THREAT VECTOR DOSSIER: INSIDE THE DARK WEB'S BANKING FRAUD ECONOMY

New research and analysis from the Arkose Labs ACTIR unit reveals how bad actors are targeting banks and their customers, infiltrating high value accounts even in the face of stringent security measures.

Cybercriminals use similar tactics and patterns across all attacks on banks. By examining specific examples, the ACTIR unit is shedding light on the latest tactics of the fraudsters orchestrating these attacks.

OVERVIEW

For financially motivated fraudsters, banks are top targets. Recent dark web marketplace activity shows that bad actors are upping their game, targeting banks and their customers with increasingly sophisticated attacks designed to circumvent multi-factor authentication (MFA) and KYC (know-your-customer) protocols.

Phishing remains the primary initial access vector for banking fraud, and today's reverse-proxy phishing scams are more convincing than those used in the past. In these attacks, the scammer positions themselves between the customer and bank, posing as the financial institution in order to intercept an MFA token in real-time, gaining access to the customer's account before they even realize they have been scammed. Phishing emails are also becoming increasingly sophisticated, with many fraudsters utilizing AI to craft emails that appear legitimate.

Phishing-as-a-service (PhAAS) toolkits are lowering the barrier of entry to cybercrime, requiring minimal technical knowledge to deploy. Fraudsters can acquire ready-made phishing templates, and some vendors even offer professional support and customization services. Tools such as the TOMATO auto-phishing tool offer URL masking and multi platform support, priced at $19.99.

In some cases, ACTIR sees bad actors target elderly people specifically, working with the assumption that older consumers might be more likely to fall prey to a spoofed website or phishing email. Beyond phishing kits and phishing email templates, fraudsters are also buying and selling tutorials, designed to teach cybercriminals about bypassing security measures and intercepting information.

> What we're seeing is that attackers spend time researching banks first looking for potential weaknesses and gaps in security before they buy phishing toolkits or build new ones for that particular use. They research potential data (leaked or openly available) related to the bank and then target those accounts initially.
>
> **— ACTIR threat researcher**

The ACTIR unit has uncovered lists of cybercrime-as-a-service (CaaS) offerings from active vendors with positive reviews, including details on the bank and account type targeted. This analysis found that account compromises which target businesses rather than individuals typically command higher prices, with vendors on the dark web specifically targeting accounts with ACH capabilities, BillPay access, Zelle transfer functionality and Interac (in Canada). ACTIR estimates that the damage to the banking industry from these crimes runs into the hundreds of millions of dollars.

Beyond phishing scams and attacks targeting KYC flows, fraudsters also use credential stuffing attacks at scale to gain access to customer accounts, and open fraudulent accounts to launder money or facilitate further attacks against financial institutions.

A GLOBAL PROBLEM

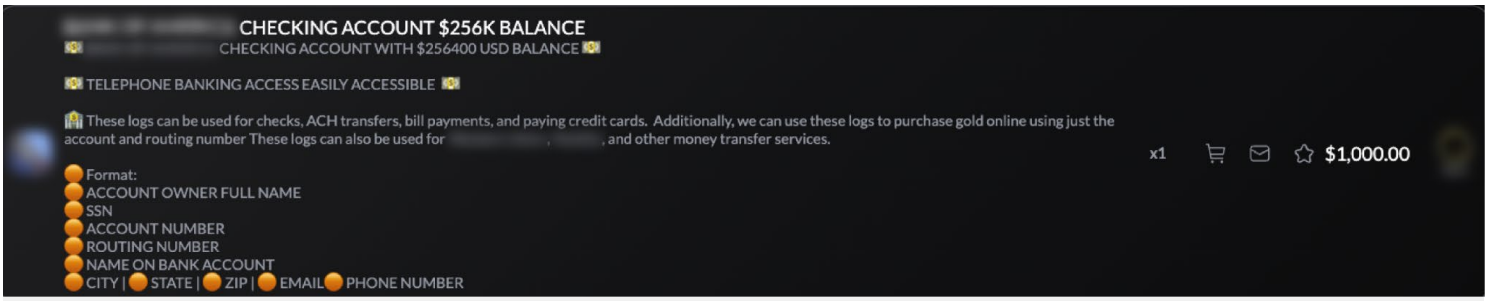
In the research conducted by ACTIR, chatter on the dark web showed more evidence of fraud against American banks than European ones. A possible explanation for this is the higher barrier of entry for attacking in Europe. Under the revised Payment Services Directive, there are stricter security requirements for online transactions. This means that financial institutions are increasing their use of OTPs, to comply with the strong customer authentication regulatory standards.

And yet, attacks are still rife, and kits are available to help fraudsters to skirt around a bank's specific defenses. As security standards increase, criminals are ever ready to pivot to new techniques. Advanced phishlets and OTP bots are used by bad actors seeking to defraud banking customers in Europe. Using Discord and Telegram infrastructure, OTP interception bots can automatically call victims posing as legitimate bank representatives. These bots use services like Snapchat to mask caller identification and social engineer victims into revealing authentication codes.

U.S. EXAMPLES

ACTIR has observed a sophisticated and evolving ecosystem of phishing attacks targeting several major U.S. banks. Evidence from multiple underground marketplaces demonstrates the availability of comprehensive attack toolkits, compromised accounts and automated systems designed to bypass security measures. For business accounts for a major U.S. bank, the ACTIR unit found that fraudsters were charging $300, while the same service for several U.S. retail banks cost around $160.

Vendors on an underground marketplace are selling scam pages that can be used to steal email access credentials and security questions. These pages are professionally designed to mimic legitimate banking interfaces, priced at approximately $62.40 USD.

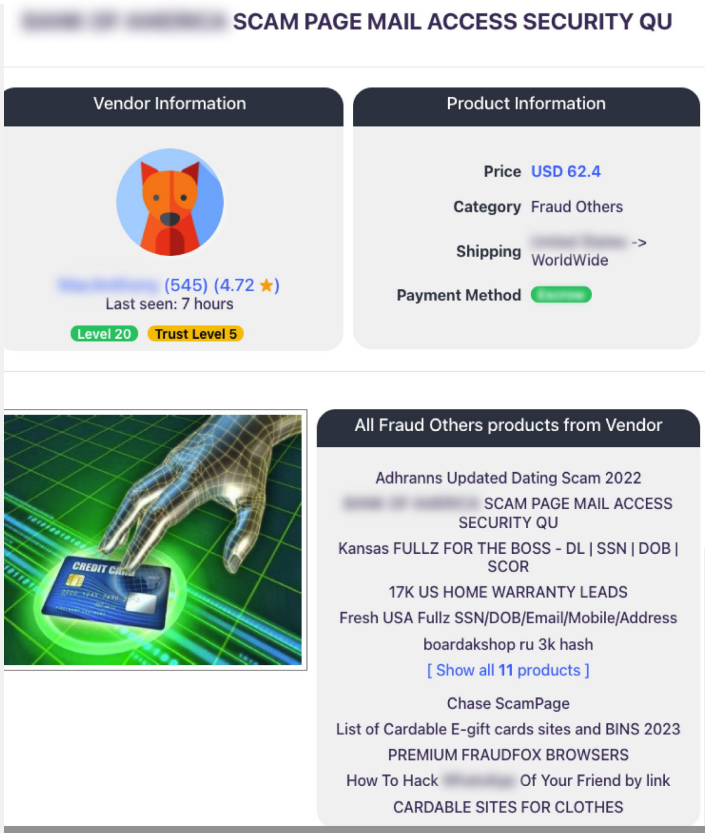


High balance account sale

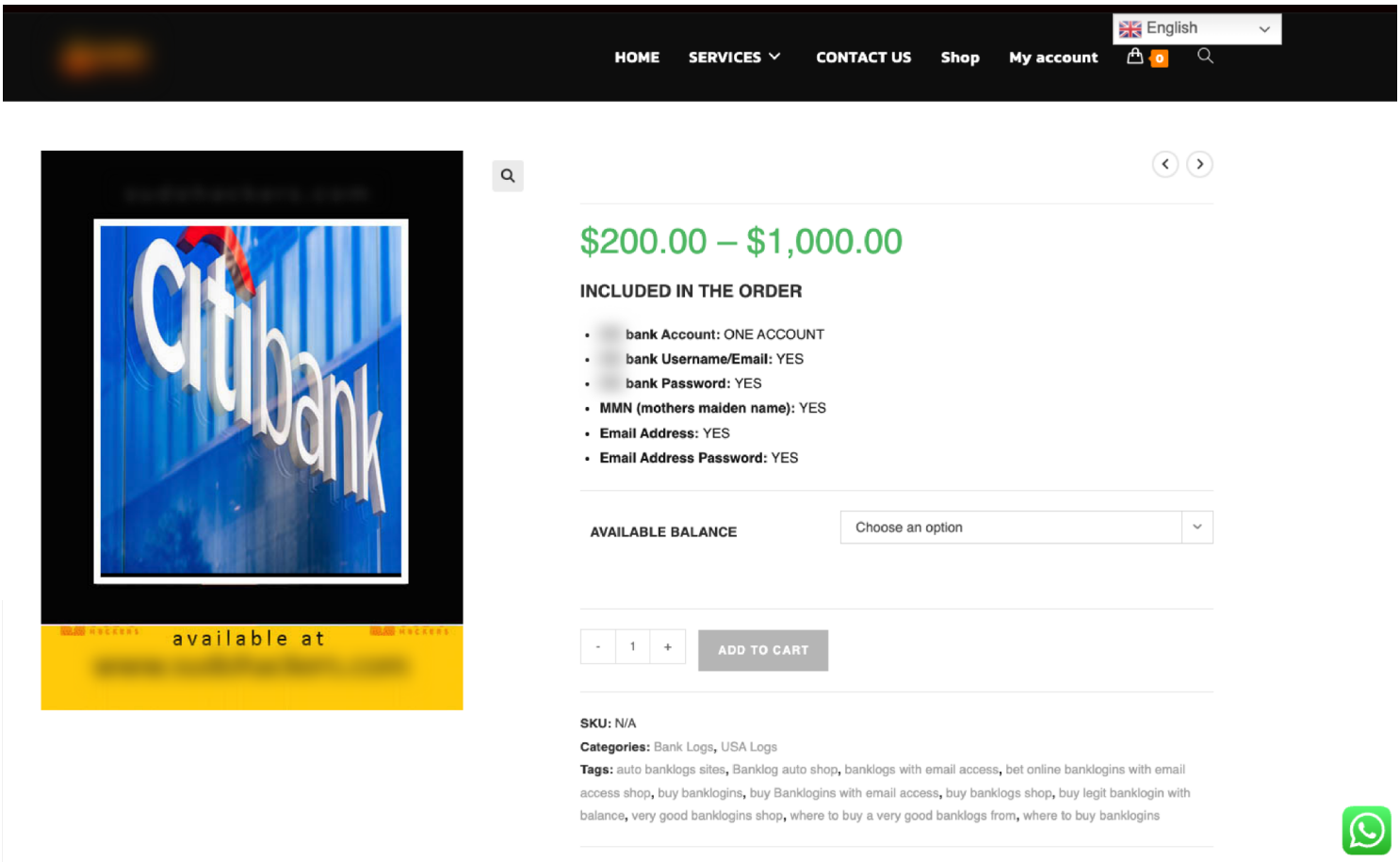
Multiple vendors offer personal account access for a major bank, ranging from $300-500, with some accounts containing balances up to $256,000 according to listings on an underground marketplace that is primarily focused on financial services.

A shop that operates on the underground financial services marketplace offers a complete identity package for the same bank, including email access and passwords for $48. These “fullz” packages, which include all of the PII data needed to launch an attack, enable account takeover and identity theft.

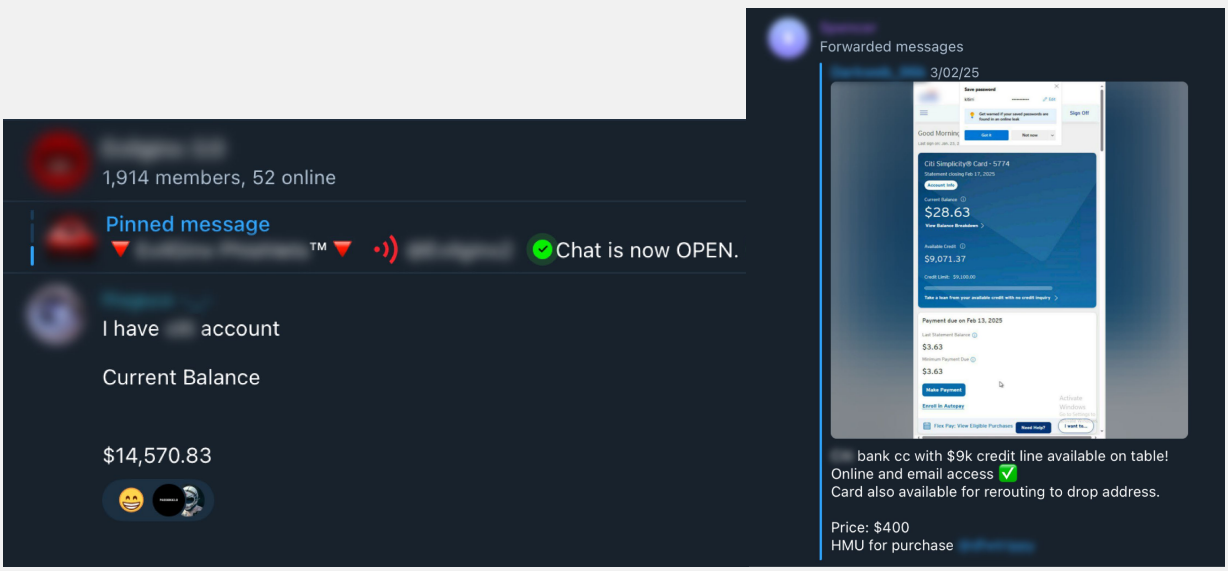
ACTIR has found phishlets designed for targeting customers of another major US bank. Phishlets are pre-built templates used to proxy real websites in adversary-in-the-middle phishing attacks. These are sold by known providers of cybercrime-as-a-service tools, including Modlishka and EvilGinx. Some providers are playing a role in training new entrants to fraud. For example, on the Sudo Hackers website, they offer a service entitled “Professional Masterclass Course (for Noobs).”



Phishing Page Sale



One website offers a course for fraud newbies



Successfully phished accounts are sold on the dark web

USING AI TO BEAT KYC CHECKS

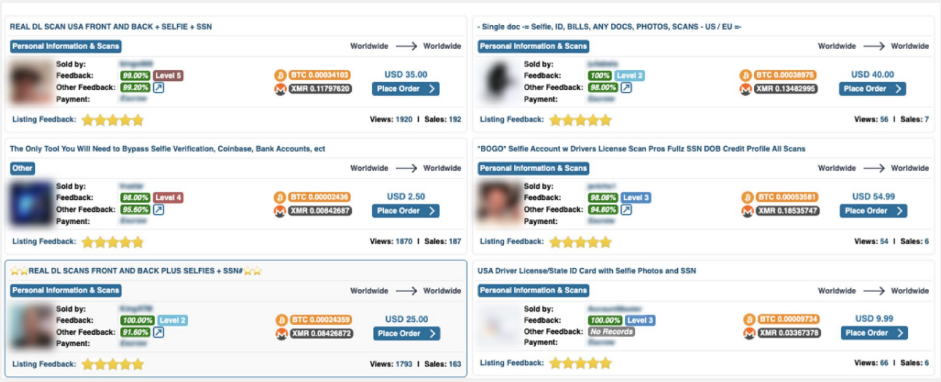
Cybercriminals use AI to quickly create false documents to help them to clear a bank's verification process. On the dark web, fraudsters are selling document templates to help others to clear KYC. Some marketplaces are solely focused on selling counterfeit passports and official documents.

In some cases, scammers are acquiring customer names that are posted on the dark web following data leaks, searching social media for photos and relevant information before using ChatGPT or a similar tool to create a fake identity document. Then, they might either use the false document for their own attack, or sell it online.

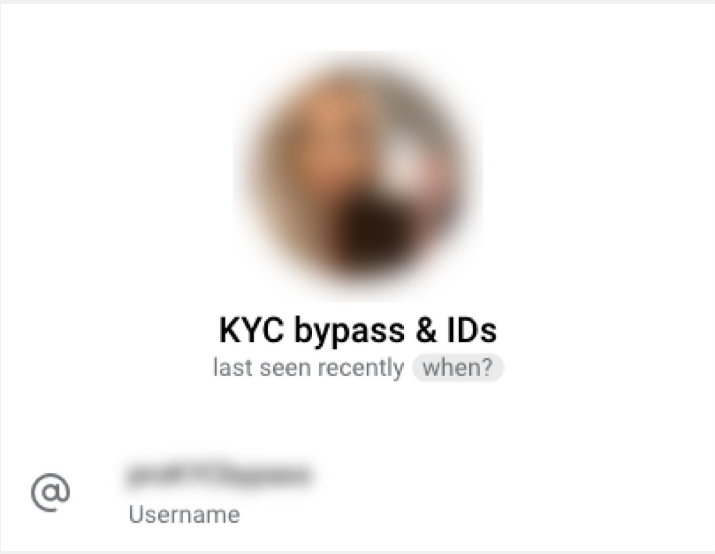
But sometimes, there's a higher barrier for entry. KYC liveness checks are designed to confirm that the person attempting to get verified is a real person. It's a measure designed to combat fraud, confirming the live presence of the individual during the verification. Fraudsters are using AI to spoof this process. With access to just an identity document such as a driving license, bad actors can mimic the face of the customer and use 3D scanning to create a deepfake video.

> Attackers can buy fake documents online and use them to trick the camera during liveness checks. We found multiple vendors offering these services on the dark web.
>
> **- ACTIR Threat Researcher**

Pricing for this enhanced KYC service varies by bank and account type. In some cases, it appears that the scammers are scamming other scammers: sellers are collecting money without providing the service.



Dark web sales of selfie verification services



Telegram channel claiming to provide selfie bypass

Bank statements are sometimes required as part of the KYC process, and templates for these are also sold on the dark web. The ACTIR unit found that for one major bank headquartered in the UK, statement templates were sold for between $5 and $50.

PRICING

Pricing for the services and products designed for cybercrime against banks varies depending on the institution and intent. And while costs might fluctuate by precise use case and target, the continued prevalence of these attacks is evidence that the dollars and cents work in the favor of the fraudsters. The ACTIR team's research demonstrates that for two-figure and low three-figure sums, fraudsters have ready access to tools that facilitate highly lucrative scams.

To recap, here's a summary of what a cybercriminal might expect to spend:

Less than $50	Less than $100	Between $100 and $250	Less than $500	More than $500
Phishing tool	A phishing page kit for major U.S. banks	KYC service for personal banking and investment accounts	Access to personal accounts with lower balances	Access to higher value personal and business accounts (with some balances as high as $256,000)
A "fullz" identity package containing valuable PII data				

ABATEMENT

Financial institutions seeking to protect their clients from fraud should maintain active surveillance for leaked credentials, and alert users promptly when their information appears in compromised datasets.

By implementing enhanced bot protection with advanced CAPTCHA and behavioral analysis, banks can dramatically reduce automated credential stuffing attacks, which are often the point of entry for fraudsters. And as fraudsters increasingly look to AI to streamline and supercharge their attacks against financial institutions and other companies, so too should businesses seek to adopt AI-powered cybersecurity solutions.

RECOMMENDATIONS

- **Implement Proactive Dark Web Monitoring and Threat Intelligence:** Establish continuous surveillance of underground marketplaces where banking credentials and attack toolkits are traded, with automated alerts when customer data appears in compromised datasets.
- **Deploy Advanced Anti-Phishing and Bot Detection Technologies:** Integrate reverse-proxy detection capabilities and behavioral analysis systems to identify real-time phishing attempts and prevent automated credential stuffing attacks.
- **Strengthen Multi-Factor Authentication with Phishing-Resistant Methods:** Transition to FIDO2/WebAuthn tokens or certificate-based authentication that cannot be intercepted by reverse-proxy phishing attacks.
- **Enhance KYC Processes with AI-Aware Liveness Detection:** Upgrade identity verification systems to detect AI-generated documents and deepfake videos, implementing multi-modal biometric verification and document forensics.

CONCLUSION

The banking sector faces an industrialized fraud ecosystem where cybercriminals operate sophisticated marketplaces targeting financial institutions with hundreds of millions in damages. The commoditization of banking-specific attack tools—from $19.99 phishing kits to AI-powered KYC bypass services—has democratized cybercrime, enabling low-skilled actors to execute advanced attacks against even security-conscious banks.

The emergence of real-time MFA interception, AI-generated document forgery, and deepfake technology for liveness detection represents a fundamental shift that traditional security controls cannot address. These are not random attacks but calculated operations with clear pricing tiers: business accounts command $300 while retail accounts sell for $160, demonstrating the organized, professional nature of modern banking fraud.

For CISOs and their teams, success requires adaptive defense strategies that evolve as rapidly as the threats themselves. The scale and sophistication of these industrialized fraud operations demands intelligence-driven, proactive security measures rather than reactive controls. Financial institutions must anticipate and neutralize threats before they impact customers and institutional assets, or risk both significant financial losses and the erosion of customer trust that forms the foundation of banking relationships.

ABOUT ACTIR

Arkose Cyber Threat Intelligence Research (ACTIR) unit is a dedicated and specialized counterintelligence team embedded in Arkose Labs. Composed of full-time experts in cyber threat analysis, digital forensics and cybersecurity operations, ACTIR's primary mission is to identify, assess, and neutralize sophisticated cyber threats. By leveraging cutting-edge technologies and methodologies, ACTIR provides actionable intelligence and orchestrates coordinated responses to mitigate threats posed by entities like Greasy Opal. Recently it partnered with Microsoft DCU and law enforcement to disrupt Vietnamese threat actor group Storm-1152. Through collaboration with Arkose Labs' award-winning SOC, ACTIR plays a pivotal role in enhancing the cybersecurity posture and ensuring the integrity of the digital infrastructure of Fortune 500, category leading enterprises, and trailblazing businesses. Access ACTIR's threat research taxonomy.

Contact ACTIR to discuss these insights: actir@arkoselabs.com

Media Contact

Cassie Stevenson
Arkose Labs
Global Head of Brand, Content and Communications
c.stevenson@arkoselabs.com