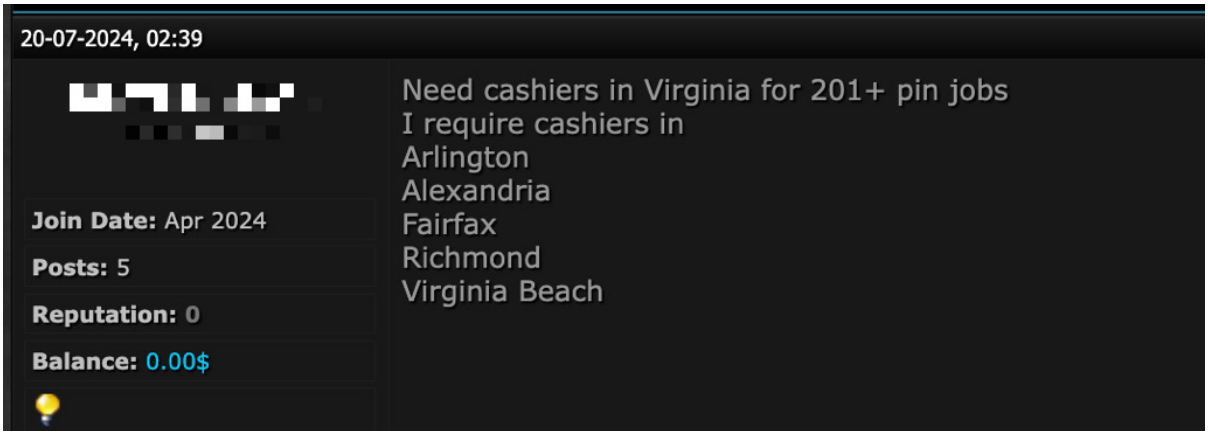


Figure 23. Forum post seeking cashiers for POS skimming

We saw several advertisements on the Dread forum seeking insiders at Bank of America, specifically a bank teller, branch employee, or loan officer who could provide account information and transaction history on a specific target.

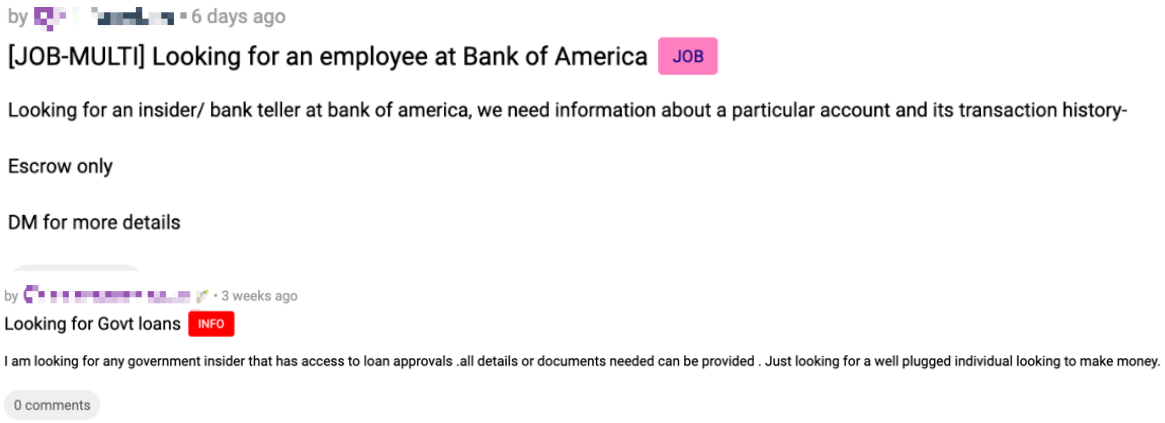


Figure 24. Forum post looking for an insider for bank loan approvals

We found a BEC insider service offering an insider in a specific finance function for sale rather than soliciting one. The seller advertised three years of insider access at a firm with reported revenues of US$25 million per year. The insider held an accounts receivable, accounts payable, and general finance role. The package also included the firm's corporate OneDrive contents, among them nondisclosure agreement data covering an automotive manufacturer client. Bidding opened at US$25,000 and was described as negotiable. The structure of the offer is characteristic of BEC preparation, in which the buyer is purchasing the insider knowledge a legitimate finance team would have—enough to author a convincing fraudulent payment instruction.

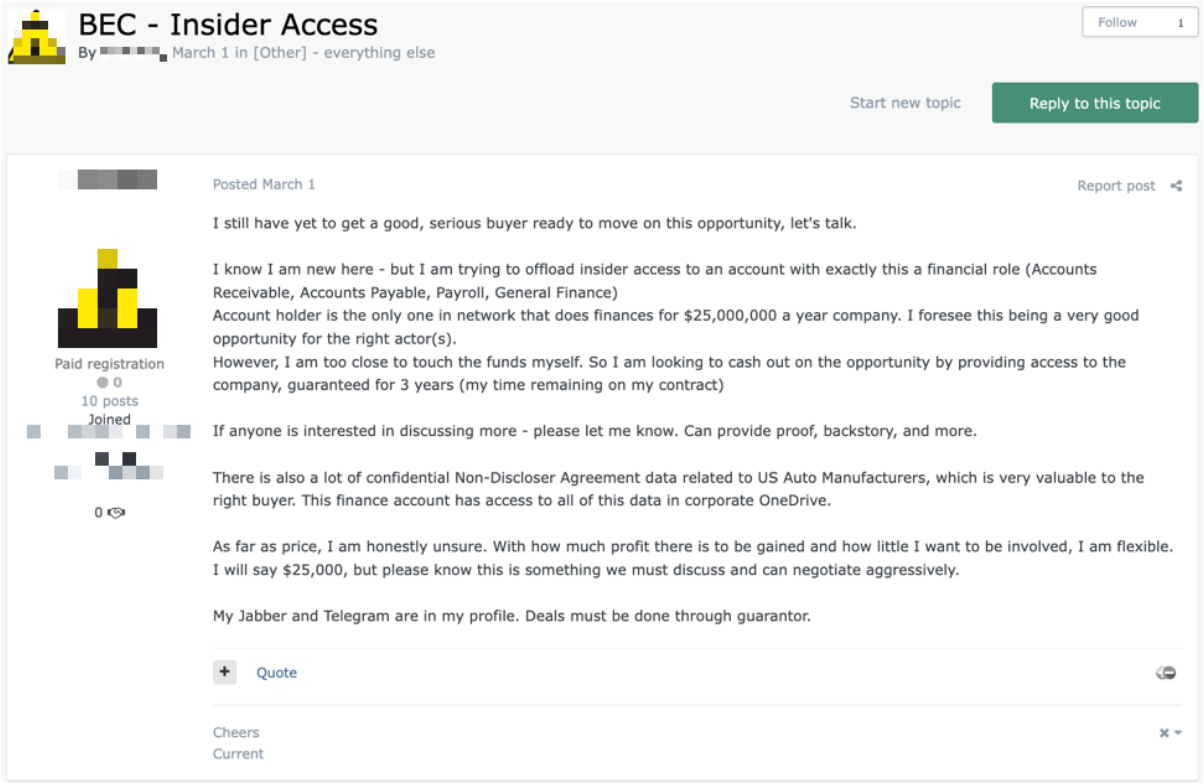


Figure 25. An insider offering their own finance-role access for sale

We found one listing, which was later banned, recruiting a person to finance a car with the help of an insider working at the dealership. In this fraud, a “striker” walks into a dealership posing as someone else using a synthetic identity. The striker is a person who physically conducts a fraudulent transaction on behalf of the organizer. The car is financed under the fraudulent identity and then typically sold quickly for cash, exported overseas, or used in further criminal activity.

In 2024, federal investigators broke up an organized fraud ring in Florida that used sophisticated synthetic identity fraud to exploit gaps in the lending system. Using fraudulent loan applications built on synthetic identities, the ring financed high-end vehicles—concentrating on luxury brands such as BMW and Mercedes—for a total exceeding US$10 million.[13]

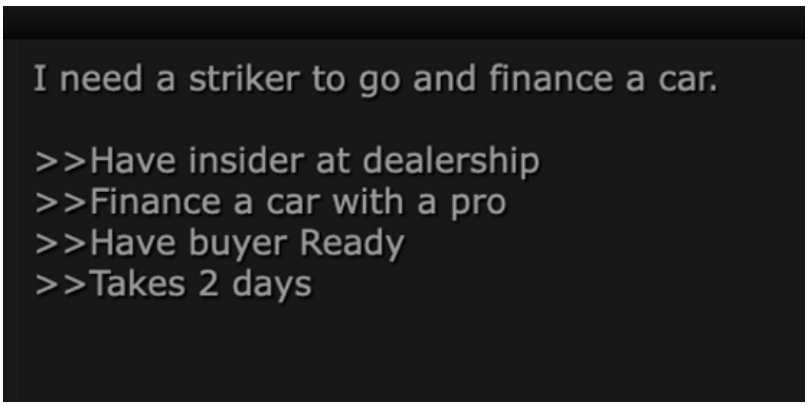


Figure 26. Post recruiting a striker for an auto-financing fraud scheme

9

Industrial and energy: Skimming at the pump

The industrial and energy sector is the least targeted by insiders. Where recruitment does occur, it is concentrated in turnkey payment-skimmer schemes. Threat actors hold the hardware and know-how, but they still need to recruit frontline gas station and store employees for the one thing they cannot manufacture: physical unsupervised access to the terminal.

Most insider activity in this sector has historically come from disgruntled employees or accounts that were never deactivated, rather than from recruited insiders working on behalf of external criminals. Even so, we found one recruitment model operating here, concentrated almost entirely on a single scheme: the installation of payment skimmers at gas stations and convenience stores.

As in the other industries mentioned so far, the offers include revenue-share partnerships, prebuilt skimmer hardware, written installation instructions, video walkthroughs, and remote data exfiltration tooling.

The barrier to entry for the insider is deliberately low, and the operation is packaged so that a cashier or attendant with a few minutes of unsupervised time at a register can deploy a working device.

The fuel retail and convenience store channel is a particularly attractive target for this model. Gas station forecourts and in-store payment terminals see high transaction volumes and are frequently operated by franchisees or independent owners with limited security staffing. Fuel pumps have also historically lagged behind major retailers in Europay, Mastercard, and Visa (EMV) chip adoption. A single compromised terminal at a busy station can yield thousands of usable card records before the skimmer is detected. Many of the advertisements listed model numbers of the skimmers available.

The insider threat at gas stations extends beyond payment terminals. The 2015 GasPot experiment by Trend Micro demonstrated that gas station automatic tank gauging (ATG) systems are a viable target. Building on that finding, an insider with the same unsupervised access used to install a POS skimmer could simultaneously manipulate the ATG system to underreport fuel volumes, running parallel financial and physical theft operations undetected.[14]

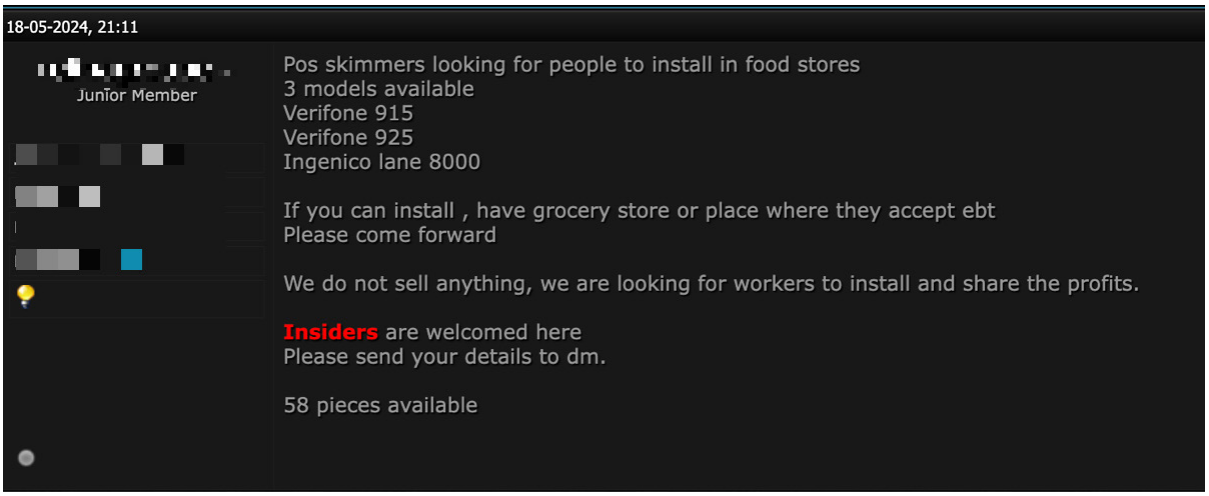


Figure 27. Forum post recruiting insiders to install POS skimmers at food stores

In one observed thread, an actor was soliciting insiders to install POS skimmers. A respondent volunteered that his girlfriend worked at a grocery chain location in Pennsylvania with 10 checkout lanes, framing her position as a viable installation site.

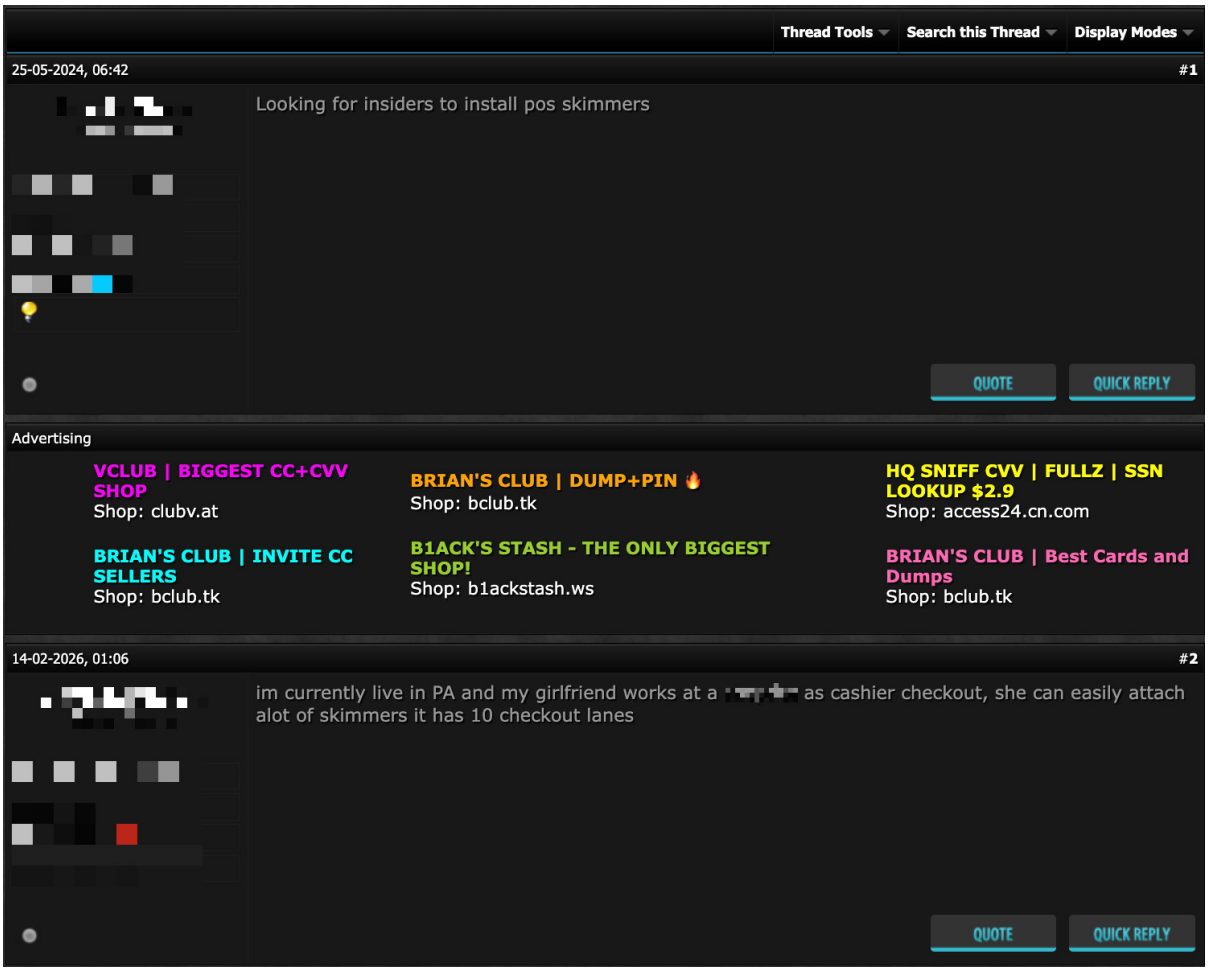


Figure 28. Response to a POS skimmer recruitment ad, volunteering an insider at a grocery store

Another post from October 2025 illustrates how the insider installer market is expanding beyond commodity magstripe theft. An actor advertised a worldwide search for reliable installers of both ATM and POS skimmers. The actor offered overlay and insert hardware, claimed to provide a PIN bypass and an EMV relay capability for Android devices, and further claimed a method for completing unauthorized EMV transactions at the card's own issuing bank's ATMs. Commercial terms included a 15% revenue share paid to the actor, drawn at random from the skimmed dataset rather than selected from preferred bank identification ranges, with a down payment held in escrow before tooling is released.

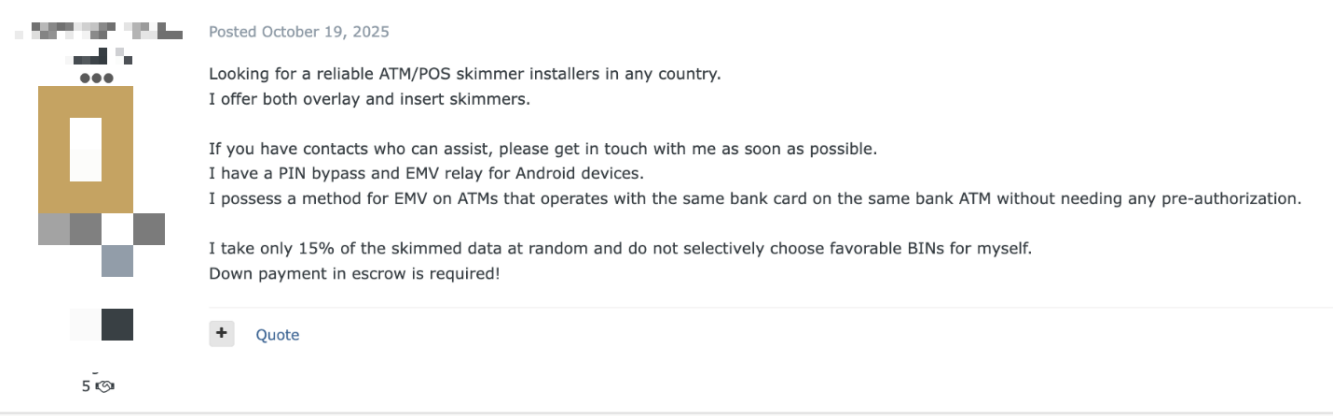


Figure 29. A post looking for insiders to install skimmers

In May 2025, we found an actor who sought a collaborator to help execute the next phase of an intrusion against a major industrial corporation in the oil, gas, and chemicals sector, claiming that internal access had already been secured through a trusted contact. The actor described insider access as already in hand, a strategic plan as already in place, and the open requirement as a technically capable partner to monetize or weaponize that access. That framing is consistent with the early stages of an extortion, data theft, or operational-disruption campaign rather than payment card fraud. It indicates that the same insider recruitment model used at the retail tier is being applied, with greater operational maturity, against enterprise targets in the vertical.

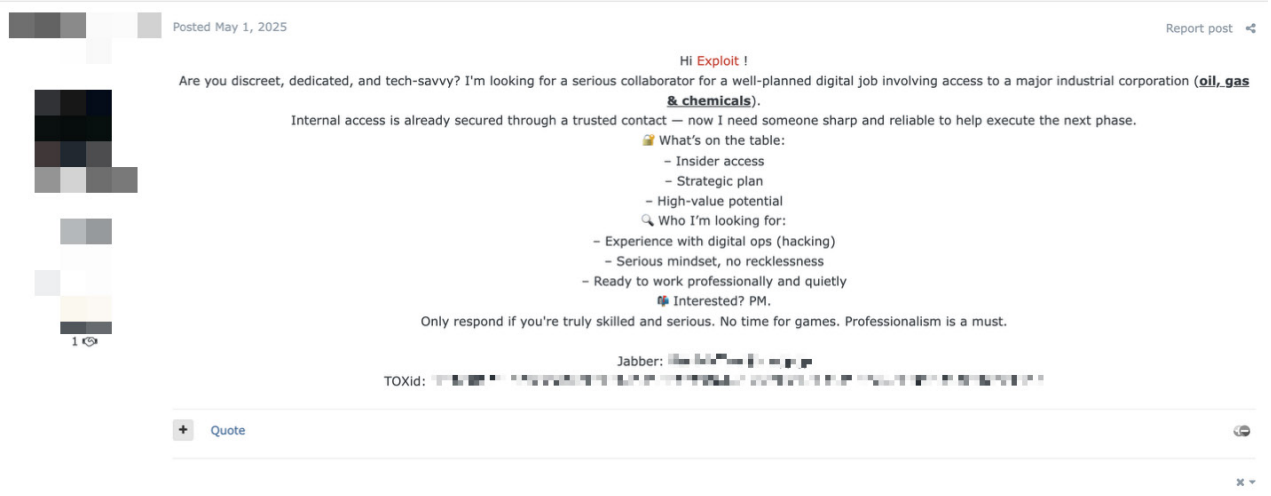


Figure 30. Post looking for insiders at oil, gas, and chemical companies

The advertisement reinforces a finding consistent across this section, which is that underground actors are actively packaging insider-enabled card fraud as a turnkey product. They are willing to invest in escrow mechanics, training material, and revenue-share structures to recruit and retain the frontline employees who make the scheme possible.

The scale of this problem is now significant enough that in 2025 the U.S. Secret Service ran 22 nationwide operations against card skimming, inspecting nearly 60,000 terminals, gas pumps, and ATMs and removing 411 devices. This underscores that card skimming operates at a national scale, consistent with the insider-enabled market documented here.[15]

10

Shipping and logistics: Tracking numbers for hire

In shipping fraud, the insider's entire value comes down to control of a single data point: the tracking scan that marketplaces, sellers, and buyers all treat as ground truth. A logistics insider who can post a false "Delivered" scan releases a fraudulent payout, and one who can post a "Return to sender" scan reverses a legitimate sale. That leverage is why carrier insiders command steady, recurring demand.

Cybercriminal forums show consistent underground demand for insiders at shipping and logistics companies, most often running fraudulent tracking scans. Documented cases involve employees who operate theft rings against high-value shipments, who draw on routing system knowledge to identify and intercept valuable packages, and who sell shipment tracking data or reroute access to outside buyers.

One post offered US$1,000 per day to a FedEx employee with admin panel access who could upload tracking number data through the internal software; the poster indicated flexibility on different access tiers.

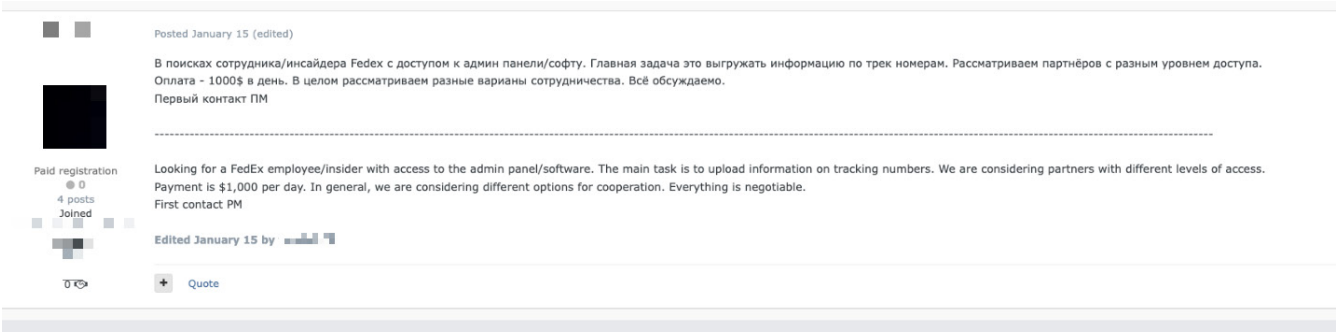


Figure 31. Post offering to pay a FedEx insider for tracking uploads

The same recruitment pattern extends to adjacent sectors that touch the logistics chain. A top-tier (“GOD” ranked) actor on a separate forum posted buyer demand for a Dell insider who could resolve order serial numbers and customer or company names from a service tag. The starting price was US$2,000 or best offer. That kind of lookup capability is valuable to fraudsters who want to impersonate shippers or intercept hardware in transit.

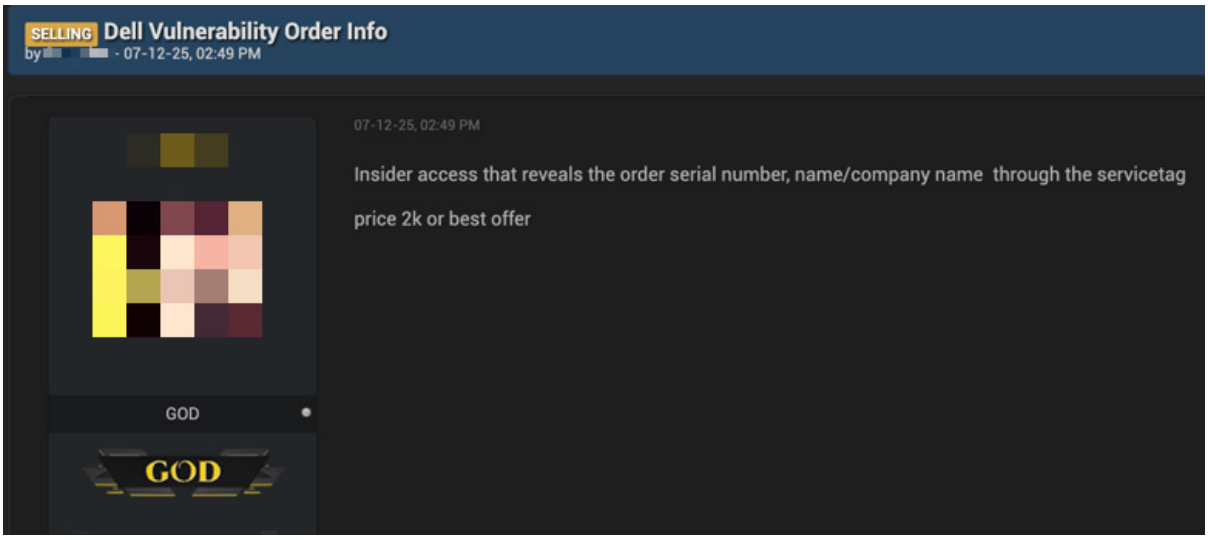


Figure 32. Forum post seeking a Dell insider with order and service tag lookup access

Recruiters also target the telecom backbone that the logistics industry runs on. One actor offered “fairly great” pay to any insider at a Session Initiation Protocol (SIP) trunking provider and added a finder’s fee for anyone who introduced one.

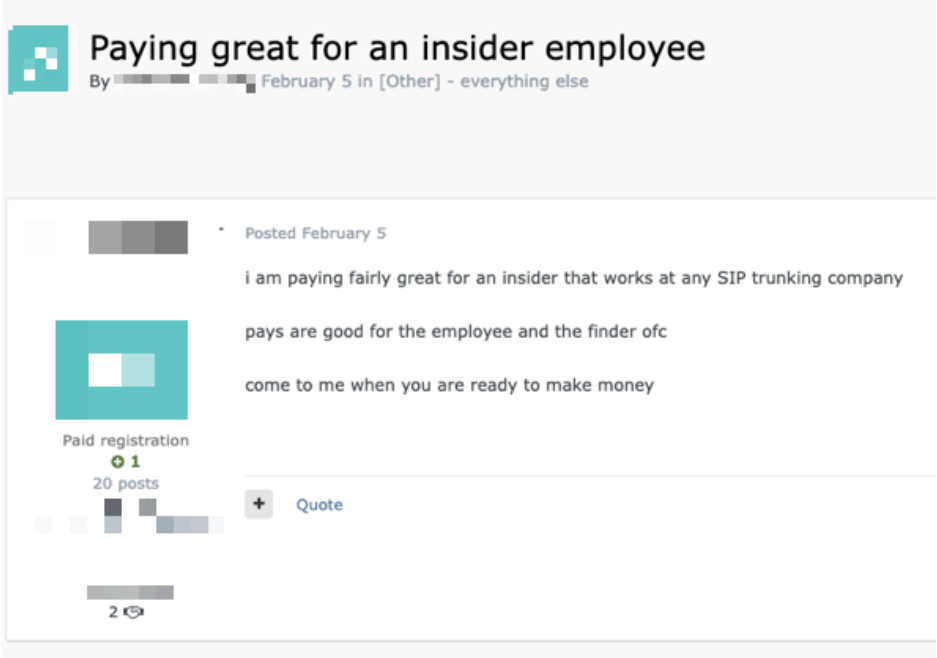


Figure 33. Recruitment post for an insider at a SIP trunking provider

A “Gold Member” buyer on a separate forum posted an open call for UPS insiders willing to run package tracking scans on Saturdays. They offered to purchase in volume and agreed to use a forum guarantor to escrow the deal.

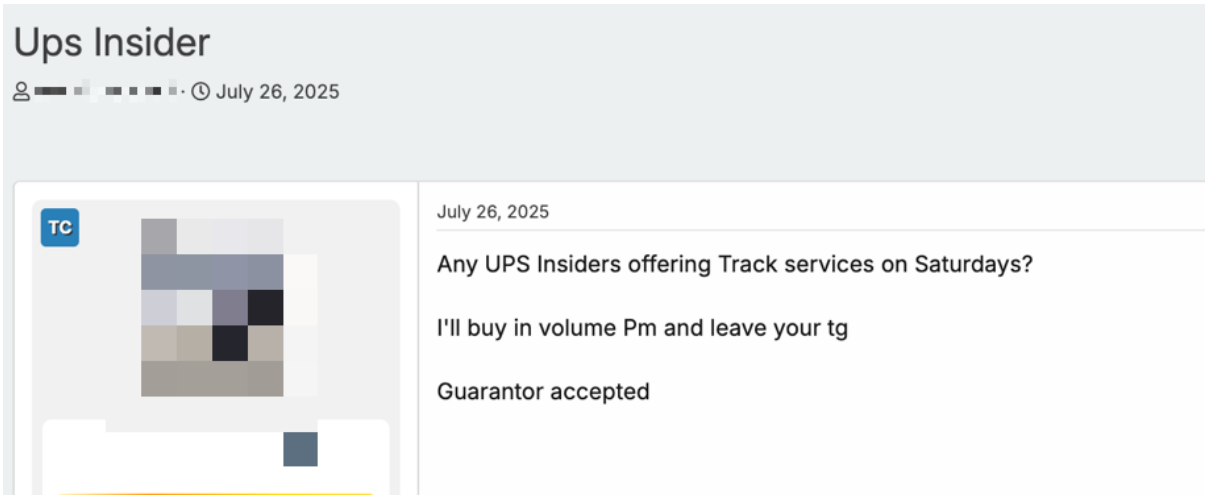


Figure 34. Post seeking a UPS insider

Tracking system access lets fraudsters generate fake "Delivered" scans that release seller payouts, reroute or stall in-transit shipments, and confirm bogus proof of delivery for stolen goods. That utility is why insider access at major carriers such as UPS draws recurring, high-volume demand on these forums.

Shipping offerings are not limited to North American regions. We found posts advertising insider access to DPD and SEUR shipping company accounts. SEUR is Spain's leading express transport company and part of the Geopost network (formerly DPDgroup), which also operates the DPD brand. Together, they provide domestic and cross-border shipping across Spain, Portugal, and over 230 countries and territories.[16] One post described allowing buyers to manipulate parcel tracking statuses an unlimited number of times for any tracking number, with return to sender scans also available.

Table 4 summarizes some of our findings on shipping fraud service prices.

Shipping carrier	Service offered	Average starting price
UPS	Delivered	From $150
UPS	Return to sender	From $100
UPS	Lost in transit	From $75
UPS	Damaged	From $100
Chronopost/DPD	Return to sender	From $50
Chronopost/DPD	Lost in transit	From $120
Colissimo	Lost	From $100
Colissimo	Return to sender	From $100
Colissimo	Delivered to shipper	From $100
FedEx	Delivered	From $100
USPS	Return to sender	From $100
USPS	Lost in transit	From $100
USPS	Damage	From $100
DHL	Return to sender	From $30
DHL	Lost in transit	From $50
DHL	Damage	From $50

Table 4. Average prices for shipping fraud services in U.S. dollars

Two teenagers employed at a UPS Store in Hialeah, Florida, carried out a theft scheme that ran from late March to mid-April 2026 targeting a husband-and-wife Amazon reseller. When the couple dropped off roughly 10 boxes of Bath & Body Works and Victoria's Secret merchandise, the UPS employees would scan only half of the packages into the UPS shipping system. The unscanned boxes were then carried out through the rear door while a lookout watched. One defendant later listed the stolen goods on Facebook Marketplace for as little as US$1 each. The scheme resulted in roughly US$40,000 in losses across approximately 80 boxes between March and April. A third suspect was also charged with disabling the store's surveillance system. The deliberate failure to scan packages is a textbook insider tracking-abuse scheme.[17]

These cases show what draws fraudsters to shipping and logistics. As in other industries, the trends seen in the underground follow the path of money, and in shipping, whoever controls the scan controls the money, which is why demand for carrier insiders stays consistent across these forums.

11

Retail: Refunds without limits

Retail insiders power a matured refunding economy in which brokers with fixed price lists recruit employees inside major chains to issue refunds while the customer keeps the merchandise. These schemes turn a once-hobbyist scam into an organized service with named operators, recurring relationships, and no caps on order value.

Underground threat actors target insiders at retail stores primarily to walk away with goods or cash for free. The dominant scheme is refunding fraud, often shortened to refunding, in which an actor claims an undeserved refund on a product the buyer keeps. Forum advertisements show refunding has matured from a hobbyist scam into an organized service.

A “refunder” is a professional fraud service that exploits retailer return and customer service policies to obtain cash or merchandise. The model is straightforward. A shopper buys a real product online from a major retailer, sends the order details to the refunding group. The group then poses as the customer, social-engineering the retailer’s support team into issuing a refund while the shopper keeps the item. The refunding group typically charges between 15% and 35% of the refund value as its cut, usually paid in PayPal or bitcoin once the retailer credits the customer.

Many threat actors state plainly that they are looking for insiders to run refund scams, with listings revealing both the breadth of retailers being targeted and the maturity of the brokering market.

We documented an insider running refunds on Best Buy orders less than 90 days old with no amount or item limit, charging a 28% fee with a US$300 minimum. We also found multiple listings for Costco insider-run refunds.

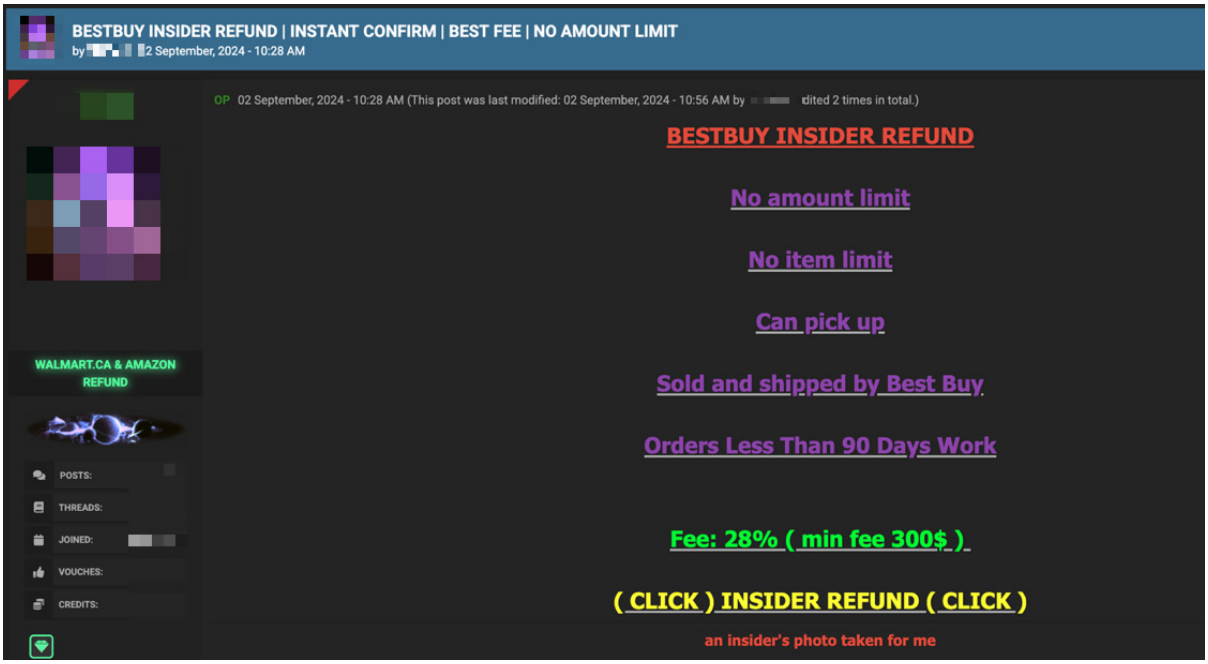


Figure 35. Best Buy insider refunding service

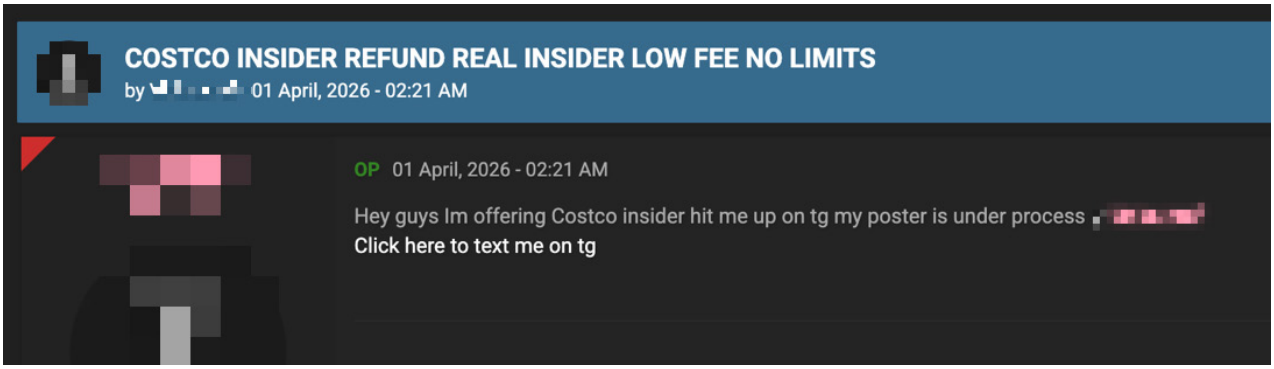


Figure 36. Post offering Costco insider services

In a listing from January 2026, the recruiter claims three years of experience. They say they have worked with more than 20 insiders, including a Home Depot employee through whom they claim to have processed over US$500,000 in refunds over a few months. They offer two engagement models: a flat per-refund fee and a middleman cut on every job.

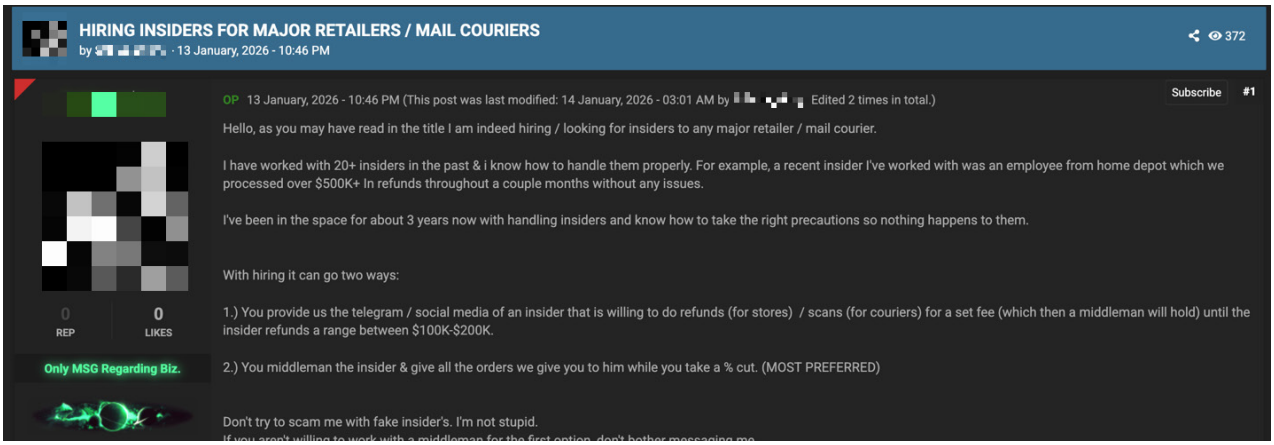


Figure 37. A post recruiting insiders at major retail stores

We identified advertisements for Nike insiders. The actor promises an insider with no caps on order total or item count with an instant turnaround, and support for reshipping. The advertisement goes further, describing the service as “safe” and free of rebills and claiming it works on freshly created accounts. Orders can reportedly be placed both after delivery and while still in transit, for a 35.5% fee on U.S. orders only

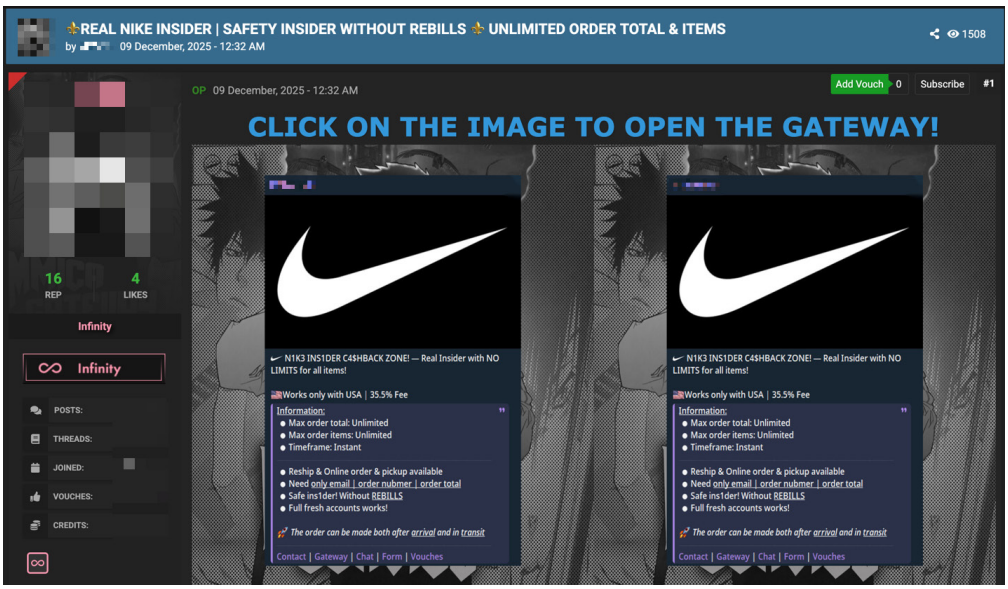


Figure 38. Nike insiders offering uncapped refund and order fraud services

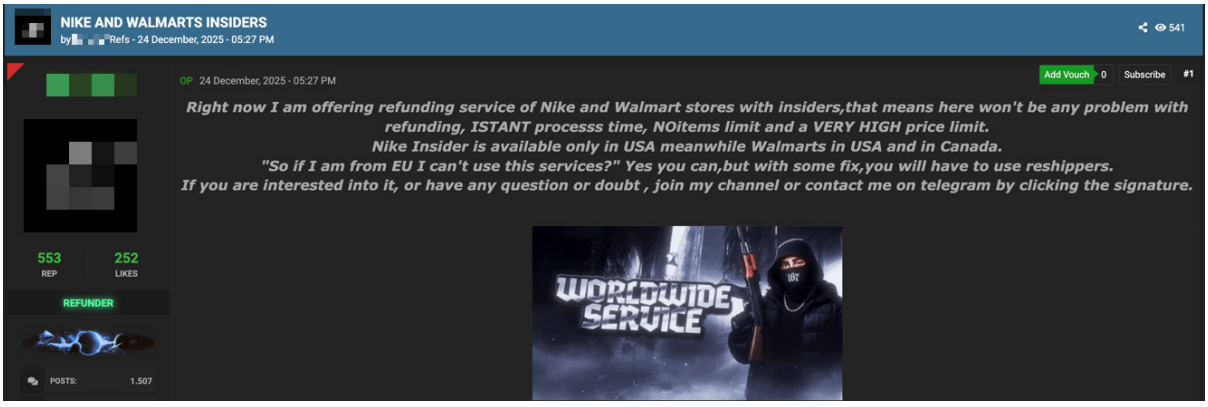


Figure 39. Post offering Nike and Walmart insider refunding services

Enforcement actions have begun to reach the organized end of this market. In 2026, members of a Telegram-based refund-fraud organization were sentenced in federal court for a scheme that ran from July 2020 to July 2022 and at one point drew more than 5,900 followers. The organization charged customers a percentage of a product's price and obtained or attempted to obtain refunds for millions of dollars in goods, including electronics, designer apparel, home furnishings, and appliances.[18]

The methods this organization used map directly onto the listings documented in this section: social-engineering retailer support representatives, manipulating shipping labels to make returned products appear received, and recruiting company insiders to process fraudulent refunds. The group also developed malware to circumvent retailer fraud-prevention systems. Several members received prison terms ranging from time served to 21 months. The sentences show that the insider-enabled refunding economy advertised on these forums has produced real prosecutions, even as new services replace the ones shut down.

12

Reviews and reputations: Five stars on demand

On a reputation platform, the rating is the product. An insider who can delete a negative review, reinstate a banned host, or inflate a score is selling the platform's credibility itself. That is a uniquely damaging asset: unlike a one-time theft of money or data, it corrodes the trust signal every other user relies on.

Airbnb is a case in point. A global online marketplace for short-term and long-term homestays, it connects property owners with travelers looking for alternatives to traditional hotels. It runs almost entirely on the trust signal of guest reviews and host ratings, which makes the insiders who can edit that signal a target for buyers. Airbnb scams take on several forms.

The most common is the phantom listing scam, in which a scammer constructs a fraudulent but convincing listing, collects payment from unsuspecting guests, and leaves them to discover upon arrival that the property does not exist. Another documented scheme involves hosts purchasing fabricated five-star reviews from third-party services to boost their listing rankings and attract more bookings. These services have been observed operating openly on underground forums and Telegram channels. In the context of insider threats, individuals have been found paying platform insiders to remove negative reviews, reinstate banned accounts, and artificially inflate ratings.

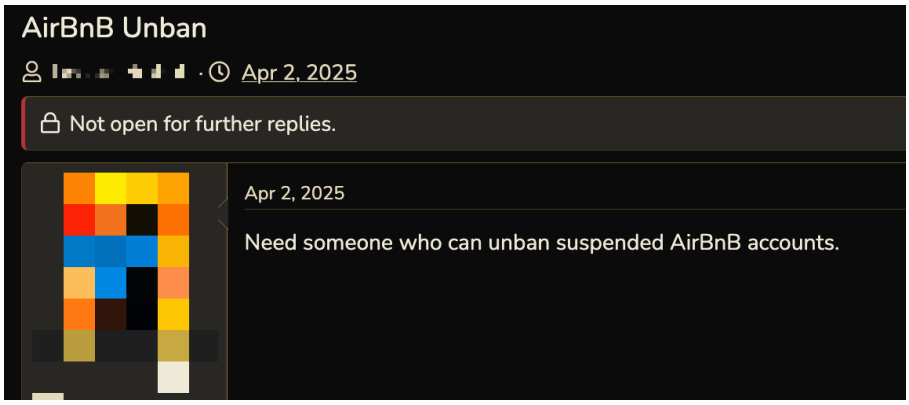


Figure 40. A buyer looking to purchase Airbnb unban services

Airbnb maintains policies and enforcement mechanisms to address fraudulent reviews, though a significant number continue to evade detection. The platform has publicly acknowledged the problem and continues to invest in detection technology. Enforcement measures include algorithmic monitoring that flags suspicious review patterns such as sudden surges in five-star ratings, multiple reviews originating from the same device or IP address, and reviews posted by accounts with no prior booking history. Account-level consequences for violations can include removal of fraudulent reviews, temporary suspension, or permanent removal from the platform in cases of repeated or severe misconduct.

We saw multiple listings for Airbnb unbans, with prices starting at US$30. Other buyers advertised that they were looking for an insider to remove negative reviews and were willing to pay up to US$100 for each review taken down. Several listings came from hosts with multiple rentals who wanted to purchase the service in bulk, paying a flat rate per listing cleaned.

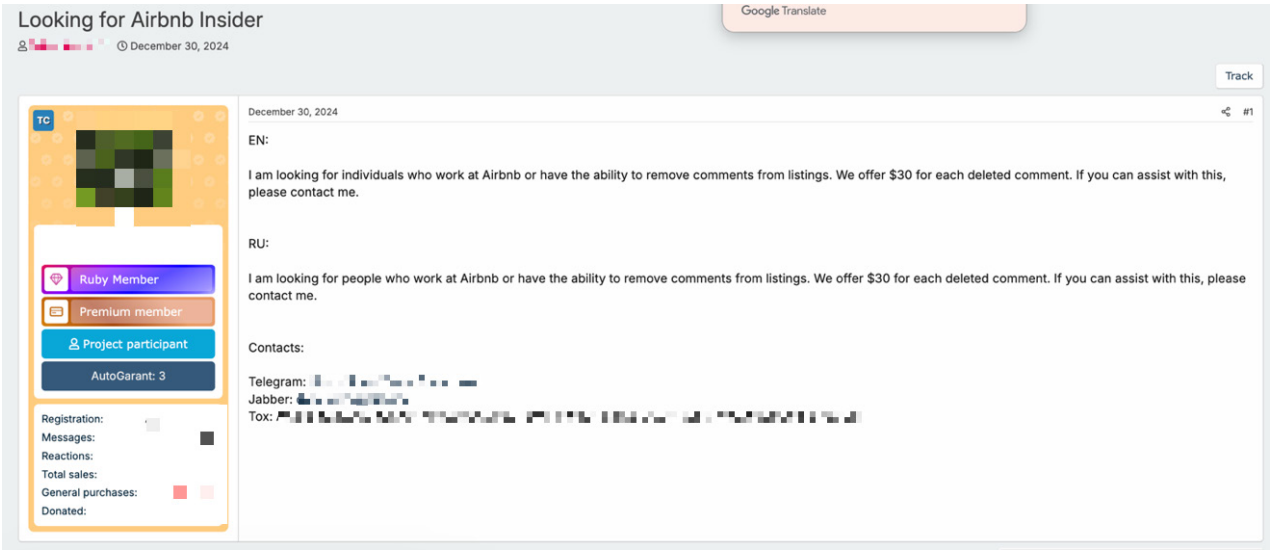


Figure 41. A buyer looking for Airbnb bad review removal

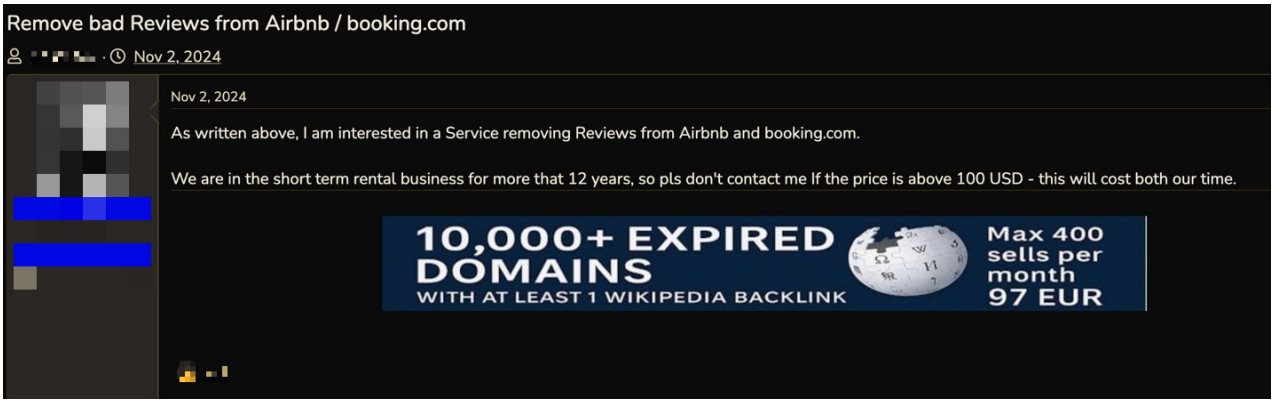


Figure 42. A buyer looking to purchase bulk negative review removal

Regulators have begun to treat this manipulation as an enforceable harm rather than a nuisance. In 2024, the Federal Trade Commission (FTC) issued its Rule on the Use of Consumer Reviews and Testimonials, effective October 21, 2024, which prohibits the sale and purchase of fake reviews and authorizes civil penalties of up to US$53,088 per violation (as of the inflation-adjusted civil penalty amounts for 2025).[19, 20] The rule reaches the exact conduct documented here, because it specifically covers insiders who create reviews without disclosing their relationship to the business and practices that suppress genuine negative reviews.

What sets this market apart from the others in this report is the nature of the assets being sold. A stolen record or a fraudulent refund takes money or data out of a system once. What an insider sells here is the platform's credibility, and on a marketplace where the rating is the only thing standing between a guest and a stranger's home, that credibility is the whole product.

13

Building the inside job

Insider recruitment has professionalized into a structured labor market. Forum recruiters frame the work as low risk and high reward, vet for high-value access over bulk volume, and use sign-on bonuses and finder's fees to turn employees into recruiters of their own colleagues. Meanwhile, a maturing supply chain increasingly splits sourcing, bribery, and payout across specialists.

Underground forums host a steady stream of posts recruiting employees across many industries to feed cybercriminal gangs, ransomware groups, and fraud rings. Postings target staff at crypto exchanges, cellular carriers, banks, law enforcement, government agencies, and even hiring platforms, with payouts ranging from a few thousand dollars per lookup to ongoing salaried partnerships.

A representative example comes from an actor who posted under the headline "Exchange insiders, Don't get burned from amateur gangs, we pay the highest and offer the best security." The pitch is aimed squarely at insiders already working with rival crews, urging them to defect on the promise of better pay and tighter operational security. To close the deal, the actor advertises a US$25,000 sign-on bonus for any insider who comes aboard and a matching US$25,000 finder's fee for referring another colleague with similar access. Interested parties are then routed to a Telegram handle for private negotiation.

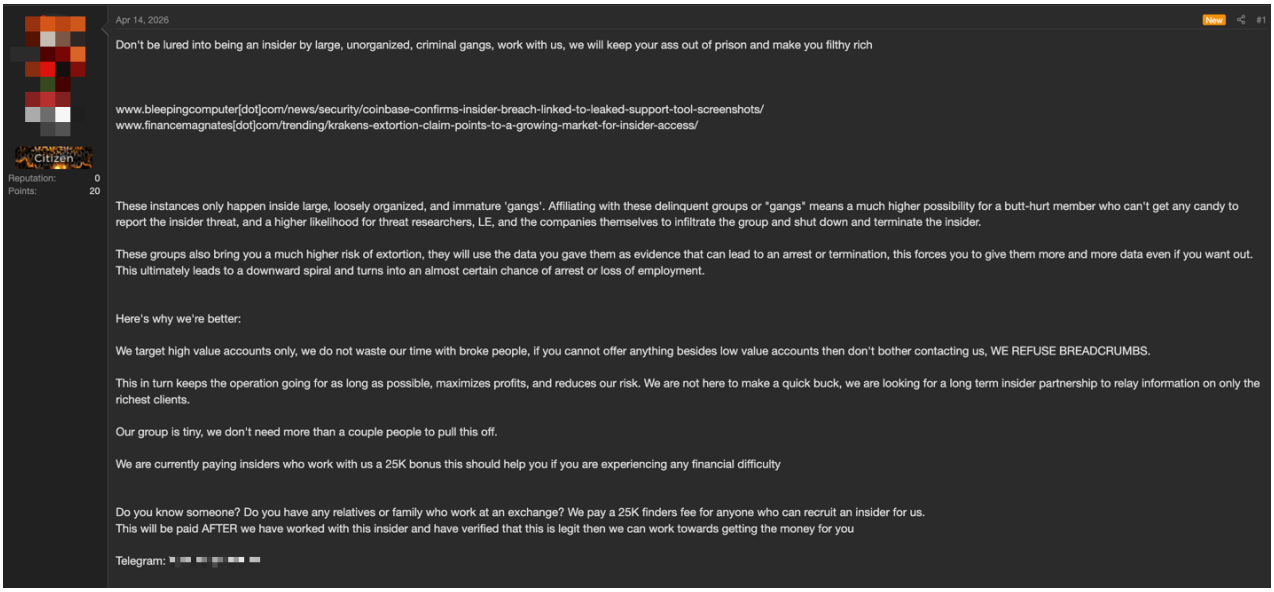


Figure 43. Recruitment post offering a US$25,000 sign-on bonus and a matching finder's fee to crypto exchange insiders

The listing is a textbook example of how recruitment on these forums blends competitive job market language with organized crime tradecraft, treating insider access as a recurring revenue stream worth poaching from competitors.

Where the actor targets insiders directly, other recruiters work one layer removed, paying skilled operators to find and bribe employees on their behalf. An actor posting in a Social Engineering subforum under the headline "NEW WORK RECRUITMENT" solicits operators skilled in open-source intelligence (OSINT). Their task is to scrape and hand-pick employees at crypto tax and exchange platforms—including CoinTracker, ZenLedger, Binance, CoinStats, CoinMarketCap, and Robinhood—then bribe them for

user information. The listing offers up to US$5,000 per employee delivered or a 15% cut of each completed job. Targets must be located in lower-wage regions to maximize bribery success. The structure shows a maturing supply chain in which sourcing, bribery, and payout are split across specialists rather than handled by a single actor.

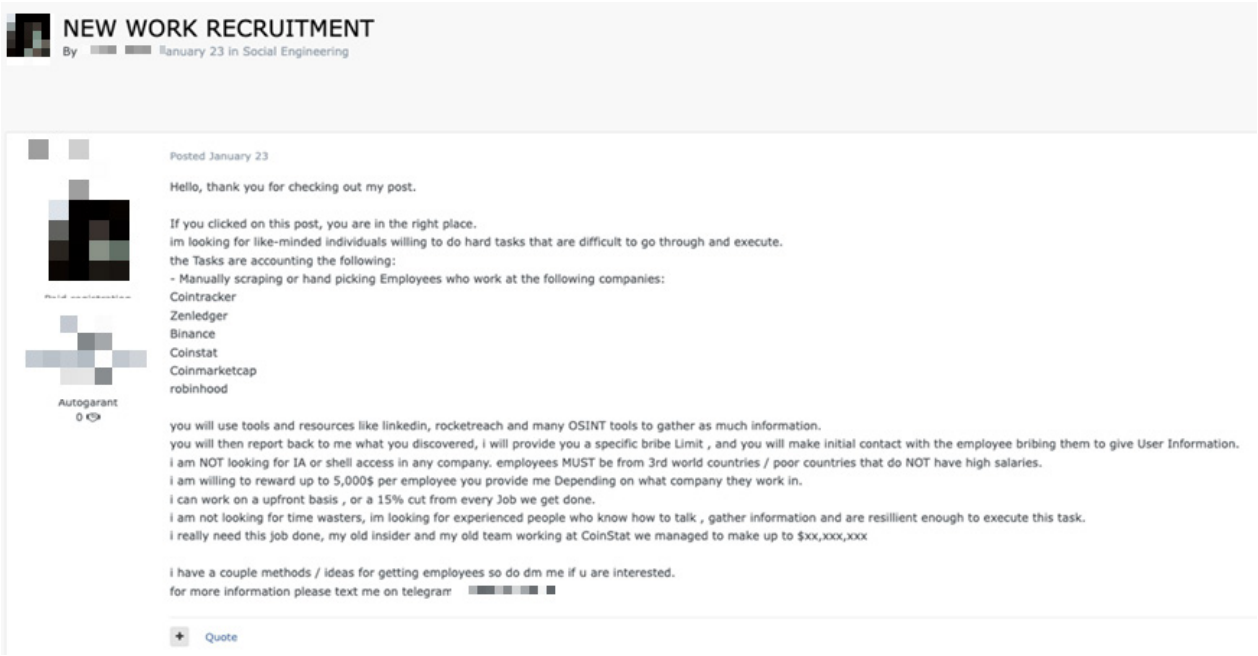


Figure 44. Recruiting OSINT operators to bribe employees at crypto tax and exchange platforms

Beyond the crypto and hiring platform niches, recruitment broadens into nearly every sector of public and private life. A listing titled “Looking for employees from different fields Globally” names cellular communications, banking, law enforcement, and government agencies as desired targets. Pay and hours are negotiated privately over qTox, and the listing routes through the forum guarantor service to escrow the deal between recruiter and insider.

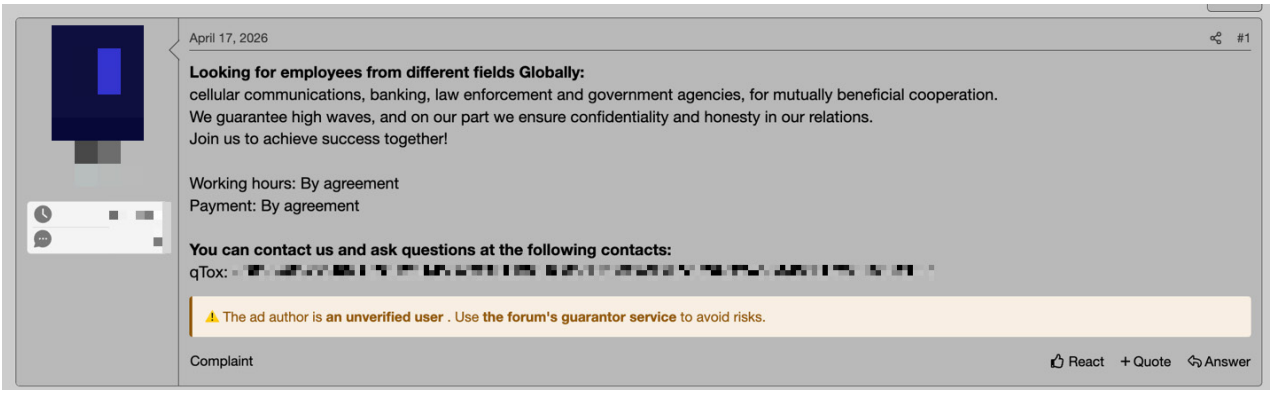


Figure 45. Cross-sector recruitment listing seeking insiders at telecom carriers, banks, law enforcement, and government agencies

The same recruiter logic extends in the opposite direction. Rather than buying access to a target company's employees, some actors buy access to the hiring platforms themselves so they can pose as legitimate employers. We found a post targeting sites that include CareerBuilder, Indeed, Monster, ZipRecruiter, and Craigslist. Compromised employer accounts let buyers post fake job listings, entice people to become insiders, harvest applicant resumes for identity fraud, and run recruitment lures. These funnel candidates into mule and money-laundering schemes.

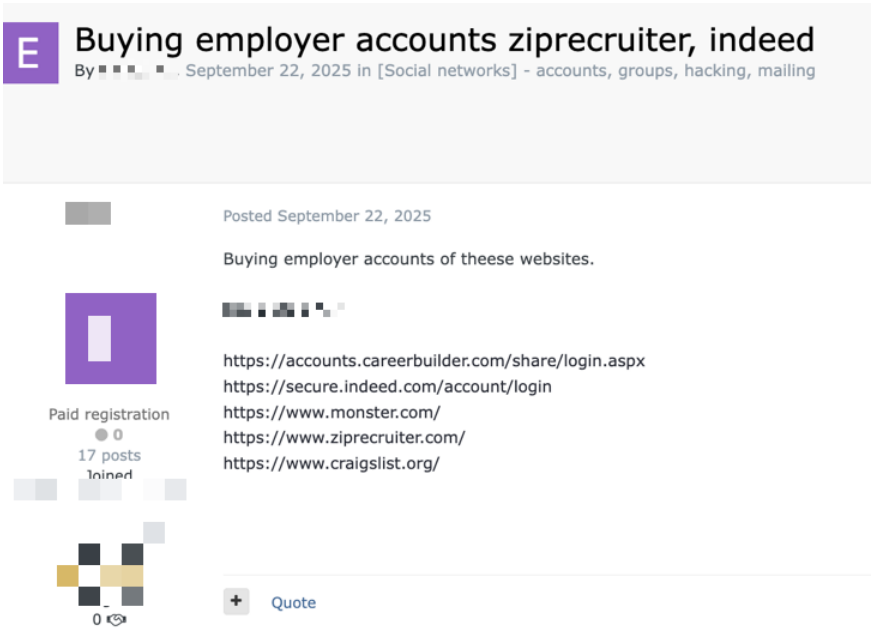


Figure 46. Post buying compromised employer accounts on major employment sites

A parallel listing under the headline "Indeed Employer account" asks for accounts in Latin America, Asia, and possibly Europe at prices starting from one dollar. The low entry price and broad geography signal commodity-level demand for hijacked recruiter accounts that fuel large-volume candidate phishing. It also confirms that the supply of stolen employer credentials is deep enough to support both bulk buyers and one-off operators.

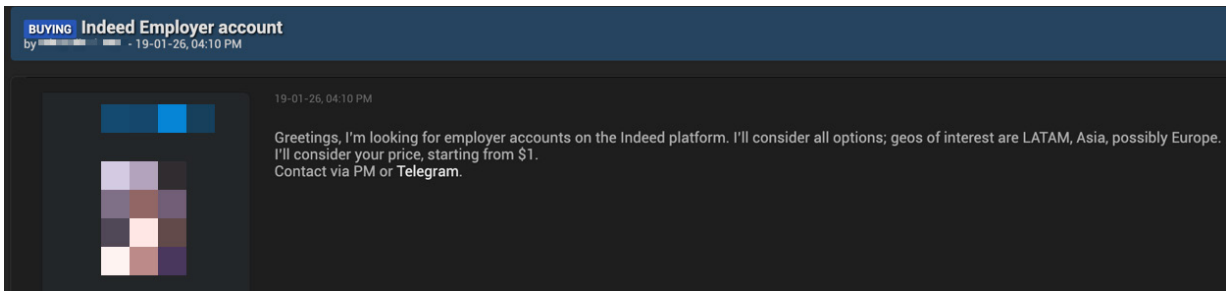


Figure 47. Buyer side post seeking Indeed employer accounts at prices starting from one dollar

These listings show a recruitment market that already spans every layer of the modern enterprise. Crypto exchanges and crypto tax platforms attract the highest bounties because account access converts directly to stolen funds. Hiring platforms and recruiter accounts feed candidates targeting pipelines for identity fraud and BEC. Telecom, banking, and government-agency staff are prized for the lookups, SIM swaps, and law-enforcement spoofing they enable. Across all these niches, recruiters lean on the same playbook of bonuses, finder's fees, and forum guarantors. That is why insider risk should be treated as a continuous, well-funded market rather than a series of isolated incidents.

The clearest illustration is that known ransomware groups now run their own open-insider programs, advertising the same kinds of payouts in branded recruiting banners aimed at employees.

A prominent extortion and data-theft group, Lapsus$, has resurfaced and is once again advertising for insiders—this time actively seeking employees from major telecom, technology, and AI organizations.[21]

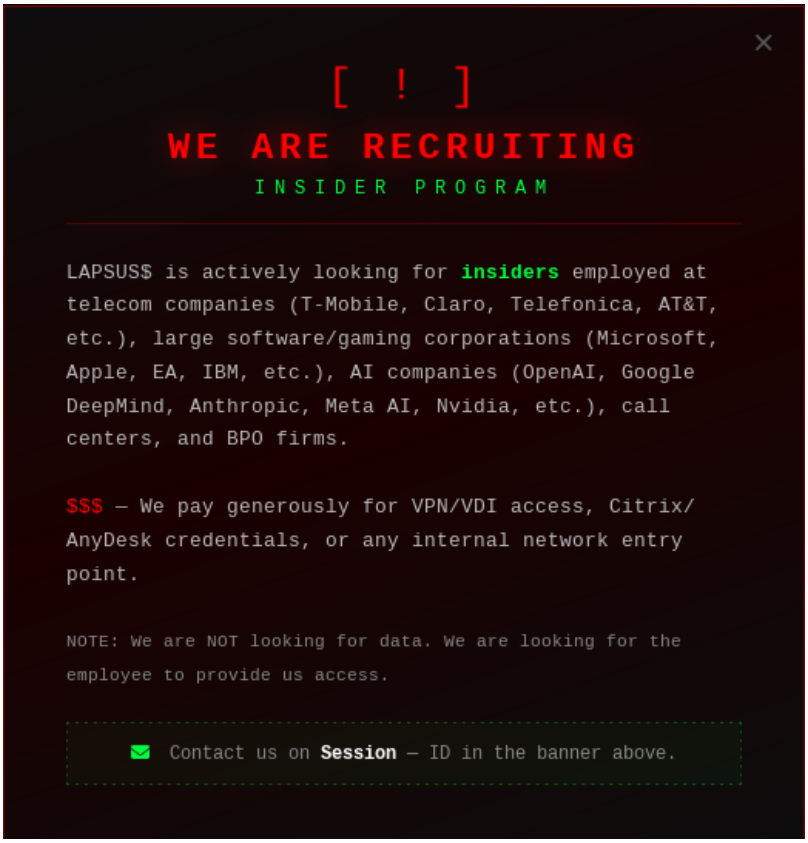


Figure 48. Insider program run by Lapsus$, a prominent extortion group

14

Conclusion

Insider risk is a business risk, not just a cyber risk. Our research suggests that insider abuse is evolving from isolated opportunism into a structured criminal market that strikes at the trust organizations depend on to operate.

The market has matured and has become part of a larger, more organized cybercriminal ecosystem. The insider is no longer acting alone, but is a link in a broader criminal supply chain. Services enabled by insiders are becoming scalable and partially commoditized, complete with fixed pricing, turnaround expectations, reseller programs, and recurring partnerships. These traits show how the insider market increasingly resembles other mature underground economies.



Authority over network access

Beyond the transformation of the insider market itself, the activity we have documented is also indicative of what cybercriminals currently value. The underground is increasingly seeking workflow authority rather than raw network access. The most valuable insiders are often not those with the most privileges, but those positioned strategically inside trusted operational processes. These are employees who can approve transactions, restore accounts, bypass fraud controls, manipulate tracking systems, access customer data, or authorize actions. These are moves that external attackers would struggle to perform convincingly from outside the organization.

Insiders in the era of AI

As cybercriminal operations evolve toward greater specialization and efficiency, insider access is likely to become more deeply embedded in schemes ranging from ransomware to BEC campaigns. The underground acknowledges the value of trusted human access. The most efficient way into an organization is not through the perimeter, but through the employee already trusted to operate inside it.

This role is not likely to change in the age of AI. The rapid growth of the AI sector is likely to make AI companies an attractive target for insider recruitment. As these organizations accumulate valuable model weights, proprietary training data, customer information, and privileged access to powerful internal systems, the demand for employees who can quietly extract that data or abuse their access is expected to rise. The same market dynamics run throughout this research: recruiters seek high-value access, and buyers pay a premium for trusted insiders. Those dynamics position the AI industry as a probable focus for future insider activity.Recommendations

15

Recommendations

If there is one practical takeaway from our findings, it is that insider risk should not be treated as an occasional HR matter or a perimeter-security afterthought. The underground market is built to exploit exactly the trusted access that traditional controls assume is safe.

We have listed recommendations to help frame defenses around this reality. They focus less on keeping outsiders out and more on limiting what any single trusted individual can do unobserved. They also focus on preparing employees for the possibility that a recruiter will approach them.

Monitor workflow exceptions as security events



Insider-enabled abuse frequently occurs through legitimate business processes rather than technical compromise.

Organizations should:

- Monitor account recoveries, manual overrides, and exception handling.
- Alert on unusual volumes or timing of manual approvals.
- Correlate workflow actions with downstream fraud outcomes.
- Review repeat use of administrative exception mechanisms.

Reduce single-person authority

Many of the underground services observed relied on one employee being able to complete an action without oversight.

Organizations should:

- Require dual approval for high-risk transactions.
- Separate duties for approval and execution.
- Introduce secondary validation for sensitive customer actions.
- Periodically review employees with unilateral authority.

Treat operational tooling as security-critical infrastructure

Customer-service platforms increasingly have the same abuse value as privileged administrative systems.

Organizations should:

- Audit access to account-recovery systems.
- Review permissions for moderation tools and fraud-review dashboards.
- Log sensitive actions performed through operational consoles.
- Conduct periodic entitlement reviews.

Assume employees are targets

Employees should be viewed not only as potential insider threats, but as targets of insider recruitment.

Organizations should:

- Include bribery and recruitment attempts in awareness programs.
- Establish reporting channels for suspicious approaches.
- Provide guidance on handling extortion or coercion attempts.
- Focus awareness efforts on high-value operational roles.

Integrate fraud and cybersecurity teams

Many insider-enabled attacks sit between traditional organizational silos.

Organizations should:

- Share telemetry between fraud and security functions.
- Jointly investigate suspicious workflow activity.
- Develop common playbooks.
- Include business units in insider-risk exercises.

Exercise caution when validating insider-enabled services

Organizations may be tempted to validate underground claims through controlled purchases or covert engagement with suspected insiders. Such activities can introduce legal, ethical, and operational risks, including supporting criminal ecosystems, compromising future investigations, and creating employment liabilities.

Organizations considering these approaches should:

- Consult legal counsel before any engagement.
- Coordinate with law enforcement when appropriate.
- Establish clear rules of engagement and executive approval processes.
- Prefer passive intelligence collection and corroboration through internal telemetry whenever possible.
- Avoid approaches that could incentivize or facilitate criminal activity.

Endnotes

1 United States Secret Service. (Jan. 9, 2026). *United States Secret Service*. “Inside Our Nationwide Crackdown On Card Skimming and Fraud.” Accessed June 30, 2026, at: Link.

2 Lawrence Abrams. (Aug. 4, 2021). *BleepingComputer*. “LockBit ransomware recruiting insiders to breach corporate networks.” Accessed June 30, 2026, at: Link.

3 Social Security Administration. (n.d.). *Social Security Administration*. “Disability Evaluation Under Social Security 2.00 Special Senses and Speech - Adult.” Accessed June 30, 2026, at: Link.

4 U.S. Department of Justice. (Apr. 30, 2026). U.S. Department of Justice. “Two Americans Who Attacked Multiple U.S. Victims Using ALPHV BlackCat Ransomware Sentenced to Prison.” Accessed June 30, 2026, at: Link.

5 Sergiu Gatlan. (Dec. 30, 2025). *BleepingComputer*. “US cybersecurity experts plead guilty to BlackCat ransomware attacks.” Accessed June 30, 2026, at: Link.

6 Gyana Swain. (Nov. 4, 2025). *CSO Online*. “Cybersecurity experts charged with running BlackCat ransomware operation.” Accessed June 30, 2026, at: Link.

7 Scott Ikeda. (Dec. 2, 2022). *CPO Magazine*. “Document Leak Reveals Meta Employees Took Bribes To Use Account Recovery Tool for Expedited Service, Account Hijacking.” Accessed June 30, 2026, at: Link.

8 Kathryn Blaze Baum and Alexandra Posadzki. (June 15, 2025). *The Globe and Mail*. “How underground brokers use their connections inside Meta to profit from hacked accounts.” Accessed June 30, 2026, at: Link.

9 Kathryn Blaze Baum and Alexandra Posadzki. (June 15, 2025). *The Globe and Mail*. “How underground brokers use their connections inside Meta to profit from hacked accounts.” Accessed June 30, 2026, at: Link.

10 United States Department of Justice. (March 13, 2024). *U.S. Department of Justice*. “Former Telecommunications Company Manager Admits Role in SIM Swapping Scheme.” Accessed June 30, 2026, at: Link.

11 Manhattan District Attorney’s Office. (Nov. 20, 2025). *Manhattan District Attorney’s Office*. “D.A. Bragg Announces Indictment Of Sim-Swapping ID Theft Ring, Including AT&T And T-Mobile Employees.” Accessed June 30, 2026, at: Link.

12 Tessa Langston. (Nov. 21, 2025). *Hoodline*. “Manhattan DA Charges Alleged SIM-Swapping Syndicate with $435K Telecom Heist, AT&T and T-Mobile Insiders Implicated.” Accessed June 30, 2026, at: Link.

13 Bart Blackburn. (Oct. 29, 2025). *dotData*. “The Invisible Thief: Synthetic Identity Fraud in Auto Lending.” Accessed June 30, 2026, at: Link.

14 Kyle Wilhoit and Stephen Hilt. (Aug. 6, 2015). *Trend Micro*. “The GasPot Experiment: How Gas-Tank-Monitoring Systems Could Make Perfect Targets for Attackers.” Accessed June 30, 2026, at: Link.

15 United States Secret Service. (Jan. 9, 2026). *United States Secret Service*. “Inside Our Nationwide Crackdown On Card Skimming and Fraud.” Accessed June 30, 2026, at: Link.

16 SEUR. (n.d.). *SEUR*. “SEUR: Shipping, Logistics, International.” Accessed June 30, 2026, at: Link.

17 Brian Hamacher. (May 7, 2026). *NBC 6 South Florida*. “Teen workers at Miami UPS Store face charges in $40K package theft, deputies say.” Accessed June 30, 2026, at: Link.

18 United States Department of Justice. (April 30, 2026). *U.S. Department of Justice*. “Members of ‘Noir’s Luxury Refunds’ Telegram Channel Sentenced to Prison.” Accessed June 30, 2026, at: Link.

19 Federal Trade Commission. (November 2024). *Federal Trade Commission*. “The Consumer Reviews and Testimonials Rule: Questions and Answers.” Accessed June 30, 2026, at: Link.

20 Federal Trade Commission. (Feb. 11, 2025). *Federal Trade Commission*. “FTC Publishes Inflation-Adjusted Civil Penalty Amounts for 2025.” Accessed June 30, 2026, at: Link.

21 ThreatMon [@MonThreat]. (April. 29, 2026). *X*. [Post]. Accessed June 30, 2026, at: Link.



Want more insights like this?

TrendAI | Resources and Insights

TrendAI™

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility and consolidated security that inspires confidence, drives innovation, and eliminates risk.

Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data.

AI Fearlessly.

Learn more: **trendaisecurity.com**

Copyright © 2026. Trend Micro Incorporated. All rights reserved. [REP00_The_Market_for_Trust_040826US]