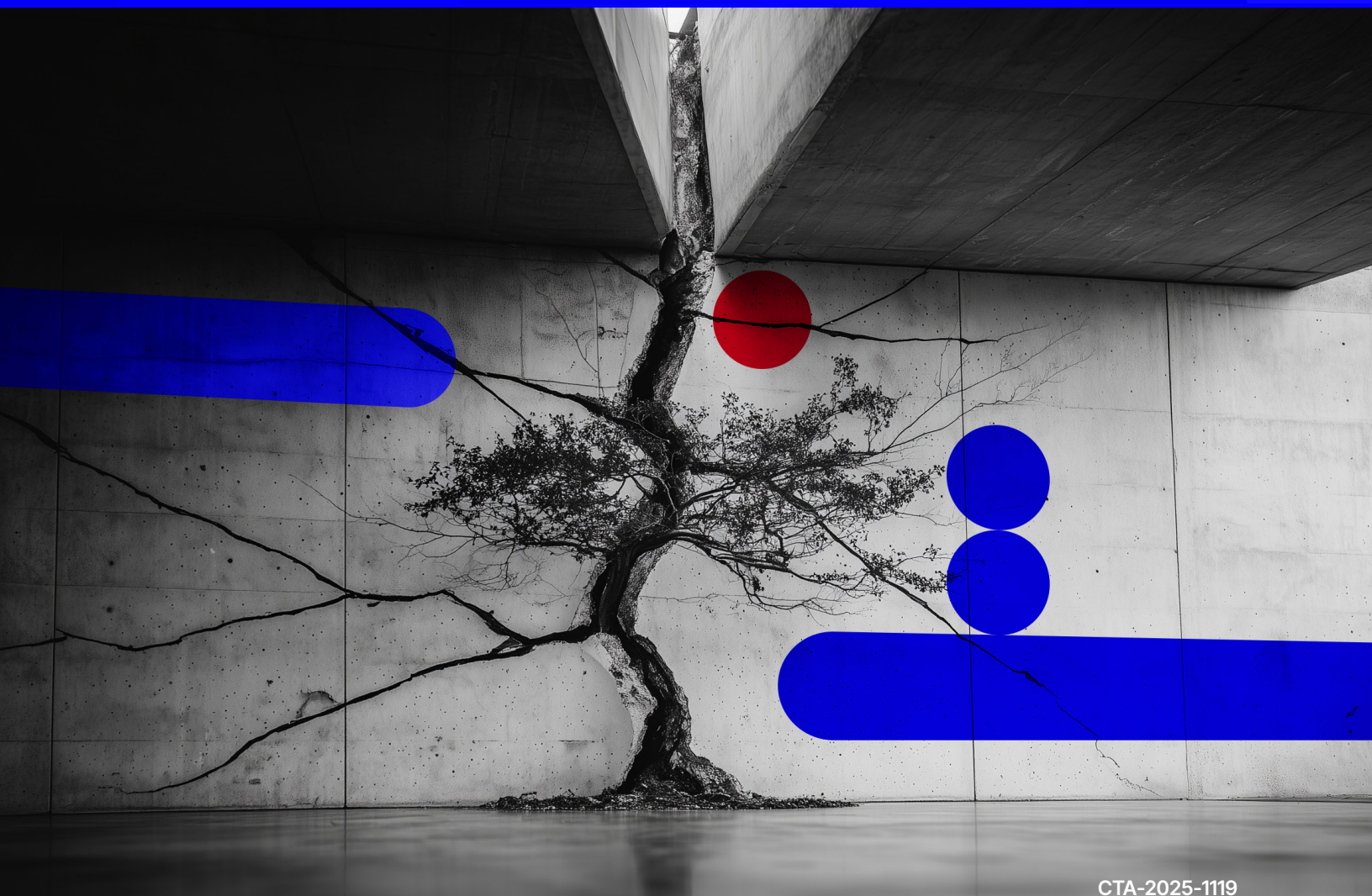
Recorded Future®

Market Opportunities and Advanced Strategies Increase the Impact and Resilience of Purchase Scams



CTA-2025-1119

Executive Summary

Purchase scams are a major emerging fraud threat in which threat actors use fake e-commerce stores to steal victim data and accept victim card payments for non-existent goods and services. Analysis by the Recorded Future Payment Fraud Intelligence team throughout 2025 indicates that threat actors leverage a dark web "opportunity economy" to increase the impact of their purchase scam operations. In particular, dark web market promotions of criminal services and emerging AI tools allow threat actors to rapidly scale their purchase scam infrastructure and develop fraud-funded ad campaigns that increase victim exposure and susceptibility.

Analysis by the Recorded Future Payment Fraud Intelligence team throughout 2025 indicates that threat actors leverage a dark web "opportunity economy" to increase the impact of their purchase scam operations.

At the same time, a suite of advanced strategies raises the resilience of purchase scam networks by masking relationships between their two key components: the scam websites that victims interact with and the financial merchant accounts used to accept fraudulent payments. Payments to merchant accounts controlled by scam threat actors are operators, which complicates fraud investigations. Transaction laundering tactics enable threat actors to conceal links between their merchant accounts and scam websites, raising the survivability of their merchant accounts. Traffic distribution systems tap modular structures, redirect chains, and victim screening techniques to maximize scam impact while reducing exposure to discovery.

Purchase scams present financial institutions, card networks, and other payment organizations with a financial fraud risk. Reducing this risk requires remediation that leverages scam merchant intelligence, which enables proactive identification of scam-linked merchant accounts before the fraud occurs. Programs that increase customer awareness are also a cornerstone of purchase scam mitigation strategy, as they empower bank customers to avoid financial loss altogether.

Key Findings

- **Purchase scams are a major emerging fraud threat.** Threat actors establish fake e-commerce stores linked to fraudulent merchant accounts, which they then use to manipulate victims into authorizing fraudulent payments for non-existent products. Purchase scams result in immediate financial loss and the theft of victim data that can be used to support downstream fraud.

- **A sophisticated dark web ecosystem allows threat actors to quickly establish new purchase scam infrastructure and amplify their impact.** Promotional activities mirroring traditional marketing — including an offer to sell stolen card data on the dark web carding shop PP24 — are widespread in this underground.

- **Malicious advertising is a common component of the purchase scam lifecycle**. Threat actors fund ad campaigns with stolen payment cards to spread purchase scams, which in turn compromise more payment card data, fueling a continuing cycle of fraud.

- **Dark web promotions surge during the holiday shopping season.** Threat actors exploit victims' changing shopping attitudes, sales promotions, and shifts in fraud controls that increase their odds of success and reduce the odds of discovery.

- **AI tools offer cybercriminals the resources to develop purchase scam campaigns.** Threat actors can likely abuse tools like Gamma, Darcula, and Lovable to generate scam content at scale, lowering barriers to entry.

- **Threat actors employ a combination of strategies to increase the resilience of their purchase scam networks.** The primary goal is to obscure relationships between the scam websites observed by victims and the financial merchant accounts used to accept fraudulent payments, complicating detection and investigation.

- **Victim authorization during purchase scams complicates fraud detection.** Because victims authorize payments in purchase scams, transactions appear legitimate to card issuers until the deception is discovered, delaying reporting and the identification of scam merchants.

- **Transaction laundering and sophisticated network designs prolong the lifespan of purchase scams.** These tactics break links between scam websites and merchant accounts and ensure that purchase scam networks are built in a resilient and scalable manner.

Threat Analysis

Purchase scams are a major emerging fraud threat. In their most common form, purchase scams occur on fake e-commerce stores linked to fraudulently acquired merchant accounts. Promotions on these fake websites manipulate victims into authorizing payments to the scam operator's merchant account for non-existent products. The result is immediate financial gain for the criminal and financial loss for the victim. Often, victim payment card data and personally identifiable information (PII) are also stolen during the scam transaction, which in turn enables additional downstream fraud.

Analysis by the Recorded Future Payment Fraud Intelligence team throughout 2025 indicates that two primary dynamics contribute to the growing threat presented by purchase scams:

- **A sophisticated dark web ecosystem enables threat actors to swiftly establish new purchase scam infrastructure and amplify the impact of their scam networks.** Promotional activity across this "opportunity economy" is widespread, mirroring traditional marketing strategies. Emerging AI tools help threat actors meet necessary skill and resource requirements.
- **Various strategies help threat actors increase the resilience of their purchase scam networks.** The goal of these strategies is to obscure links that can be used to detect and investigate a threat actor's purchase scam infrastructure — particularly scam websites observed by victims and the financial merchant accounts used to accept victim payments.

The Dark Web Marketplace and AI Tools Amplify Purchase Scam Impact

Opportunities to purchase stolen data or criminal services on the dark web and leverage emerging AI tools help threat actors rapidly establish purchase scam networks and amplify their impact. For threat actors, the goal is to maximize return on investment for costs incurred to operate the purchase scam.

Generally, threat actors increase purchase scam impact in two ways:

- **Scaling infrastructure effectively:** While domains for hosting scam e-commerce websites and fraudulent merchant accounts to accept payments are the two core requirements to establish a purchase scam network, other services and tools help increase their impact.
- **Increasing victim susceptibility:** After establishing their purchase scam networks, threat actors must ensure victims fall for the scam. Ad services propagate purchase scam lures to victims. AI tools help threat actors swiftly generate content to bait more victims into the scam funnel.

Sales promotions across the dark web allow threat actors to quickly scale purchase scams

Promotions broadcasting special offers, discount codes, and limited-time sales are widespread across the dark web criminal economy. Recent activity on dark web forums reveals a surge in seasonal promotions that mirror legitimate seasonal promotions during the holidays. By leveraging these promotions, threat actors can scale their scam and fraud operations more effectively, streamlining their resource requirements.

For example, in October 2025, sellers on BlackHatWorld Forum used Halloween-themed marketing hooks to promote sales of services that support purchase scam activity, including proxy services and social media accounts.

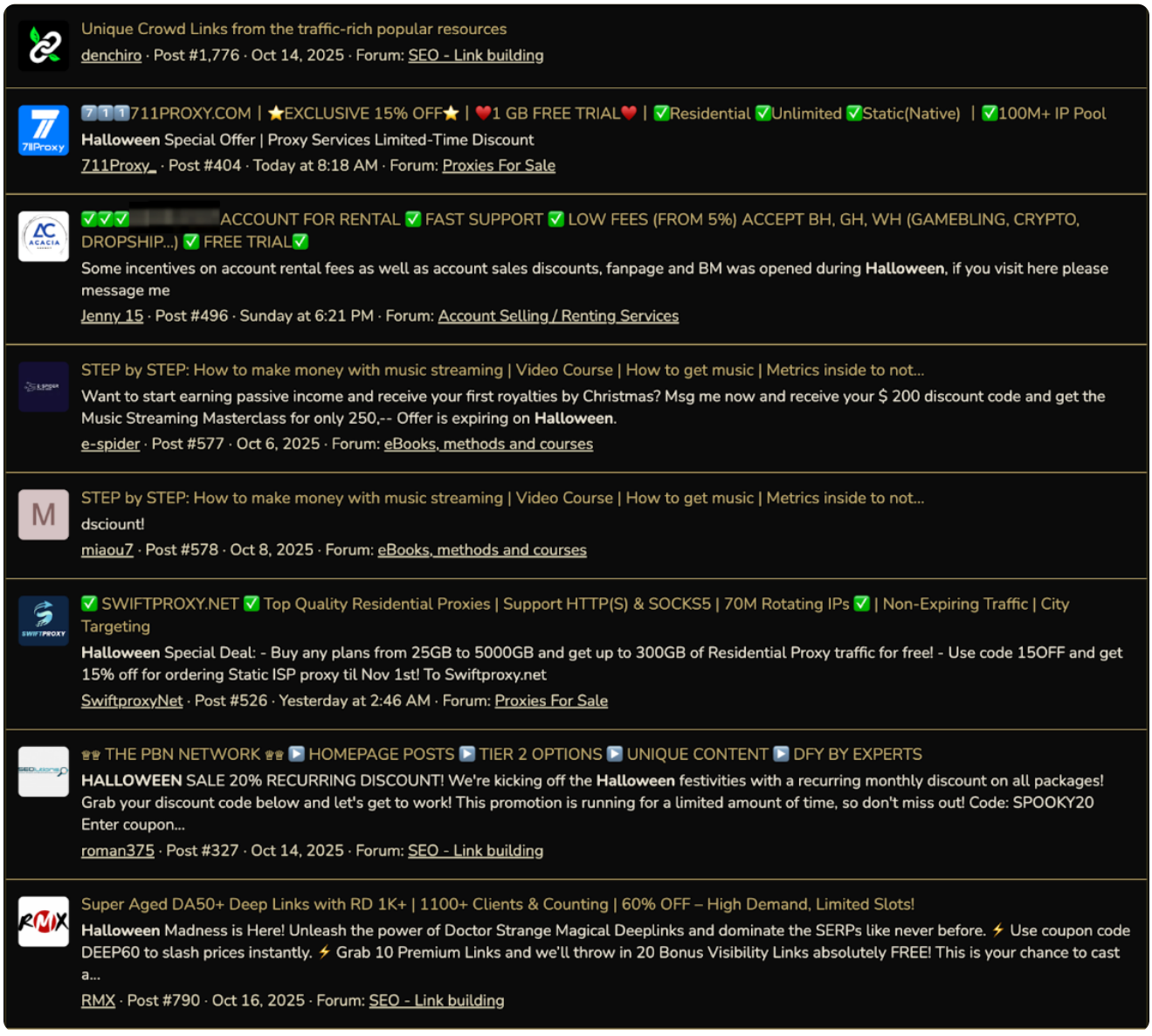


Figure 1: During the holidays, seasonal promotions of criminal services are widespread on dark web forums (Source: BlackHatWorld Forum)

Dark web forums are key sources that support purchase scam activity. This underground market activity typically occurs within clearly structured frameworks. On October 19, 2025, the threat actor "BassTrackerBoats" on BlackHatWorld published a “Black Friday 2025 Official Thread” to consolidate forum sales promotions ahead of the holiday shopping season and establish clear guidance for all promotions. Early sales offers on the thread were for services that support purchase scam websites, including mobile proxies, WordPress GPL packages, search engine optimization backlink services, and discounted web domains. By mid-November, activity in this thread and across similar dark web forums will likely increase as the holiday shopping season ramps up.

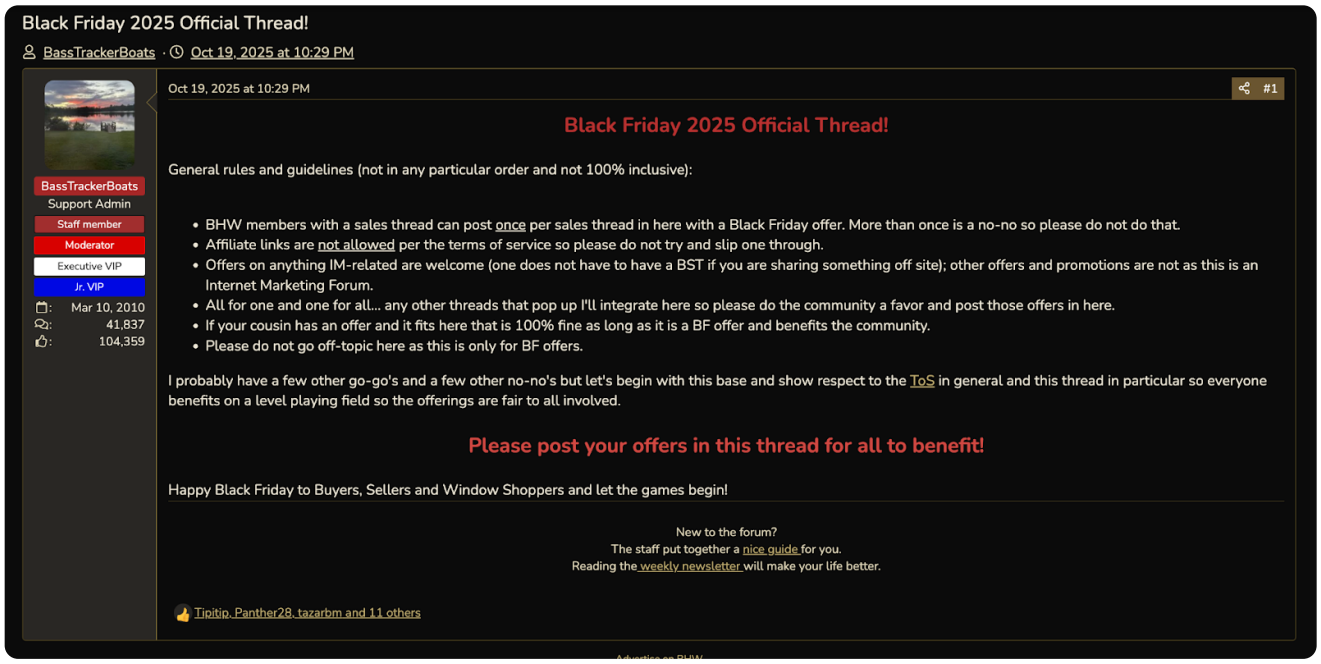


Figure 2: A timeline of some of the high-level cyber attacks conducted by Russia that were reported to have targeted Ukraine in the lead-up to the 2022 invasion.

Other resources in the dark web opportunity economy also help inexperienced cybercriminals develop purchase scam networks. For example, two posts authored in October 2025 by the threat actor "albanec” on Club2Crd shared information for disseminating purchase scams via malicious online ad lures, which are commonly used to deliver purchase scam websites to victims on social networks:

- On October 19, 2025, albanec posted a tutorial detailing how to use stolen payment cards to fund online ad campaigns. The threat actor called ad campaigns the "jackpot of digital fraud" due to ad spend’s instantaneous nature and reduced traceability compared to physical purchases.
- On October 20, 2025, albanec described ad cloaking, a technique that uses technical screening in malicious ads to target viable victims for the underlying purchase scam.[1] The threat actor called the tactic critical for bypassing monitoring on major ad platforms, noting that scam ad campaigns were vulnerable to account closure and website blocklisting without it.

[1] A similar victim screening method was previously observed in the “ERIAKOS” scam campaign in June 2024. Purchase scam websites in the ERIAKOS campaign were only displayed to victims who accessed the website through its corresponding ad lure on a mobile device.

Malicious advertising funded by stolen payment cards supports a broader fraud lifecycle. Threat actors use stolen cards to fund ad campaigns that propagate purchase scams, which in turn lead to the compromise of more payment card data. This stolen data can then be used to fund more malicious advertising campaigns, enabling additional downstream fraud.

Offers to sell stolen data to support purchase scam ad campaigns — as well as direct fraudulent monetization — are common across the dark web. On September 28, 2025, the threat actor "nod32-777," who is also the administrator of the PP24 dark web carding shop, advertised a "Black Friday" promotion on an underground forum, targeting both buyers and sellers of stolen data. The user advertised a 30% discount on all goods and services for ten days, highlighting PP24 as a "carding supermarket" and noting its high-quality inventory of stolen data, which includes victim Social Security numbers, bank accounts with routing number data, and payment card records with available card security codes. In addition to advertising discounted sales, nod32-777 encouraged sellers to supply databases with freshly stolen card data.

The surge of dark web promotions during the holiday shopping season is no coincidence. Threat actors are keen to exploit victims' changing shopping attitudes, sales promotions, and shifts in anomaly detection–based fraud controls that increase their odds of success and reduce the likelihood of discovery. Recorded Future Payment Fraud Intelligence analysts have previously observed threat actors abusing changes in merchant authentication requirements during the holidays to mask fraudulent purchases under specific price thresholds.

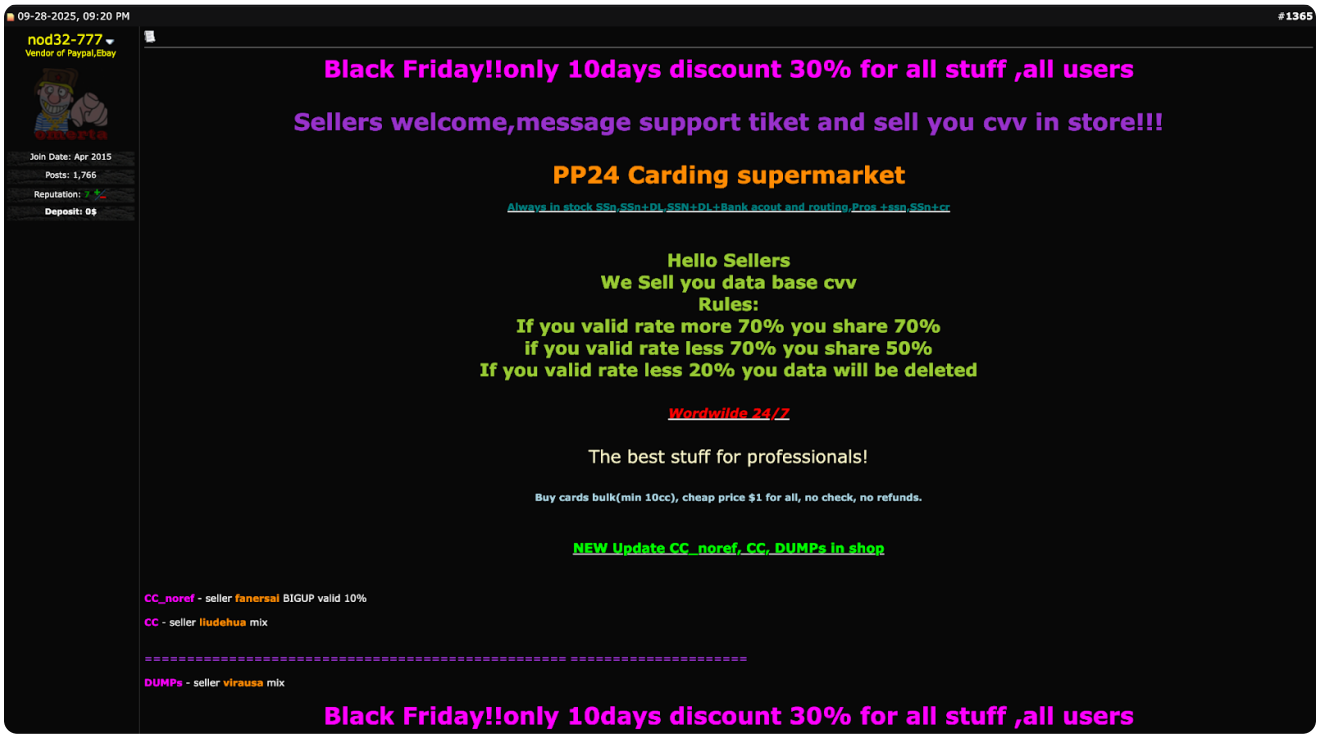


Figure 3: A user representing a dark web carding shop marketed promotions for stolen card data (Source: Recorded Future)

Recorded Future Payment Fraud Intelligence analysts have observed recent growth in the volume of merchant accounts linked to seasonal purchase scam websites targeting US victims. The identified scam domains abuse various well-known brands. Most of the websites are linked to the email address info@sellergloab[.]com. The merchant accounts processing payments for these purchase scam websites use merchant descriptors linked to two distinct merchant identifiers.

Over time — and particularly during the approaching holiday period — this network of identified merchant accounts and scam domains will likely continue to evolve and expand, incorporating more domain and merchant infrastructure over time, as will other purchase scam networks.

Ad services and emerging AI tools help scam operators increase victims' susceptibility

Market opportunities also allow threat actors to develop workflows and leverage tools that increase victim susceptibility to their purchase scams. Payment Fraud Intelligence analysts identified affiliate marketing network data that indicated lucrative Black Friday ad payouts for "CC [credit card] sweepstakes" promotions. These affiliate ad offers are almost certainly related to ongoing purchase scam campaigns that redirect victims from ads to scam attack funnels, increasing victim susceptibility and operational scale through targeted ad exposure.

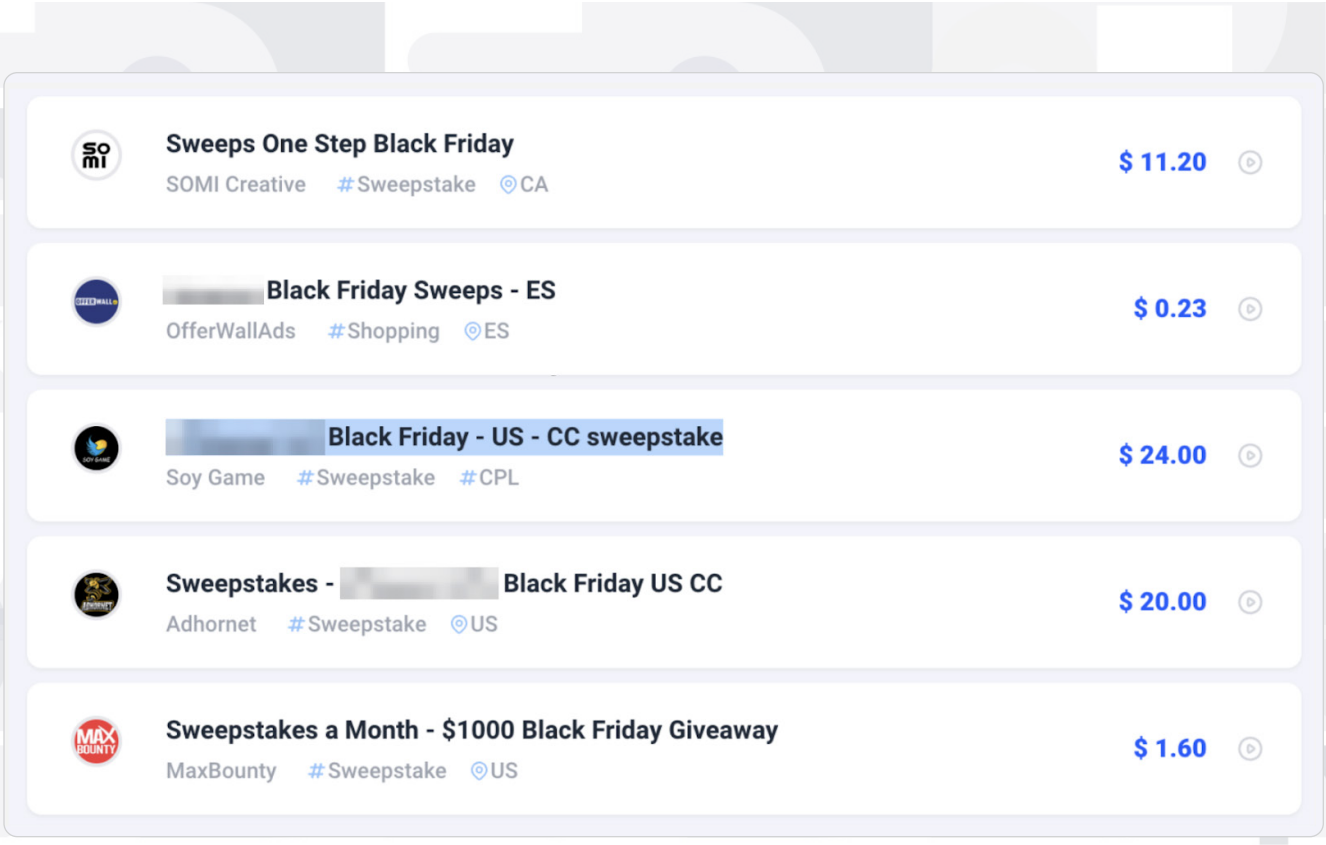


Figure 4: These ad payouts for Black Friday visitor traffic are almost certainly linked to scams (Source: affplus[.]com)

Market offerings of this nature have grown common in recent weeks due to the end-of-year holiday shopping season. Consumers tend to increase shopping spend during the holidays and often maximize value by taking advantage of sales promotions, creating an opening for purchase scam operators to entice more victims into their scam attack funnels. During an ongoing purchase scam investigation, the Recorded Future Payment Fraud Intelligence team identified several online advertising campaigns that target victims for holiday-themed purchase scams (in this case, for Halloween).

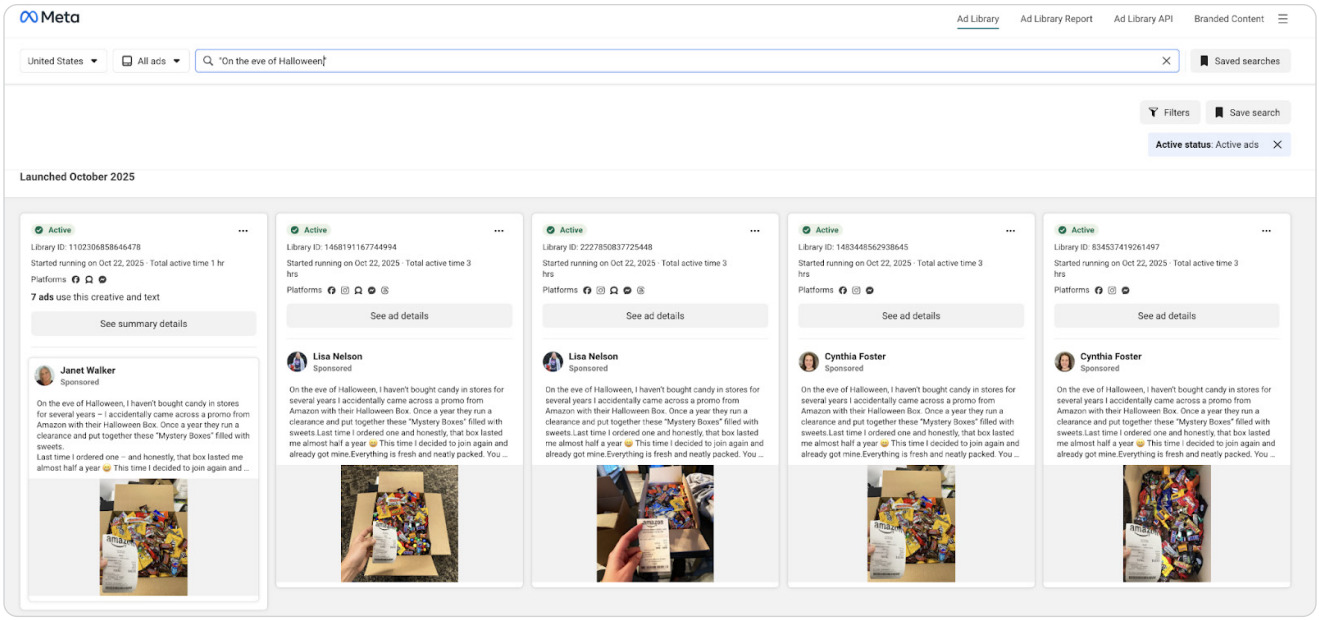


Figure 5: These ad campaigns for "Halloween giveaways" almost certainly support scams (Source: Meta Ad Library)

Cybercriminals engaged in purchase scam activity also continue to leverage generative AI. This adoption has amplified the effectiveness of social engineering and content generation, enhancing threat actors' ability to attract victims to their scam websites.

In 2025, three AI threats will likely allow threat actors to amplify the impact of their purchase scams:

- **Gamma:** On April 15, 2025, Abnormal reported that threat actors abuse Gamma, an AI-powered presentation tool, to deliver polished multi-stage phishing campaigns impersonating legitimate login portals. Malicious emails from compromised accounts directed victims to Gamma-hosted presentations with corporate branding and call-to-action links, which guided victims to credential harvesting pages. While attackers captured victim login credentials and session cookies to facilitate multi-factor authentication bypass and account takeovers, similar abuse can very likely support purchase scam activity.
- **Darcula:** On April 24, 2025, Netcraft reported that the Chinese PhaaS toolkit "Darcula" integrated AI capabilities in a recent update. The AI integration allows users to generate and translate phishing forms in any language, customize form fields, and maintain layout and style. According to Netcraft, these capabilities lower entry barriers for threat actors seeking to create phishing kits, likely increasing the speed and scale at which phishing attacks can

be launched and complicating automated detection and takedown. As with Gamma, this toolkit can likely support purchase scam activity.

- **Lovable:** On August 20, 2025, Proofpoint reported that threat actors increasingly abuse Lovable, an AI-powered website builder, to generate and host phishing and fraud campaigns. Observed activity for these websites included data theft through impersonation of delivery and banking services. Since February 2025, Proofpoint has detected tens of thousands of malicious Lovable URLs, with many websites using CAPTCHA to increase their credibility and Telegram-based exfiltration to streamline stolen data collection.

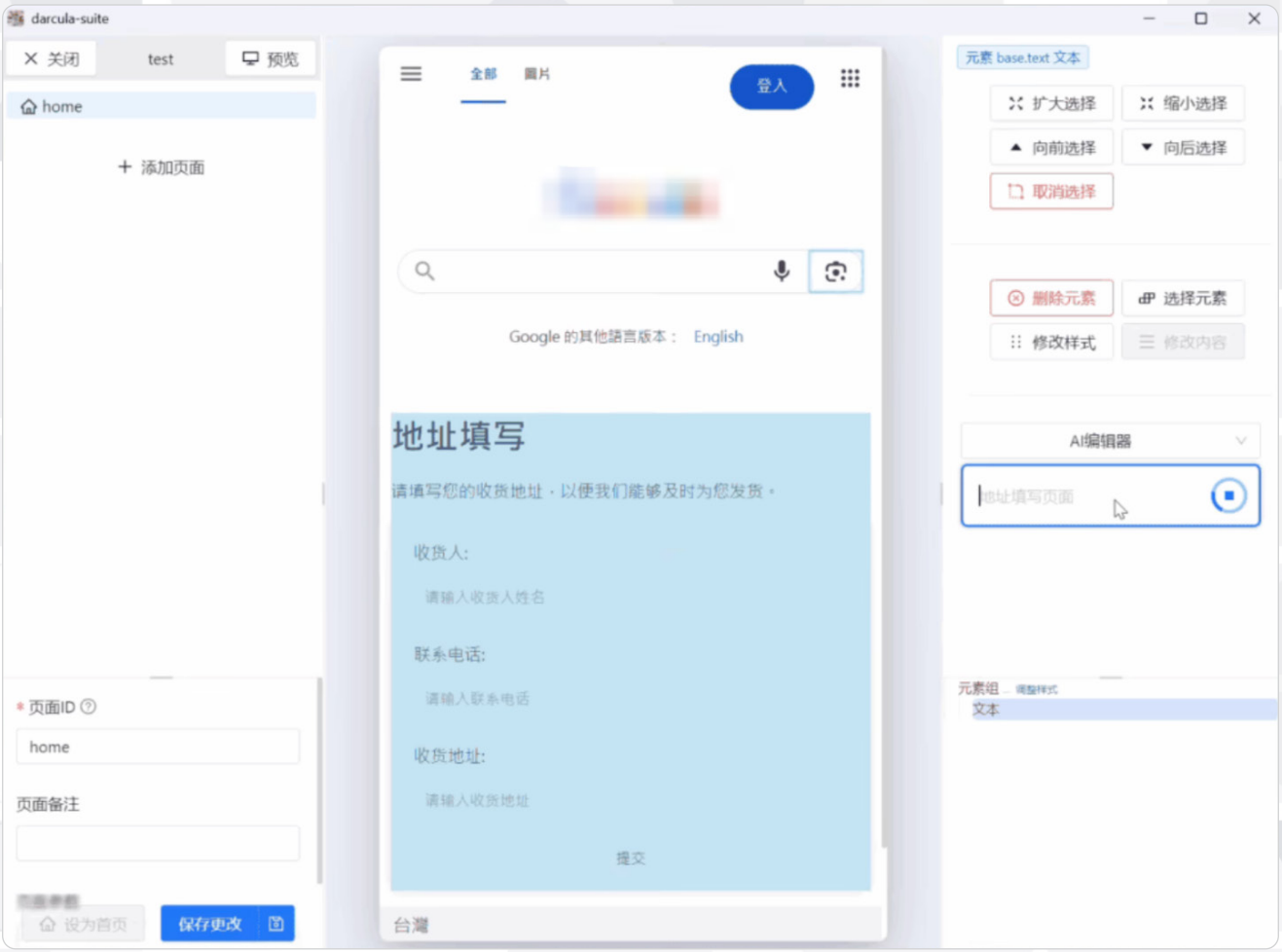


Figure 6: Darcula's AI integration responds to a prompt to generate an "Address Filling Page" (translated from Chinese) (Source: Netcraft)

Advanced Resilience Strategies Prolong the Lifespan of Purchase Scams

Beyond the initial deception, purchase scams are increasingly sophisticated in how they leverage victim authorization, merchant infrastructure, and reporting delays to complicate detection and investigation.

Victim authorization complicates discovery, reporting, and investigation

In purchase scams, fraudsters pose as trustworthy sellers of goods and services that are never delivered. Because payments to scam merchant accounts occur over card payment rails, transactions authorized by victims appear legitimate until they discover they were deceived.

For anti-fraud purposes, this victim authorization distinguishes purchase scam fraud from typical third-party fraud, which sees fraudsters using stolen financial data to make unauthorized purchases.

Victim authorization offers two advantages to purchase scam operators:

- Immediate financial gain
- Fraud detection challenges

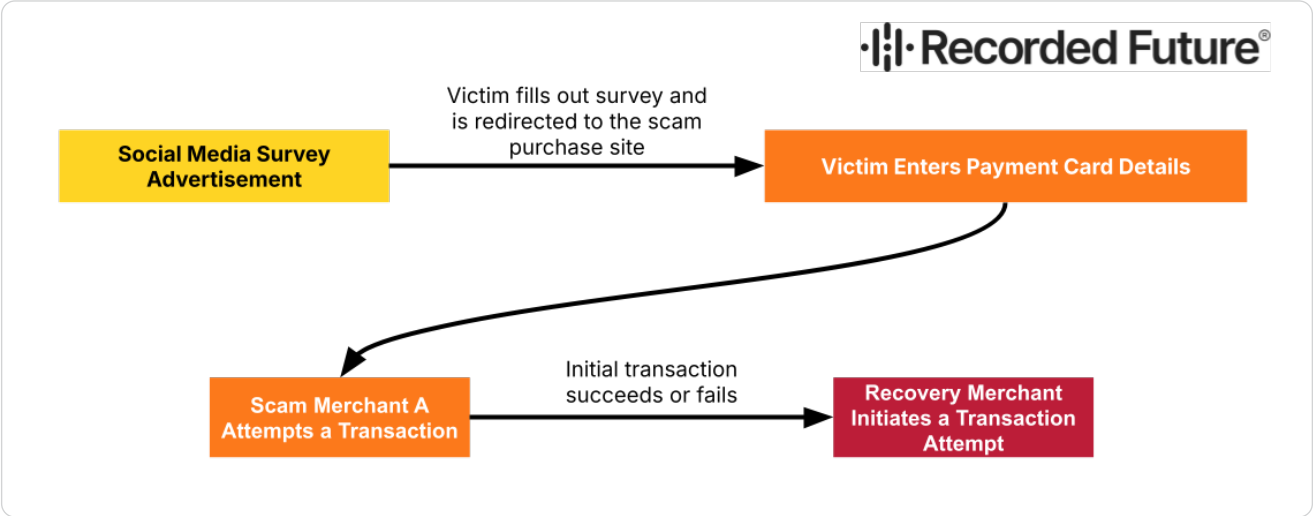


Figure 7: After receiving victim authorization, one purchase scam campaign uses purported transaction recovery services to attempt two sequential fraudulent transactions, effectively "double-monetizing" the card data (Source: Recorded Future)

Immediate financial gain and risk of downstream fraud

The primary advantage that victim-authorized payments offer threat actors is immediate financial gain. Whereas other fraud attack vectors require a more substantial investment of time and resources to cash out stolen data, purchase scam transactions offer immediate payouts to the scam operator.

Despite their primary reliance on linked merchant accounts, purchase scam websites also commonly steal victim data during the fraudulent transaction. In these cases, downstream fraud losses occur through subsequent fraudulent transactions.

Authorization and delayed reporting create detection challenges for card issuers

The victim's inherent participation in purchase scams limits the effectiveness of card issuers' fraud model–based detection methods, preventing the discovery of purchase scams. As a result, financial institutions depend on customer reporting to detect purchase scam activity and scam-linked merchant accounts.

The result of this is a substantial delay between the actual purchase scam payment, identification of the fraud event by the card issuer, and subsequent reporting to card networks — reporting that can be vital for effective scam merchant detection across the wider payment ecosystem.[2]

Scam operators account for this grace period when planning purchase scam operations. To compensate, they often prepare inventories of scam domains in anticipation of eventual takedown requests while cycling merchant accounts across different scam domains to reduce their association with any single scam website and extend their lifespan.

To protect merchants, scam operators obscure links with attack funnels

Transaction laundering tactics allow scam operators to hide links between their fraudulent merchant accounts and scam websites. This obfuscation is aimed at increasing the resilience of scam-linked merchant accounts, which are costly to acquire. Transaction laundering occurs when a merchant processes transactions for entities that the acquirer is unaware of, exposing the acquirer to unknown risk. In practice, transaction laundering lets purchase scam operators circumvent detection during know-your-business (KYB) checks and ongoing monitoring by acquirers and payment facilitators.

For purchase scams, transaction laundering is clearest in the divorce between the merchant URLs that scam operators provide during merchant onboarding and the URLs of scam websites that victims actually interact with. Merchant onboarding processes assume that merchant information is provided in good faith; therefore, screening fails to identify malicious purchase scam domains that are not linked to merchant account applications. As a result, traditional KYB checks are less effective at proactively identifying scam merchants because the link between the merchant and the scam domains is intentionally broken.

[2] The payment ecosystem is adapting in recognition of this challenge. For example, Mastercard has introduced subtype codes for various scam typologies, including purchase scams, allowing for improved dispute resolution and tracking of scam-linked fraud.

Ultimately, this deliberate separation prolongs the operational lifespan of the entire purchase scam network. The result is delayed takedown and greater fraud exposure.

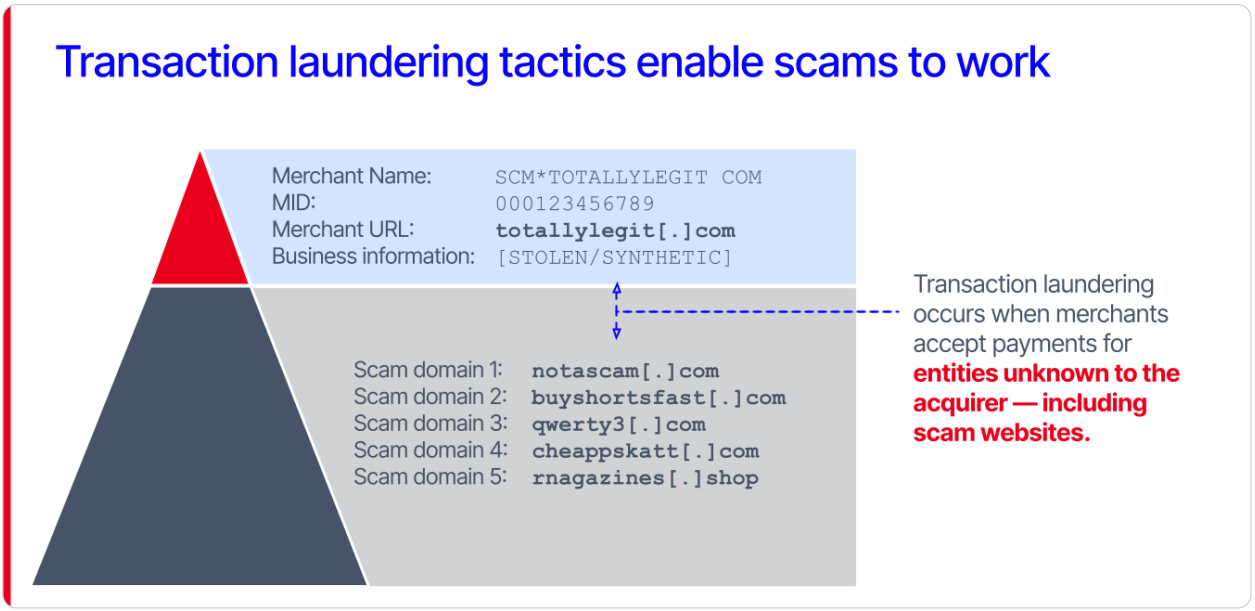


Figure 8: Scam operators intentionally break the links between scam domains and merchant URLs that might enable proactive detection of the malicious activity by acquirers and payment facilitators (Source: Recorded Future)

Subscription traps involve fraudulent enrollment in recurring payments. In these schemes, scam websites that victims interact with never display subscription terms clearly. However, URLs directly associated with the fraudulent merchant account display subscription terms in plain sight. In addition to masking the relationship between the two, this tactic also likely complicates fraud investigations and chargeback disputes.

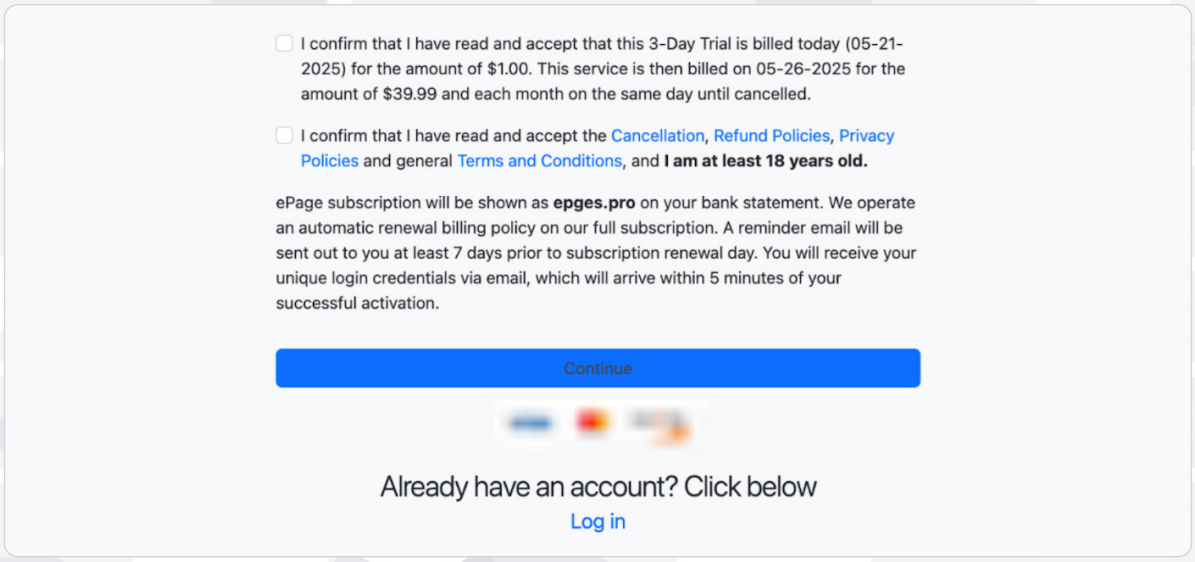


Figure 9: One scam campaign exploiting negative billing option payments — a subscription trap — displayed the billing logic on its merchant pages while concealing the billing logic on the scam websites encountered by victims (Source: epges[.]pro)

Even within a single purchase scam campaign, clever design structures mask links between scam websites. In one campaign that redirected visitors through multiple scam websites, a website soliciting personal information used a disclaimer to distance itself from liability for downstream scam payments on linked websites:

> This website is a landing page to promote third-party websites or products. We do not bill for membership to this website. By registering you will be redirected to the registration page of one of our partner's websites. Names or images that may be displayed on this website were transmitted by an external affiliate. We do not assume responsibility for the availability of them.

Tenuous connections between scam websites and merchant accounts often shed light on how the networks are operated. In November 2024, Recorded Future Payment Fraud Intelligence analysts uncovered a network of eight scam websites that used brand abuse and typosquatting tactics and were promoted via social media ads leveraging holiday shopping themes. Websites associated with the merchant accounts were designed to appear legitimate, providing a layer of credibility. However, shared identifiers — IP addresses, phone numbers, and physical addresses — revealed an additional twenty interconnected domains tied to eleven shell companies. Threat actors likely used these domains and companies to register fraudulent merchant accounts associated with the scam activity.

Modular builds, redirects, and access filtering increase scam resilience

Scam operations often work in multi-stage attack funnels targeting specific victims. One common tactic is the use of a traffic distribution system (TDS) within a greater affiliate marketing model that attracts victims to the purchase scams. In these campaigns, each stage of the purchase scam entices the victim to the next website toward the scam's culmination: the victim-authorized transaction.

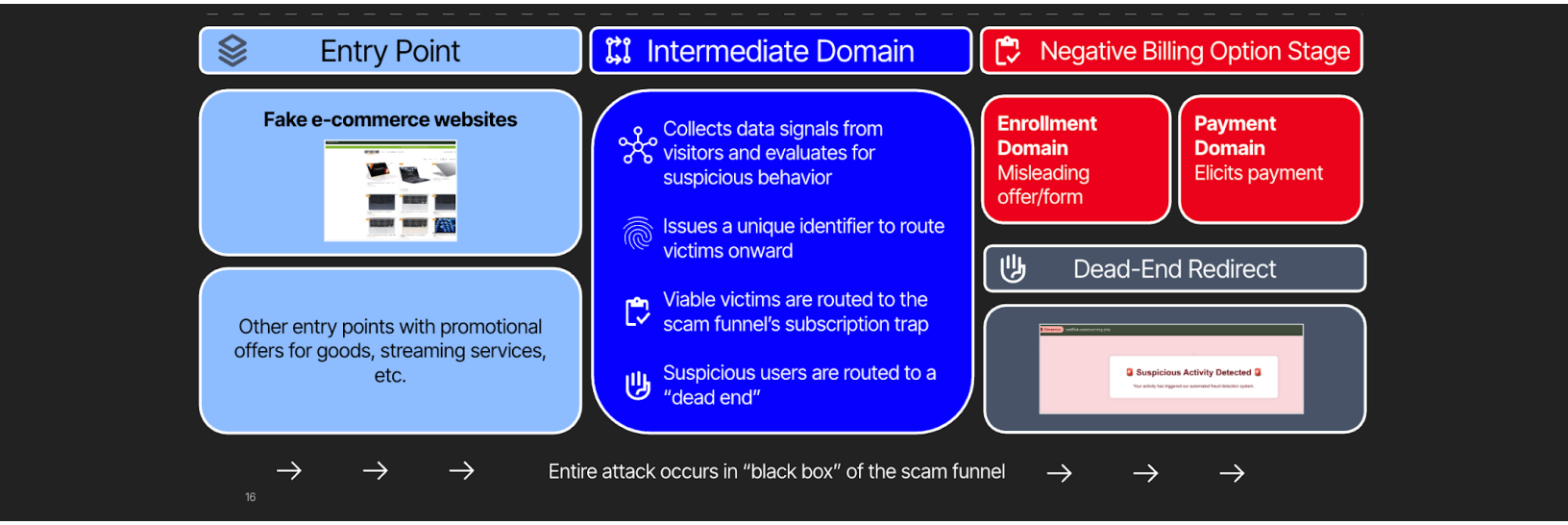


Figure 10: Multi-stage scam funnels gradually draw victims in, with each step carefully engineered to lead them closer to the final trap (Source: Recorded Future)

Modular build: Scams incorporate redundant components

TDS-based scam operations use a modular design, spreading their activity over interchangeable components. Within this modular setup, elements like landing pages, payment systems, and ad lures can be quickly deployed or substituted. This setup allows scam networks to quickly scale. Moreover, because there is no single point of failure, the scam network will remain operational if elements of the infrastructure are reported and removed, increasing the resilience of TDS scam clusters to takedown.

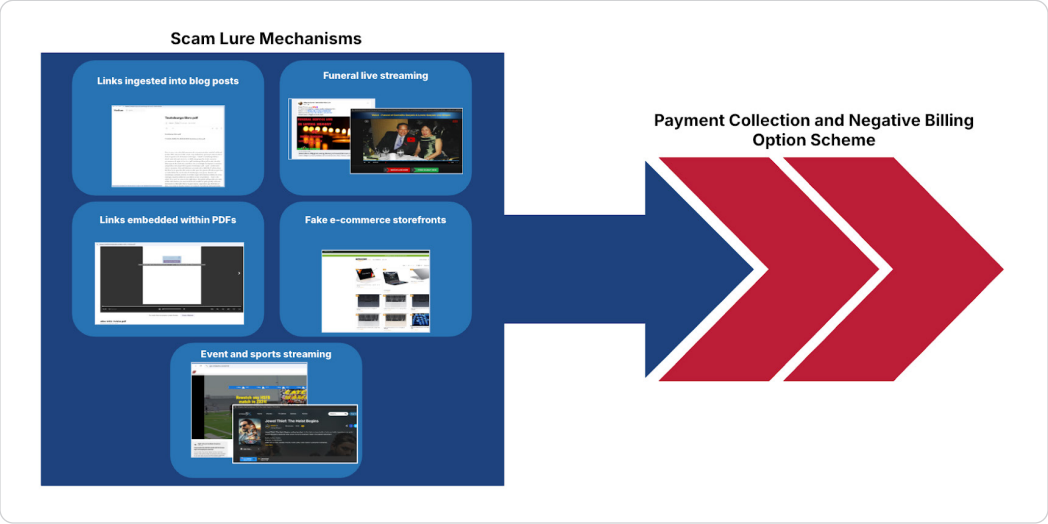


Figure 11:
One scam campaign used interchangeable scam lure mechanisms to entrap victims
(Source: Recorded Future)

Redirect chains: Victims coaxed through multi-stage scam attack funnels

Redirect chains, common in TDS scam operations, entice victims to continue through multiple pages before bringing them to the culmination of the attack, where the victim-authorized transaction occurs. For victims, each step masks the original source and the operator's intent, discouraging reporting. For financial institutions, the multi-stage redirect chains complicate investigation.

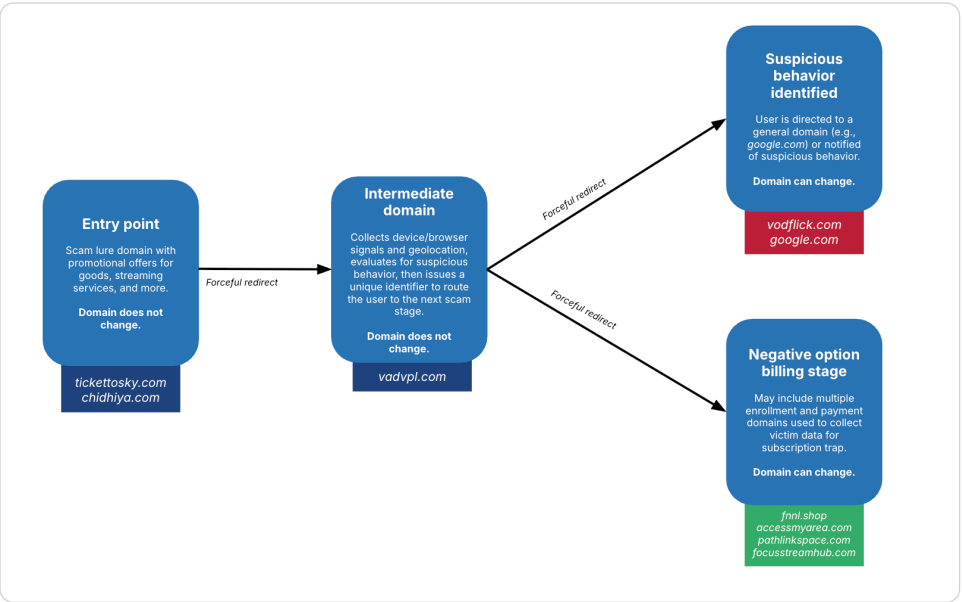


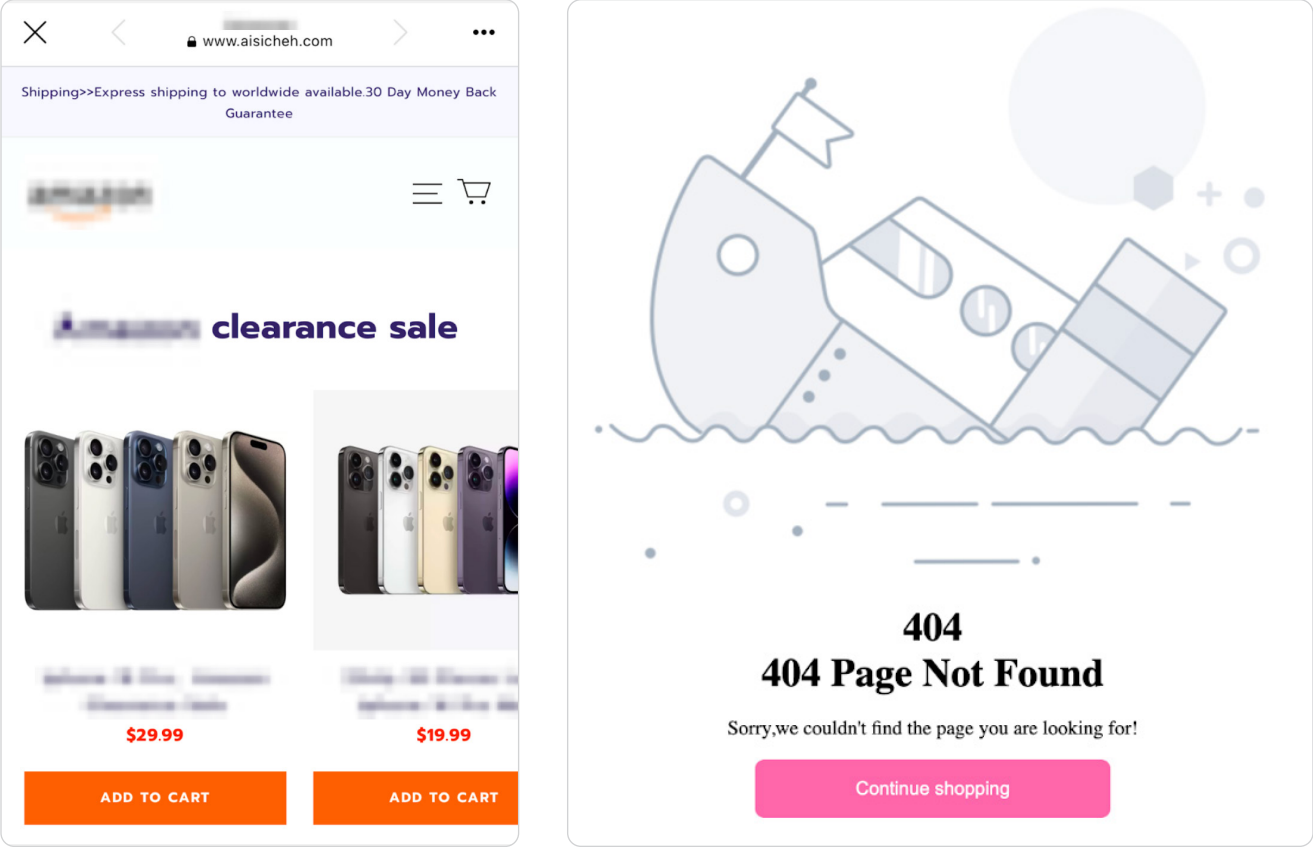
Figure 12:
Scam networks often redirect victims through a multi-stage attack (Source: Recorded Future)

Access filtering: Scam funnels screen victims for access

TDS scam campaigns employ access filtering techniques to selectively admit viable victims while blocking unwanted visitors. By analyzing features like device type, browsing behavior, and other indicators, these systems ensure that only targeted individuals proceed to the culmination of the purchase scam. Security researchers and web crawlers are redirected to dead ends or non-malicious pages, bolstering the scam's resilience to investigation.

Examples of parameters used for access filtering include:

- Presence of security tools (e.g., visitors using VPNs)
- Website access method (as indicated by referrer header)
- Geographic location (as indicated by visitor IP address)
- Device type (as indicated by visitor user-agent data)



Figures 13 and 14: The "ERIAKOS" scam campaign displayed different content to different visitors, depending on the device used and method of access (Source: aisicheh[.]com)

A more sophisticated variation of access filtering occurs when content is selectively displayed to different visitors. Scam websites observed in the "DEIMOS" scam ecosystem serve content based on the victim's region, showing generic pages to non-targeted users. This functionality conceals the scam campaign's true purpose when visitors do not match the targeting criteria.

Mitigations

E-commerce scams present financial fraud risks to card issuers and compliance risks to merchant acquirers, especially in cases where linked scam merchant accounts are also abused to support transaction laundering activity. To reduce these risks, apply the mitigation strategies described below.

Card Issuers

- Leverage Recorded Future Payment Fraud Intelligence Scam Merchant Data to proactively detect and mitigate fraud with scam merchants.
- To prioritize fraud prevention over potential customer friction, immediately decline transactions with identified scam merchant accounts and track customer card accounts that have transacted with the merchant for additional fraud signals.
  - Escalate the fraud risk score of customer accounts that attempt transactions with the merchants or flag the account for additional review.
  - Consider the presence of additional fraud signals on flagged accounts as a high-confidence basis to reissue the customer card or apply other remediations. Other fraud signals include downstream transactions with confirmed Tester Merchants or a match between the flagged account and for-sale Partial Card Data on the dark web.
- To minimize customer friction, assess transaction data within your cardholder portfolio with the identified scam merchant accounts before taking action against either the merchant accounts or customer card accounts.
  - Bucket all customer transactions with the identified scam merchants.
  - Determine a fraud incidence threshold in accordance with your organization's risk tolerance. This threshold should be higher than the baseline fraud incidence rate observed across your portfolio.
  - If customer transactions within the bucket exceed the fraud incidence threshold, automatically block all customer transactions with the identified merchant accounts and consider card reissue.
- Solicit scam website leads from your customers to identify other scam networks that pose a threat to your customer base. Customer reporting is crucial to identifying scam websites early.
- Review fraud intelligence reporting to stay abreast of trending scam threats to your customers and your organization.

Merchant Acquirers

- Leverage Recorded Future Payment Fraud Intelligence Scam Merchant Data to proactively detect and mitigate fraud with scam merchants.
- Analyze confirmed scam merchants to identify other likely fraudulent merchant accounts in your portfolio. Fraudulent merchant accounts acquired by the same threat actor tend to use similar data and are registered within a short period of time.
- Flag suspected fraudulent merchant accounts for enhanced due diligence, investigation, suspension, or termination in accordance with your risk tolerance.
- Flag merchants with excessive chargeback rates for targeted review.
- Ensure that merchants meet required data security standards for storing, processing, and transmitting cardholder information.

Customer Awareness and Education

- Only provide personal and payment information on secure, trusted websites.
- Research companies before you make purchases from them. Review complaints on open sources and ask trusted contacts to understand others' experiences with the company.
- For companies you trust, verify the legitimacy of e-commerce websites and their payment subdomains before making purchases. Check the website's URL, ensure that it uses HTTPS, and compare it to the official website's URL.
- Understand the terms and conditions for purchases you make, and be aware that honest businesses do not hide these terms from their customers. Do not continue with your purchase if the terms and conditions differ from your understanding of the offer. Be wary of pre-checked boxes that may give your consent to sign up for expensive monthly subscriptions.
- Understand how to cancel subscriptions or terminate paid memberships. Free trials may have a time limit before automatically initiating subscriptions; ensure that you understand these deadlines.
- Be wary of unsolicited communications or advertisements. The threat actors responsible for this scam infrastructure primarily used social media advertisements to disseminate their scam websites.
- Stay aware of common scams and phishing techniques and remain vigilant when interacting with online social media content.
- Report scams to your card issuer and dispute losses to attempt to recover your funds through chargebacks.

Outlook

The dark web opportunity economy is highly developed and will likely continue to facilitate purchase scam activity. Financial institutions, card networks, and other payment organizations are acutely aware of the threat that purchase scams present (as well as the difficulties in detecting them), but robust proactive mitigation strategies against purchase scams are still developing. While crucial stakeholders have begun buttressing the card payment ecosystems' resilience against purchase scams — as seen in Mastercard's scam subtypes for card issuer fraud reporting — it will likely be some time before reliably effective anti-scam strategies gain broad acceptance. Regardless of the form these measures take, they will likely incorporate proactive scam merchant data intelligence, which leverages research and pattern analysis to identify purchase scam websites and merchants before their wider deployment.

Looking forward, AI-driven automation will likely continue to fuel the potential impact of purchase scam ecosystems. In recent years, AI has already reshaped the fraud landscape by enabling convincing real-time deception through deepfakes and phishing content generation. This development will likely persist and expand. Although requirements to operate purchase scam websites are not as steep as in other cyber-enabled fraud schemes, AI nevertheless allows purchase scam operators to achieve vast scale at great speed, raising exposure and financial losses.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at **recordedfuture.com**.