CYBER
THREAT
ANALYSIS

Recorded Future®

By Payment Fraud Intelligence

November 26, 2024

Scam Websites Take Advantage of Seasonal Openings and Established Methods to Maximize Impact

Scam websites are effective when threat actors can fool cardholders and banks. Cardholders are the direct victims of scams, and banks' anti-fraud systems are designed to protect them from fraud.

Seasonal opportunities — including holidays, shopping events, and trending social topics — lower the threshold for success for scam operators and raise victim susceptibility to the scam.

Threat actors' monetization strategies drive the functionality of their scam websites and payment forms, with different monetization strategies offering advantages and disadvantages to threat actors.

Executive Summary

Analysis by the Recorded Future® Payment Fraud Intelligence team has identified scam websites as a growing fraud attack vector in recent years. This report delves into the methods used by threat actors for scam website operations, the decisions they face when organizing and conducting scam website operations, and how these decisions manifest for scams' direct and indirect victims: cardholders and financial institutions.

Scam websites present financial fraud risks to financial institutions and brand reputation risks to merchants and organizations imitated by the scam operator. At a high level, scam website operations occur across various stages. After threat actors procure the resources necessary for their scam operation, they design and distribute scam lures capable of reaching as many victims as possible in a short period of time. Threat actors must weigh the ease of compromise against the ease of monetization when determining how to monetize their scam website, and their chosen monetization method will determine the functionality of the scam website and payment form.

Key Findings

- For scam websites to be effective, threat actors must primarily fool two parties: cardholders and banks. Cardholders are the direct victims of any scam, and banks often share liability for those cardholders' fraud losses.
- Broadly, threat actors' ability to deceive cardholders and banks can be assessed by examining their choices across five categorical stages: procurement, scam lure content, scam lure delivery, scam website and payment form, and fraudulent monetization.
- Seasonal opportunities — including holidays, shopping events, and trending social topics — lower the threshold for success for scam operators and raise victim susceptibility to the scam.
- Scam lures depend on adaptability and success, and their distribution occurs during high-volume, short-lived campaigns via online advertising services, SMS text messages, phone calls, and email.
- Monetization strategies drive the functionality of scam websites and payment forms, with different monetization strategies offering advantages and disadvantages to threat actors.
- Soliciting scam website leads from customers and increasing customer awareness are the most effective mitigation strategies against scam website operations.
- Scam website operations will likely continue to evolve rapidly, and the use of merchant accounts for scams will likely grow — although government regulation may moderate this outcome.

Background

If fraud is defined as deception for the sake of personal financial gain, then few schemes embody fraud as well as the scam. The image is classic: a huckster pitches snake oil, and a victim parts with their purse. When the fraudster skips town with their ill-gotten gains, the victim is left with no recourse.

In reality, the truth of how scammers operate is more nuanced — especially following the advent of e-commerce and online advertising. At first glance, scam websites posing as merchant-operated online stores or government entities can be indistinguishable from the real thing, and tricky terms and language often provide a facade of legitimacy that shields the scam websites from suspicion and remediation. Worse, online scams sometimes blur the lines between legitimate and malign activity, leaving financial institutions perplexed as to who is truly at fault and how to recoup losses once victim complaints begin rolling in.

Threat Analysis

For scam websites to be effective, threat actors must primarily fool two parties: cardholders and banks. Cardholders are the direct victims of any scam website, and their card or financial account information serves as the vehicle through which the scammer will siphon funds. The impact of successful scam attacks eventually trickles up to banks, which can be liable for their customers' fraud losses.

This liability offers banks a vested interest to protect their customers from scam websites and other fraud. Therefore, a successful scam website operation must not only disarm a cardholder's suspicion but also evade the bank's anti-fraud systems in order for the operator to cash out whatever financial information is coaxed from the direct victim. This is another iteration of the classic Castle Dilemma: banks' anti-fraud teams must work from a place of relative disadvantage to defend their customers from nefarious activity that occurs beyond the castle walls: the firewalls, network monitoring, and threat intelligence feeds that comprise the bank's defenses against direct attacks targeting the institution.

Broadly, threat actors' ability to deceive cardholders and banks boils down to the *how* and *why* of their scam website execution, which can be broken down across five categorical stages:

> **Stage 0: Procurement.** The threat actor assembles the resources, tools, and infrastructure they will need to conduct their scam website operation.
> **Stage 1: Scam lure content.** The threat actor designs their scam lures, exploiting psychological triggers and seasonal opportunities to maximize impact.
> **Stage 2: Scam lure delivery.** The threat actor organizes the distribution of their scam lures to susceptible victims, focusing on volume and intensity.
> **Stage 3: Scam website and payment form.** Upon the victim's arrival to the scam website, the threat actor taps into the force of urgency to coax action from the victim.
> **Stage 4: Fraudulent monetization.** Depending on how the scam website is configured, the threat actor leverages the victim's action — usually inputted stolen information — for monetary gain.

Seasonality Creates Opportunities for Online Scam Operators

Perhaps more than any other sphere of fraud activity, scam websites are highly dependent on opportunities created by seasonal trends and events. Examples include holidays — Halloween and Christmas are perennially popular — shopping events — think Black Friday and Cyber Monday — and government events — tax filing season or the open enrollment period for US healthcare.

Seasonal opportunities are important for threat actors because they not only lower the threshold to success for threat actors but raise the susceptibility of victims, who are more likely to fall for the urgency generated by the threat actor's scam lure and website. The tax filing season, for example, includes a built-in deadline that raises the urgency for taxpayers to take action before facing penalties. Similarly, Black Friday offers limited-time discounts that cardholders are eager to pounce on, and relaxed anti-fraud systems meant to reduce customer friction may inadvertently enable fraud.

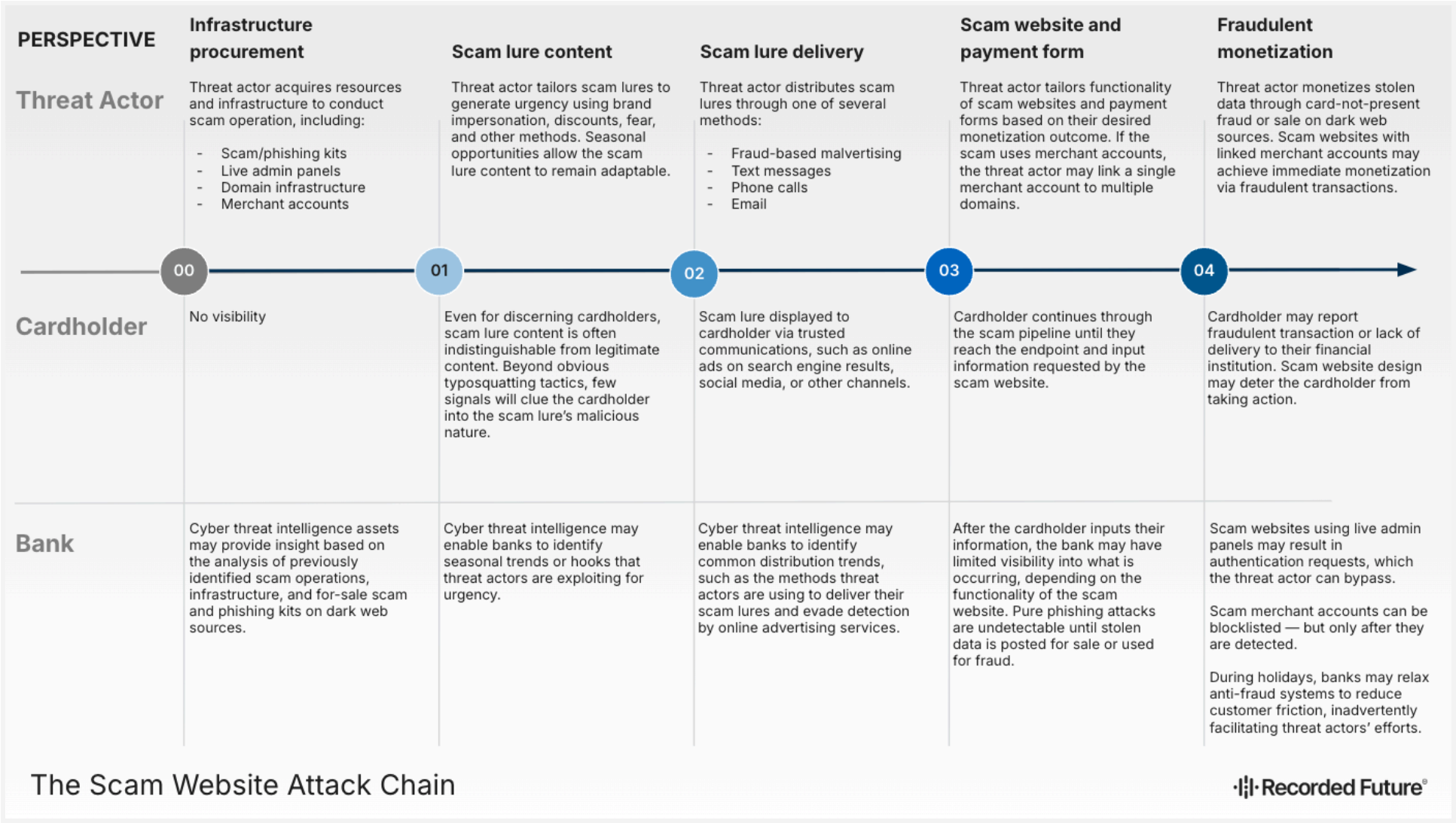


Figure 1: *The success of scam website operations can be understood by examining how and why threat actors design and conduct the scam website operation across several categorical stages, beginning with the procurement of tools they will need for the scam and ending with the method they use to monetize the victim's action on the scam website (Source: Recorded Future)*

Stage Zero: Infrastructure Procurement

The first thing a threat actor must do to launch a scam website is obtain access to the resources, tools, and infrastructure that they will use as the bedrock for their operation.

- **Domains:** Threat actors must register domain names and find web hosting for their scam websites. They typically do this at scale, creating a roster of ready-to-go scam domains that can be deployed as old domains are reported and lose credibility or are taken down. When exploiting seasonal opportunities, threat actors leverage typosquatting — for example, to imitate the US Internal Revenue Service (IRS) in tax season or the US Postal Service (USPS) during holidays.
- **Phishing/scam kits:** On the dark web, threat actors with a knack for web development offer ready-to-go phishing and scam kits for sale to scam website operators. These kits expedite scam website setup for fraudsters, who use the kits as cookie-cutter templates to mass-produce scam websites. As with domains, phishing and scam kits often capitalize on seasonal events and holidays. Some kits are complete with live admin panels that allow threat actors to directly interact with (and defraud) their victims in real-time, specifically by intercepting one-time passwords (OTPs) to provision digital wallet card tokens or authenticate during 3-D Secure transactions.
- **Merchant accounts:** A growing number of scam websites abuse fraudulent merchant accounts, which threat actors must acquire and link to the website. This process usually requires bypassing payment processors' know-your-customer (KYC) screening and identity verification processes, measures mandated by government regulators to prevent money laundering and financial fraud. For threat actors who lack the expertise to bypass KYC screening, a cottage industry of third-party merchant account acquisition services on the dark web can still allow scam operators to acquire access to merchant accounts.
- **Traffic and advertising services:** Similar to phishing and scam kits, some third-party services on dark web sources offer web traffic as a service, using various means to drive visitors to malicious websites. Arranging support from these services allows threat actors to quickly supply their scam websites with victim leads. Scam website operators can also abuse legitimate online advertising services for the same end.
- **Knowledge:** Fraud and anti-fraud is a game of cat-and-mouse. To emerge on top, threat actors work in a fundamentally collaborative environment, sharing effective tactics, techniques, and procedures (TTPs) on the dark web to stay ahead of their adversaries. Many dark web sources offer scam website workflows, tutorials, and tips that help lower barriers to entry and increase impact for threat actors who may lack experience in scam website operations.

Examples of Scam Website Infrastructure Procurement

In the table below, we list three examples of threat actor offerings that can be used to support infrastructure procurement for scam website operations:

Threat Actor Offerings Related to Infrastructure Procurement
On September 17, 2024, a threat actor on a prominent dark web forum advertised the sale of ten fully verified US-based merchant accounts for $800. These accounts have allegedly passed comprehensive verification and include access to linked bank accounts under the account holder's name, a verified selfie, and full personal information with supporting documentation. This sales offer would likely grant threat actors the means to conduct fraudulent transactions disguised as legitimate business operations.
Since September 30, 2024, a threat actor on a prominent dark web forum has offered custom phishing kits that leverage reverse-proxy techniques. This service uses Evilginx3, a man-in-the-middle reverse-proxy attack framework marketed as a sophisticated phishing method that intercepts user sessions and bypasses multi-factor authentication (MFA). Unlike traditional phishing attacks that only capture victim inputs, this service is alleged to capture session cookies and provide full access to user sessions, allowing attackers to bypass additional security layers such as SMS- or authenticator-based MFA.
On October 1, 2024, a threat actor on a prominent dark web forum advertised a verification service for creating verified personal, business, and merchant accounts across various payment platforms. This service allegedly enables fraudsters to establish merchant accounts that appear authentic, facilitating illicit financial activities disguised as legitimate business operations.

Table 1: *The threat actor offerings in the table above are recent examples of scam-related infrastructure procurement activity (Source: Recorded Future Payment Fraud Intelligence)*

Another Perspective: Banks and Cardholders

Threat actor procurement occurs behind the scenes. Without cyber threat intelligence (CTI) assets capable of detecting threats upstream of the eventual fraud attack, banks have precious little insight into what is occurring at this stage, and cardholders know absolutely nothing.

Banks are not completely defenseless. Examples of CTI insight that could inform effective fraud action include monitoring previously identified scam domain clusters to detect newly registered domains that indicate the scam operator may be pivoting their operation to another seasonal opportunity. Additionally, monitoring dark web sources for offers of phishing and scam kits that target their financial institutions, impersonate popular merchants, or exploit seasonal openings could help operational and fraud teams tailor their strategies to proactively mitigate scam website impact.

Stages One and Two: Scam Lure Content and Delivery

Once a threat actor has acquired access to the requisite resources, tools, and services for their scam website operation, they must then begin distributing their scam websites to victims using lures. One way of looking at this is the beginning of a dark-side sales funnel, with the emphasis being on victim manipulation. For the threat actor, the key here is urgency and volume: their lures must be designed to entice as many victims to act in as short a timespan as possible, all before raising alarm bells.

Scam Lure Content

Threat actors use a variety of TTPs to generate urgency among victims, but the lure's content and adaptability often enable these varied TTPs to work. Threat actors tap into seasonal opportunities to model their scam lures on topics they think will generate urgent action among victims before a more critical examination helps the victim catch on.

Threat actors use various methods to generate urgency among victims, including the following:

- **Brand impersonation:** This perennial tactic allows threat actors committing scams to tap into victim trust for high-profile brands, helping lower their guard to avoid a more critical examination of the website's credibility.
- **High, limited-time discounts for attractive products:** Many shoppers take advantage of promotional offers, and a good discount on the right product can have them pulling out their cards before they realize an offer is too good to be true.
- **Fear through imitation of government agencies:** Particularly popular during tax filing season, this scam lure hook exploits the victim's fear of criminal or civil penalties to entice them to act.
- **Trending social topics:** Threat actors rapidly adopt new social trends to exploit victim bias and emotion — for example, through scam donation pages for political campaigns during elections or charities during humanitarian crises.
- **Updating account and financial information for common merchants and services:** Scam website operators use delayed package deliveries or tax refunds as pretextual hooks to request victims to update their information on the scam website.

Another Perspective: Banks and Cardholders

Banks can leverage CTI capabilities to perform brand monitoring that may provide insight at this stage of the scam attack chain. Mileage here may vary, especially when adapting brand monitoring capabilities to find scam websites imitating popular retailers rather than the institution itself. For cardholders, even if you are inherently suspicious of online advertisements or marketing communications, you are unlikely to know that a scam lure is nefarious based on content alone. Threat actors meticulously design their scam lures to exploit your psychology and spur you to action. They know when you are likely filing your taxes, shopping for deals with relaxed scrutiny and spending habits, and expecting deliveries. They model their lures after actual landing pages, marketing communications, and advertisements, and like search engine optimization (SEO) professionals, they tailor every word and image until it is effective.

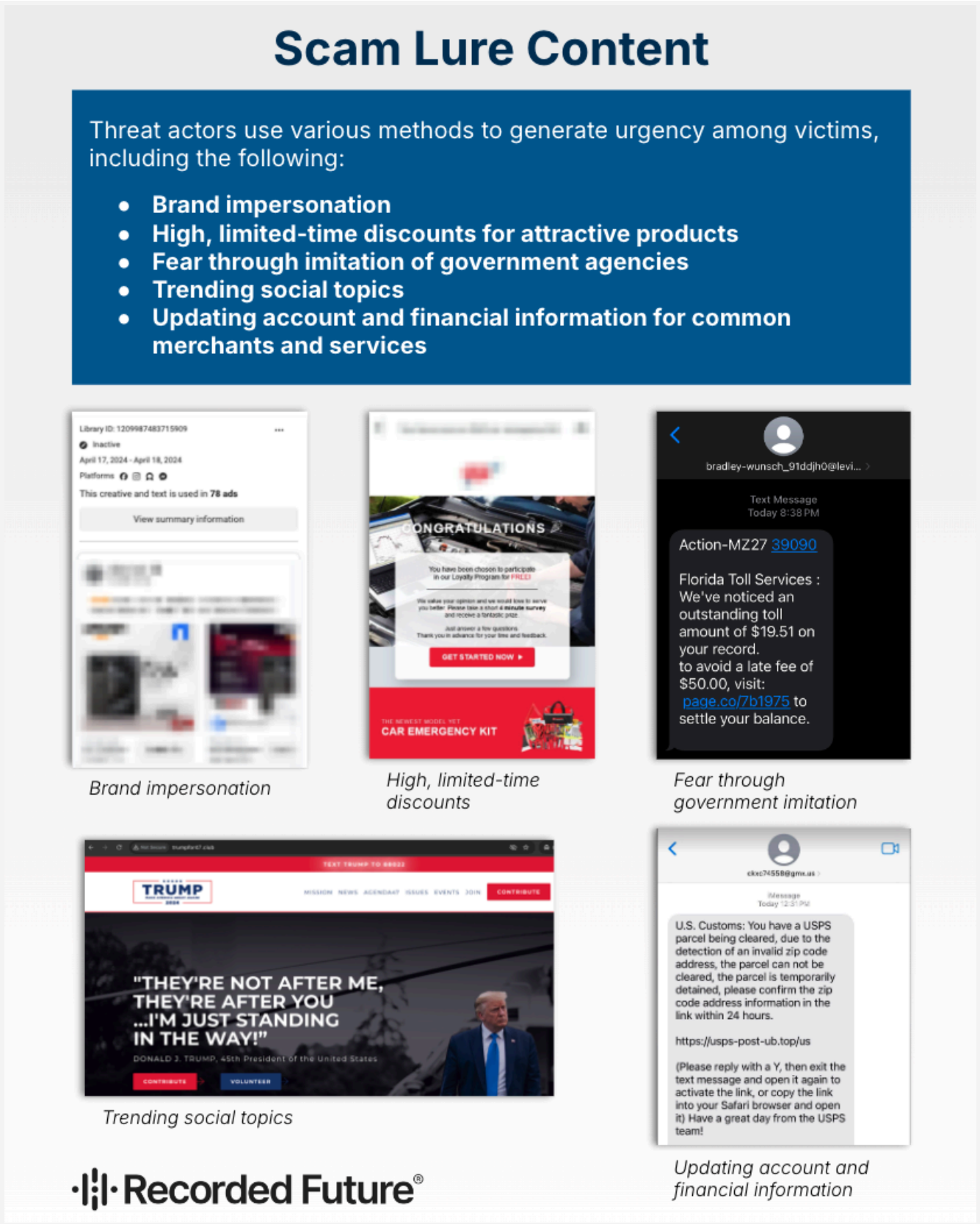


Figure 2: *Threat actors tailor the content of their scam lures to generate urgency among victims (Source: Recorded Future)*

Scam Lure Delivery

The scale of success for a scam website operation will always depend on the scam operator's ability to distribute their scam websites to as many victims as they can within a short period of time. Scam websites are typically short-lived because defrauded cardholders are quick to report the websites when they fail to receive the goods or services they purchased.

There are three primary methods for delivering scam lures to victims:

- **Ads on social media and search engines:** Threat actors tap into a sophisticated, fraud-focused malvertising ecosystem to deliver scam and phishing websites as well as malware. Third-party services compromise victims' online advertising accounts or payment cards and use these to fund fraudulent advertising campaigns that distribute scam websites. These scam websites compromise even more sensitive data, contributing to a vicious cycle. Online ads are advantageous because they can reach a wide audience with minimal targeting effort — specifically over social media or in promoted search results on popular search engines.
- **SMS and phone calls:** Smishing and vishing lures have grown increasingly common in the past year, especially for a recent smishing-based USPS scam website trend. Threat actors can use widely available phone number databases for victim targeting while spoofing their own phone numbers, obfuscating their true identity and intentions.
- **Emails:** Email is an "old faithful" among the varied means of delivering scam lures. Similar to phone numbers, cardholder email addresses are widely available for targeting, and a well-designed scam lure email is indistinguishable from a legitimate marketing email. Like phone numbers, email addresses can also be spoofed.

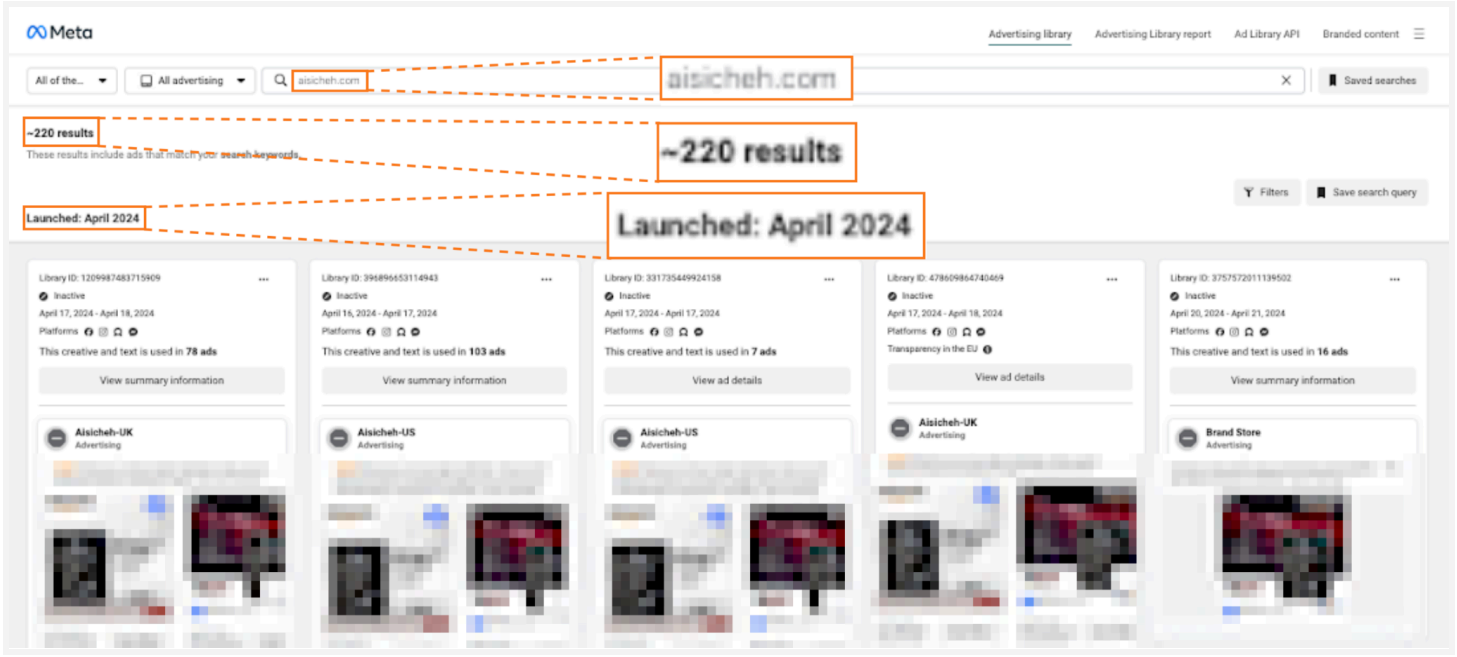


Figure 3: *The online advertising campaign for this ERIAKOS scam website included 220 ads (Source: Recorded Future)*

Another Perspective: Cardholders

While online advertising and remote communications are rife with malicious activity, they are not exclusively used to deliver scam lures. The reality is that most of us have received far more legitimate offers and communications via these channels than scam lures. Many of us are likely predisposed to trust what we see in social media ads and search engine results, for example — especially since the scam lure content threat actors use is common among legitimate entities, who employ many of the same methods to promote their goods and services.

Examples of Scam Lure Content and Delivery

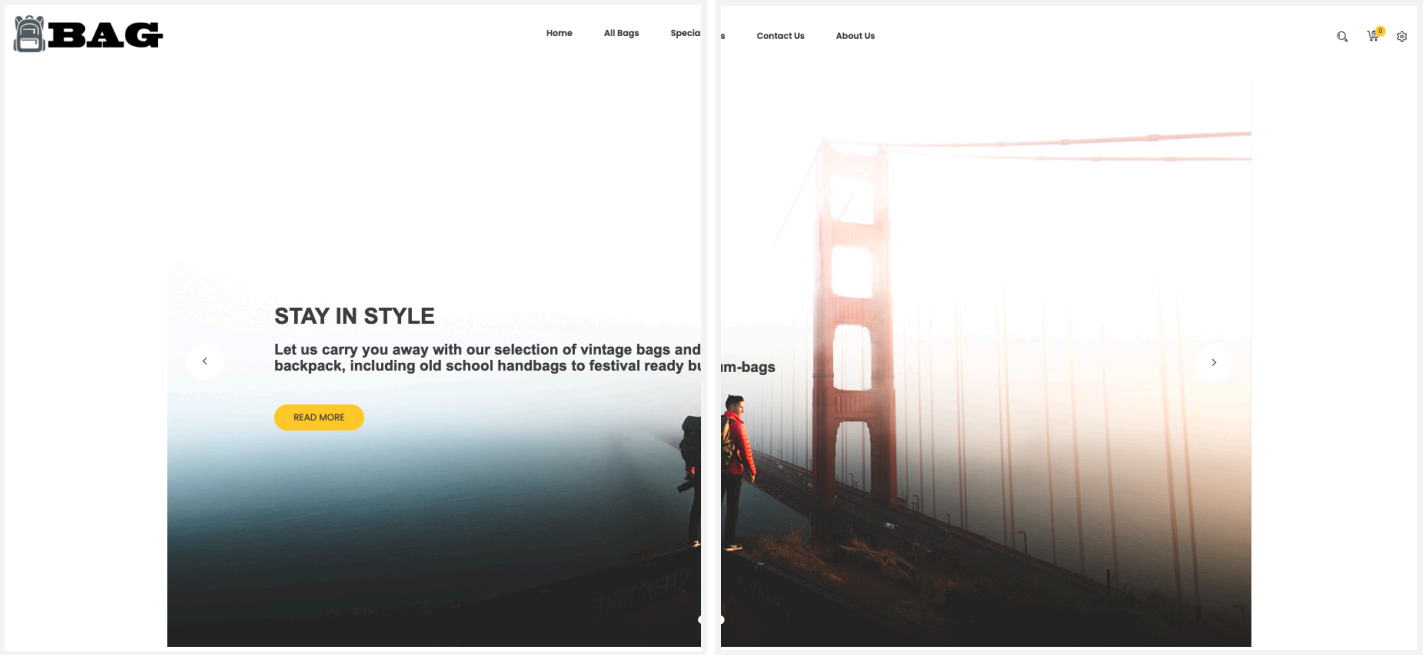
In the table below, we list two examples of threat actor offerings that can be used to support scam lure content and delivery for scam website operations:

Threat Actor Offerings Related to Scam Lure Content and Delivery
On July 23, 2024, a threat actor on a dark web forum claimed that they were actively spamming Spanish victims using a customized sender ID for Spanish banks. "Sender ID" refers to a recognizable or custom sender name that appears as a name or phone number when sending spam messages, usually via text message or email. The sender ID often mimics a legitimate entity, such as a bank or service provider. The use of a customized sender ID can make messages appear more trustworthy, increasing the likelihood that recipients will open them or follow any embedded instructions.
On October 15, 2024, a threat actor on a dark web forum advertised the sale of high-quality HTML templates for email spam intended for threat actors operating scam websites who require reliable traffic through one-time or mass email distribution. These HTML letters are designed to closely mimic the appearance of legitimate emails, complicating recipients' ability to detect the deception and increasing the likelihood that they will click on links embedded in the message. The offering includes several features to optimize deliverability and effectiveness: a customized "trust legend" to enhance credibility, high-quality design, anti-spam coding, text encryption, and randomization to avoid spam filters.

Table 2: *The threat actor offerings in the table above offer recent examples of activity pertaining to scam lure content and delivery (Source: Recorded Future Payment Fraud Intelligence)*

Stage Three and Four: Scam Websites and Payment Forms

Once victims enter the scam funnel through the lure, the scam website itself forms the remainder of the funnel, terminating in a payment form or account information update form that the entire scam pipeline has been built to support. To a large degree, the actual design of the scam website is superficial: the scam website will likely make use of the same scam lure design principles we outlined above, but as long as it is convincing enough to keep the victim progressing to the final input form, it will likely be effective.



Figures 4 and 5: *As long as scam websites are convincing enough to propel victims through the attack pipeline, their design is a superficial concern. These two scam websites both used identical designs and were linked to fraudulent credit card transactions. (Source: Recorded Future, partner financial institution)*

Similarly, on the surface, the input forms of any scam website operation will not largely differ from each other, offering victims the ability to enter personal or financial account data. However, while the layout of scam websites and payment forms may appear indistinguishable, their underlying functionality usually reflects strategic decisions the threat actor has made that determine how the victim's data will be monetized — and by extension, what ability the bank has to detect and prevent downstream fraud. Threat actors have multiple, flexible monetization avenues for their scam websites, and these must be built into the design of the scam website operation. In other words, a scam website's monetization path will determine its functionality.

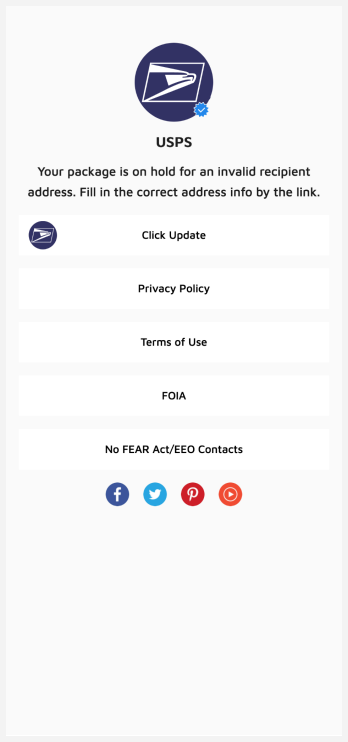


Figure 5: *A USPS-based smishing lure redirected victims to this scam website landing page (Source: Recorded Future)*

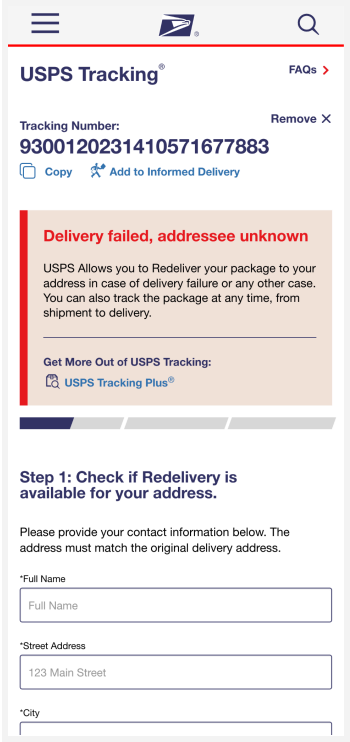


Figure 6: *Proceeding through the scam landing page brings victims to a data input form (Source: Recorded Future)*

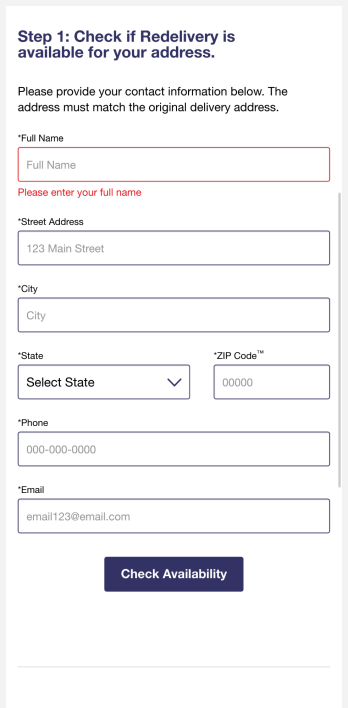


Figure 7: *The scam website requests victims to input data under the pretext of updating shipping information (Source: Recorded Future)*

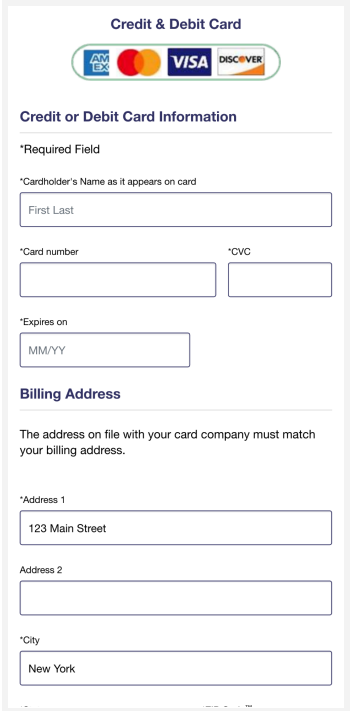


Figure 8: *After inputting their data, victims are directed to make a payment (Source: Recorded Future)*

Pure Phishing: CNP Fraud and Dark Web Sales

Scam websites that use pure phishing tactics to steal customer data likely offer threat actors several advantages at the cost of certain trade-offs. Upon successful data theft, the scam operators can directly commit card-not-present (CNP) fraud and other downstream fraud attacks with the stolen data or post the stolen data for sale on dark web sources. The second approach allows the scam operator to focus on the effectiveness of their scam websites without concern of detection by the bank — all while magnifying the fraud attack surface for the exposed data.

Pure Phishing: Pros	Pure Phishing: Cons
• Input forms can be tailored to steal any data field, including card security code (CSC, commonly known as card verification value, or CVV). • Websites require minimal configuration. • Compromise via phishing is undetectable by bank anti-fraud systems. • Stolen data can be used for card-not-present (CNP) fraud or sold on dark web sources. • Posting cards for sale allows threat actors to safely overlook detection concerns, pushing monetization barriers downstream to another threat actor.	• CNP fraud monetization requires a substantial time investment. • For scam websites purporting to sell goods or services, the absence of a corresponding transaction could clue in victims that their data has been stolen.

Table 3: *Scam websites that use pure phishing tactics are simple and reliable at the cost of monetization and detection trade-offs (Source: Recorded Future)*

Another Perspective: Banks

Pure phishing is a relatively simple activity that minimizes detection opportunities for banks. Anti-fraud teams at banks scan for phishing websites or likely phishing domains that target their institutions, but if a threat actor's scam website is modeled after a legitimate e-commerce website, the operation will likely remain undetected until downstream fraud occurs later in the attack chain.

Although reliable for threat actors, the use of pure phishing does create one opening for defenders: cardholders may notice the absence of a corresponding transaction in their card management account activity for scam websites modeled after e-commerce websites. Canny cardholders noticing this may inform their financial institutions, providing an opportunity for anti-fraud teams to proactively remediate downstream fraud activity.

Live Admin Panels: Higher Success Rate during CNP Fraud for Authorized Transactions

The use of live admin panels with scam websites helps buttress detection weaknesses that occur when monetizing phished data, but the cost is a higher resource demand and more configuration effort. Live admin panels combine the data compromise and monetization into a single, integrated workflow that makes remediation nearly impossible without timely upstream intelligence.

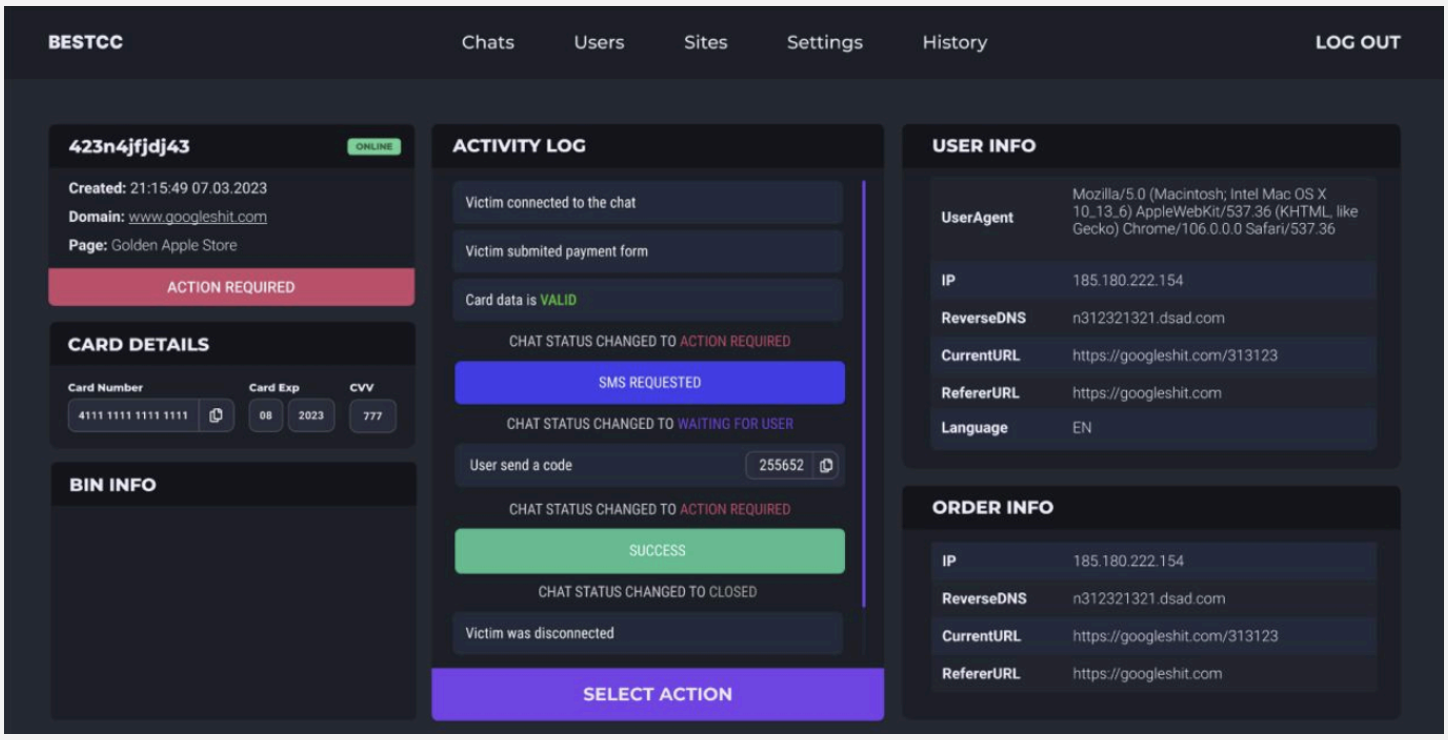
The increased effort and resource demands of operating live admin panels are not for nothing: an effective variation of scam websites combines live admin panels with mobile wallet fraud to conduct CNP fraud at a high success rate. Live admin panels enable threat actors to simultaneously compromise card data, intercept the OTPs necessary to fraudulently provision the card to a digital wallet under the fraudster's control, and monetize the data by intercepting another OTP to approve a fraudulent transaction.

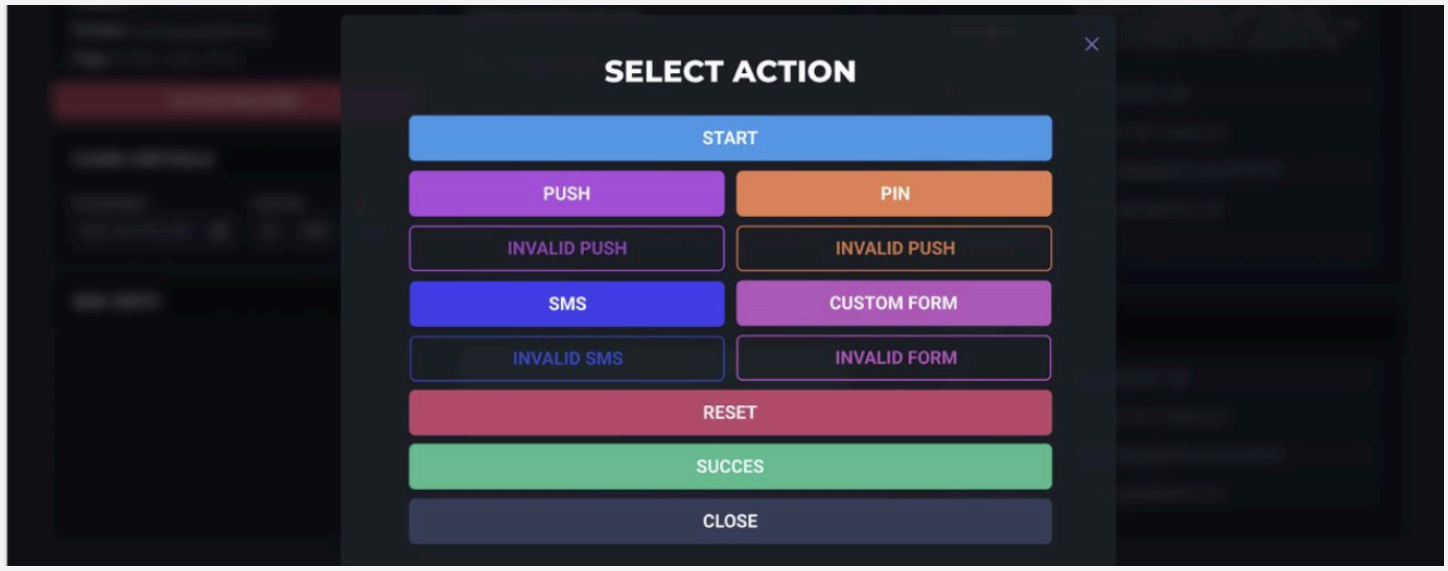
Live Admin Panel: Pros	Live Admin Panel: Cons
• Input forms can be tailored to steal any data field, including card security code (CSC, commonly known as card verification value, or CVV). • Input forms can be tailored to steal MFA codes, including OTPs necessary to authorize transactions and provision accounts to mobile wallets. • Financial institutions have difficulty identifying fraud originating from cards that have been fraudulently provisioned to mobile wallets via live panels. • Thanks to MFA bypass, stolen data can be used for card-not-present (CNP) fraud with a higher success rate.	• The cardholder will almost certainly identify and report the fraudulent transaction when they fail to receive their purchase. • Panel-capable phishing kits may require additional investment from the threat actor during procurement. • Websites require additional configuration. • The threat actor may need to operate the panel in real-time.

Table 4: *Live admin panels on scam websites reinforce some of the weaknesses of pure phishing attacks in return for higher operational demands (Source: Recorded Future)*

Another Perspective: Banks

Live admin panels entail simultaneous card compromise and monetization that makes fraud detection and prevention highly difficult. From a fraud analyst's point of view, even if a transaction is suspicious, successful (though fraudulent) authentication via an intercepted OTP would likely make the transaction appear legitimate, if unusual.





Figures 9 and 10: *A threat group offers a streamlined phishing panel that can be used to facilitate man-in-the-middle fraud transactions, including on scam websites (Source: Recorded Future)*

Fraudulent Merchant Account: Immediate Monetization, CNP Fraud, and Dark Web Sales

A scam website operational method that has gained steam in recent years involves threat actors registering fraudulent merchant accounts (which often stand behind dummy companies) and linking them to scam websites. This approach allows threat actors to achieve a "one-two punch": first, immediate monetization of inputted victim data through a fraudulent transaction on the merchant account, and then downstream resale of the victim data on dark web sources. Some scam websites also include fine print to justify recurring charges (via a subscription scam) against the victim's account, which is likely intended to complicate fraud investigations arising from victims' complaints.

More sophisticated scam website groups use payment cloaking that enables threat actors to process transactions and obfuscate transaction sources without accessing client information directly. These groups operate two scam website clusters — an "A" pool of scam websites and a separate "B" pool of websites connected to merchant accounts — with a plugin that transfers data between them. This cloaking method enables threat actors to connect merchant accounts to scam websites on an ad hoc basis to enhance threat actors' ability to avoid detection, route regional users to specific merchant accounts, and connect B-pool websites to phishing pages that link stolen card data to digital wallets.

Fraudulent Merchant Account: Pros	Fraudulent Merchant Account: Cons

• Double-monetization:
  ○ Linked merchant account allows for immediate (and recurring) monetization through fraudulent transactions.
  ○ Access to the merchant account data allows the threat actor to commit downstream CNP fraud or sell victim card data on dark web sources.
• Misleading terms on the website can complicate fraud investigations or discourage cardholders from reporting fraud.
• A lack of obvious connections between the scam lure, scam website, and merchant account can complicate fraud investigations or discourage cardholders from reporting fraud.
	• Registering merchant accounts and bypassing KYC verification require substantial effort and resources.
	• Merchant account data offers banks an ironclad method to detect and prevent fraudulent transactions once the scam merchant account is identified.
	• The cardholder may report the fraudulent transaction when they fail to receive their purchase.

Table 5: *While linking fraudulent merchant accounts to scam websites is likely the most resource-intensive of the scam methods, it ensures a minimum return through immediate — or recurring — fraudulent transactions (Source: Recorded Future)*

Another Perspective: Banks

Of all the scam attack methods described in this report, the use of merchant accounts falls most squarely in the gunsights of banks' anti-fraud assets. The presence of merchant account data means that after banks identify fraudulent merchant accounts involved in scam activity (through customer reporting, for example), they can blocklist those accounts and prevent additional fraud.

However, if a scam website operator has identified a reliable workflow to alter merchant account data or exploits sloppy KYC onboarding procedures to frequently register merchant accounts, blocklisting scam merchants may become a game of whack-a-mole. In these cases, anti-fraud teams cannot proactively detect and prevent scam activity without timely upstream intelligence. Additionally, as with phishing, the possible downstream sale of compromised data on dark web sources expands the fraud attack surface for victims, further exposing the bank's customer to attack.

Examples of Scam Websites and Payment Forms

In the table below, we list two examples of threat actor offerings that can be used to support scam websites and payment forms for scam website operations:

Threat Actor Offerings Related to Scam Websites and Payment Forms
Since September 2020, a threat actor on a prominent dark web forum has offered to sell access to a phishing toolset. The threat actor claims this toolset is for penetration testing and demonstrating vulnerabilities; however, the toolset likely has a high potential for abuse. The phishing toolset was developed to resemble legitimate websites in order to steal victim login credentials, email addresses, and other personally identifiable information (PII). The threat actor uploaded examples of these phishing websites and how they operate via a GIF image within the forum thread. Within the examples, the threat actor demonstrates how the toolset and its panel work, how information is collected, and how the phishing websites are displayed for victims.
On October 22, 2024, a threat actor on a prominent dark web forum advertised the sale of custom-built scam pages designed to impersonate well-known brands. These pages are designed to deceive victims by imitating target websites. According to the seller, the scam pages are highly customizable, featuring an admin dashboard and query parameters to adjust various settings. Additionally, the threat actor offers personalized targeting options, enabling the display of user-specific details such as names and pre-filled addresses, which can increase trust and improve the scam's effectiveness in capturing sensitive information, such as credit card details and OTPs for linking cards to digital wallets.

Table 6: *The two threat actor offerings in the table above offer recent examples of activity pertaining to scam websites and payment forms (Source: Recorded Future Payment Fraud Intelligence)*

Mitigations

- Solicit scam website leads from your customers to identify scam groups that pose a threat to your customer base. Engagement with customers is crucial to identify scam websites such as those identified in this report, which primarily target users on social media and employ various methods to reduce the likelihood that victims will report them as scams.
- Provide scam website leads to your CTI assets or Recorded Future Payment Fraud Intelligence to identify related scam websites that may pose a risk to your customers. Early information sharing is crucial to determine the scope and threat level posed by scams.
- Review fraud intelligence reporting to stay abreast of trending scam threats to your customers and your organization. Adjust your detection strategies accordingly.
- Share common elements for identified scam website operations with your customers and encourage them to avoid interacting with these websites.
- Leverage Recorded Future Payment Fraud intelligence (PFI) to detect and mitigate possible scam websites using the PFI common-point-of-purchase (CPP) dataset.
- Leverage Recorded Future Brand Intelligence to detect and mitigate brand impersonation threats common among scam websites.

Scam websites pose a direct risk to financial institutions' customers. To reduce this risk, encourage your customers to apply the following mitigation strategies:

- Only provide personal and payment information on secure, trusted websites.
- Research companies before you make purchases from them. Review complaints on the Better Business Bureau's (BBB) official website, ask trusted sources, or perform a web search 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.
- Be wary of unsolicited communications or advertisements. Scam operators frequently use social media advertisements or other online 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 the BBB and dispute losses to attempt to recover your funds through chargebacks.

Outlook

Looking forward, our analysis of scam website operations indicates that the fraud strategy is undergoing a rapid evolution reminiscent of the early development of Magecart e-skimmer TTPs. The sophistication of these TTPs is impressive. In July 2024, the ERIAKOS scam campaign deployed scam websites that were only accessible on mobile devices and via scam lures — a tactic likely intended to reduce the odds of detection by automated scanners. Another scam website operation consisting of 348 scam websites likely used low-value initial transactions approved by the cardholder to establish a transaction history that would enable the threat actor to complete downstream, recurring high-value transactions.

The development of linked, fraudulently registered merchant accounts for scam websites is one such innovation and is likely here to stay. The merchant account scam website tactic is equally effective when targeting US cardholders and cardholders in other jurisdictions, who may be protected by more stringent payments and data security regulations that invalidate other fraud attack vectors. For this reason, the use of linked merchant accounts with scam websites is likely to grow more prominent in the future, and threat actors may begin to increasingly rely on the tactic after future-dated PCI-DSS v4.0 requirements — which will likely complicate Magecart e-skimmer attacks, a popular CNP card compromise method — become mandatory in 2025.

Regulatory protections will likely moderate the threat actors' ability to successfully conduct scam website operations. For example, in October 2024, the US Federal Trade Commission introduced a "click-to-cancel" rule designed to make canceling subscriptions as easy as beginning them, which would likely hamper threat actors' ability to conduct subscription scams. Similar anti-money laundering and KYC regulations applied to a single standard across the payments ecosystem would likely hamstring threat actors' ability to fraudulently register merchant accounts used for scam websites, as our analysis indicates these merchant accounts tend to be associated with a handful of merchant acquirers, indicating sloppy KYC onboarding may be to blame. Closing these loopholes — especially in jurisdictions that lack robust KYC regulations — would vastly complicate scammers' ability to operate merchant accounts.

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 Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com