Report | January 2026

The Rise of Fake Banks in USA & UK

Analysis by CTM360

CTM360®

INDUSTRY	COUNTRY	REGION	DATE
BFSI	US - UK	NA & EU	18-01-2026

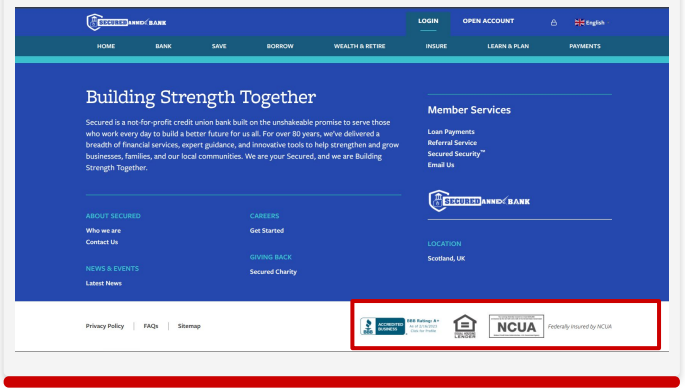
OVERVIEW :

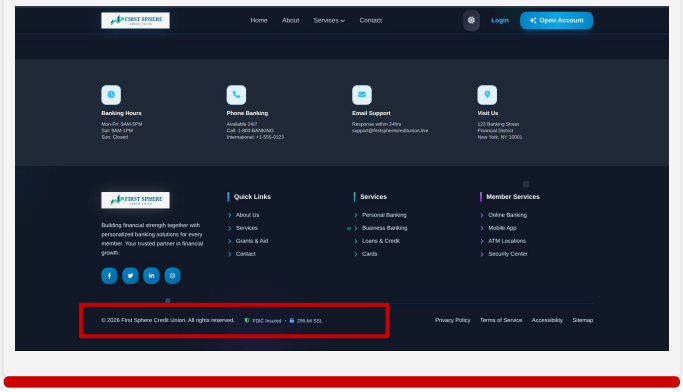
As the digital landscape evolves, fake financial institutions are becoming increasingly sophisticated. These fake entities pose as legitimate banks or lenders despite having no legal authorization, regulatory approval, or physical presence. **CTM360** has identified an ongoing fraudulent campaign and we have named it **Fake Banks**. The growth of fake banks is a global trend, with more cases expected to emerge targeting other regions. This report focuses on an ongoing campaign targeting users in the **United States** and **United Kingdom,** where region-specific regulatory impersonation is used to enhance credibility. Fraudulent bank websites often display fake regulatory approvals to appear legitimate.

They operate entirely online through cloned, fully functional websites that mimic real banking platforms and claim to provide services such as loans, mortgages, grants and promising higher credit card limits without approval. Many of these fraudulent sites are optimized for search engines, allowing them to appear in legitimate search results and increasing their visibility to potential victims.

This fraud falls under the category of **Advance Fee Fraud**, where the primary objective is to deceive individuals into depositing money or revealing sensitive information. The threat actor rely heavily on social engineering, often engaging victims through integrated live-chat support or instant messaging to create a false sense of credibility.

Account creation is deliberately designed to be simple, requiring minimal verification. Once an account is created, victims are pressured to provide personal or banking information. A common tactic involves **push payments**, where victims are instructed to pay agent fees, processing fees, or account activation charges in order to access or approve financial services. In many cases, victims are directed to transfer funds through **cryptocurrency wallets** or payment platforms such as **PayPal**, which helps obscure the threat actors identities and significantly complicates fund tracing and recovery.



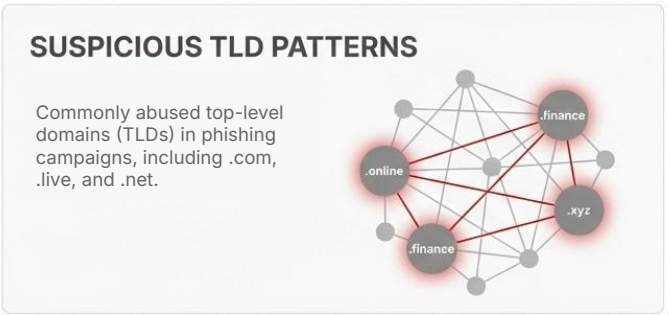


Fake regulatory seals FDIC & NCUA

Key Findings on Fraud Campaign:

- Over the past year, more than **11,000+** fake banking websites have been identified across USA and UK. In the U.S., over **8,000** fraudulent sites were detected, while the U.K. accounted for more than **3,000** many hosted on dedicated domains using fake bank names.
- Monetization is carried out through cryptocurrency wallets, collecting push payments in digital currencies under the pretense of offering legitimate financial services.
- A notable pattern of top-level domains (TLDs), such as .com, .live, .net, and similar extensions has been observed.

Breakdown of Fake Banking URLs



"Fake banks are emerging globally, with more cases expected in other regions"

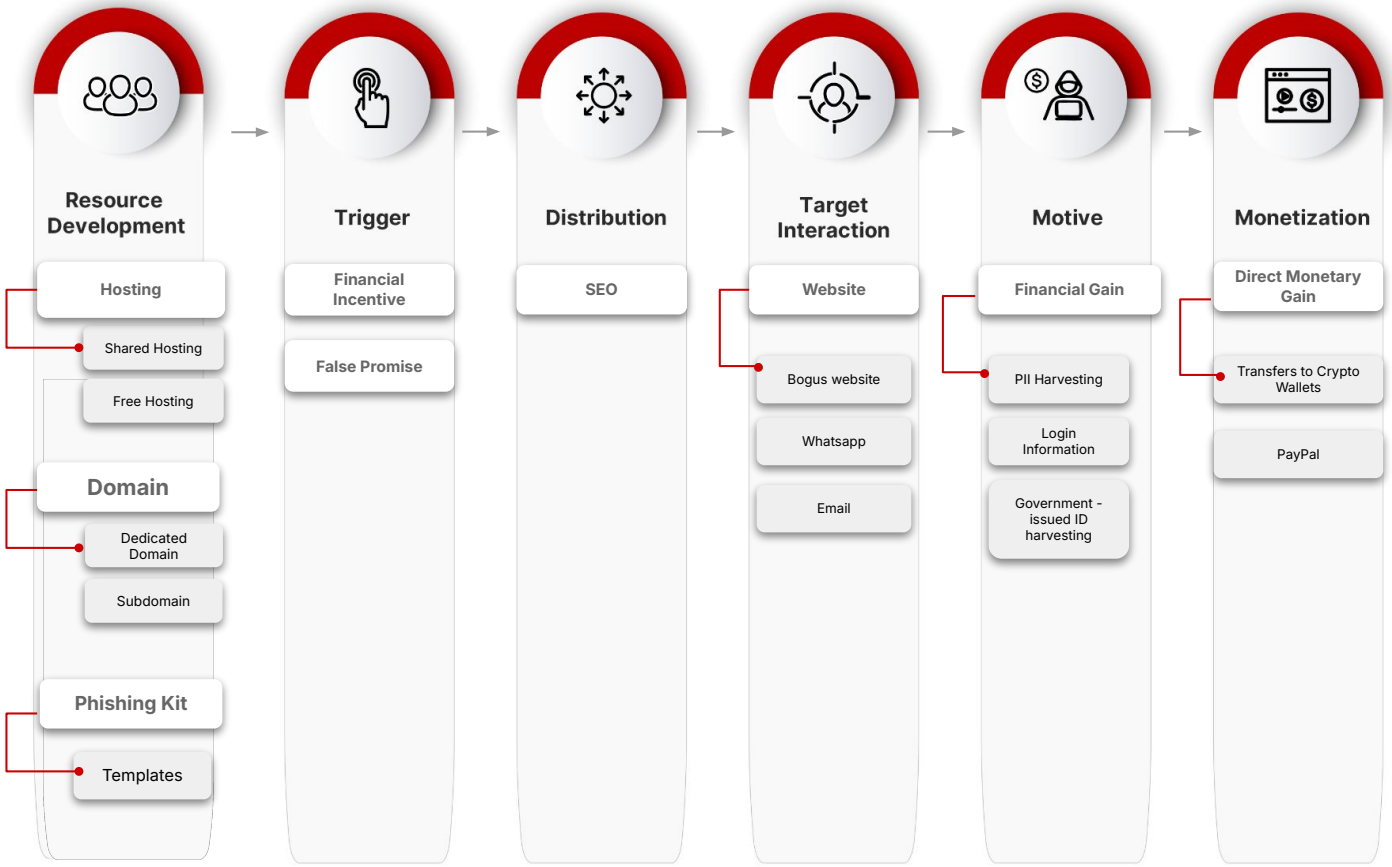
FRAUD STAGES:

CTM360 Fraud Navigator

CTM360's Fraud Navigator is inspired by the MITRE framework. It illustrates how fraudsters operate through different stages of a fraud and classifies frequently used techniques, helping teams recognize and respond to recurring fraudulent activity.
Built on the MITRE model, it identifies seven key stages in a fraud: resource development, Evasion, trigger, distribution, target interaction, motive, and monetization. There are commonly 2 phases in the fraud, represented as Phase 1 (in grey) & Phase 2 (in light red).

This Fraud Navigator have been mapped to this fraud campaign, providing insight into the fraud's lifecycle and shedding light on the techniques, entry points, and attack objectives.

By breaking down the fraud across these stages, the framework enables a clearer understanding of how these campaigns evolve and where defenses can be most effectively applied.



*Fraud Navigator - **Fake Banks fraud***

CTM360 Observations: Structure and Workflow of Fake Bank Ecosystem

Stage 1: Resource Development

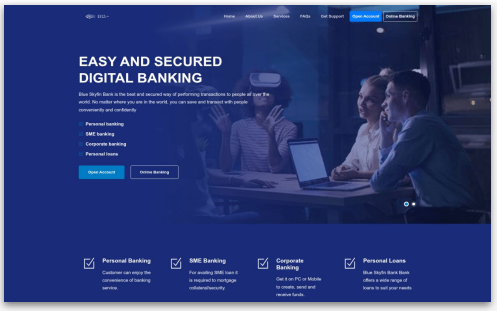
A defining characteristic of the fake bank ecosystem is its heavy reliance on **mass replication** techniques. Threat actors register numerous domains and deploy identical website templates across them, enabling the rapid creation of fake bank websites that advertise non-legitimate financial services, including fraudulent loans, fabricated investment products, and cloned online banking portals. This approach allows fake bank operators to scale their operations quickly and maintain a consistent appearance across thousands of domains.

Patterns of Resource Duplication:

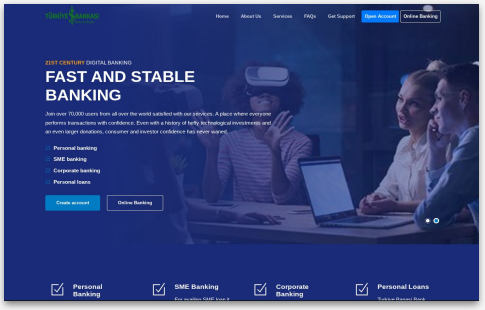
- **Identical HTML structures:** Core code elements, style sheets, and scripts remain unchanged across multiple fake bank domains, indicating the use of standardized templates.
- **Reused imagery and branding:** Logos, promotional banners, and background graphics are copied without modification to reinforce the appearance of legitimacy.
- **Shared metadata and keywords:** Meta descriptions, page titles, and SEO keywords are duplicated word-for-word to enhance search engine visibility and attract victims.
- **Uniform registration patterns:** Threat actor rely on high-volume, high-churn domain registration strategies using low-cost and anonymous registrars, enabling rapid deployment and easy replacement of blocked or taken-down domains.

axtrafinance[.]com

fedelixgroup[.]com



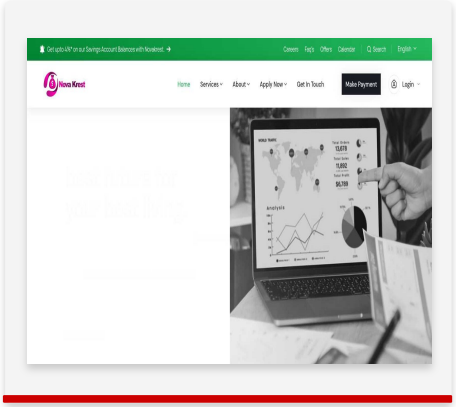
blue[-]skyfin[.]us

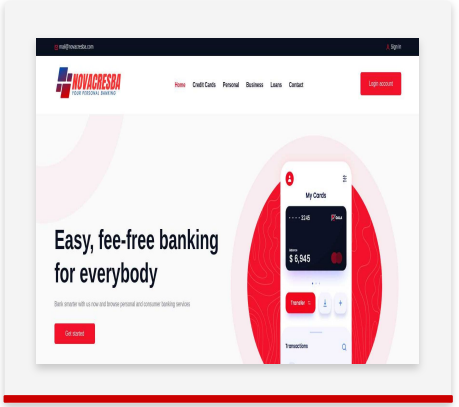


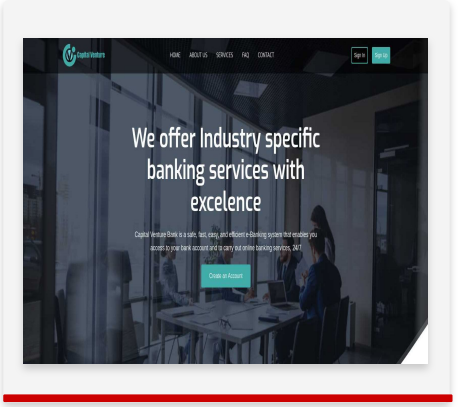
turkiyebanasi[.]com

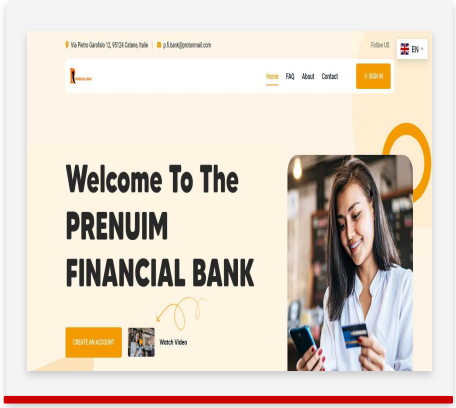
CTM360 Observations: Structure and Workflow of Fake Bank Ecosystem

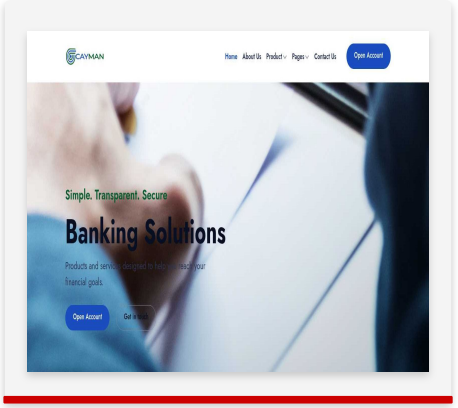
The sample screenshots below showcase identified fake website templates, including the deceptive themes.

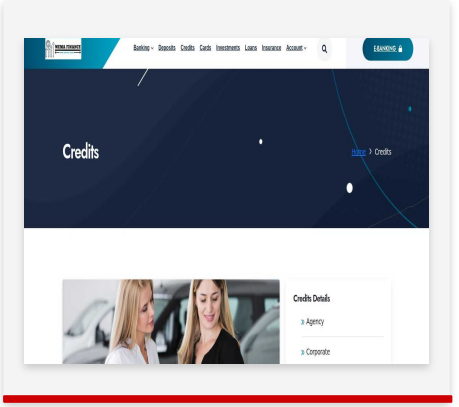


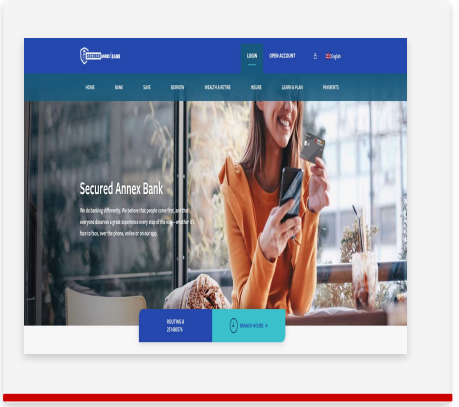












30+ Observed Fake Bank fraud Templates

CTM360 Observations: Structure and Workflow of Fake Bank Ecosystem

Stage 2 & 3: Trigger and Distribution

SEO Exploitation by Fake Banks

One of the most deceptive aspects of fake banks is their strategic use of Search Engine Optimization (SEO) to enhance visibility and perceived credibility.

Common Techniques:

- **Keyword Stuffing:** Websites commonly rely on keyword stuffing by repeatedly embedding popular financial terms within page content, headers, image alt text, and URLs.
- **Targeted Phrases:** Multiple variations of highly searched financial terms to capture a broader audience. By tailoring keywords to different regions, languages, and user intents such as **instant loan approval**,**low-interest personal loan** or **no credit check,** they increase the likelihood of appearing in search queries and attracting potential victims.
- **Algorithm Exploitation:** Actively abusing SEO tools and optimization techniques to gain rapid visibility in search results, allowing the sites to rank quickly and create a misleading appearance of credibility and trustworthiness.

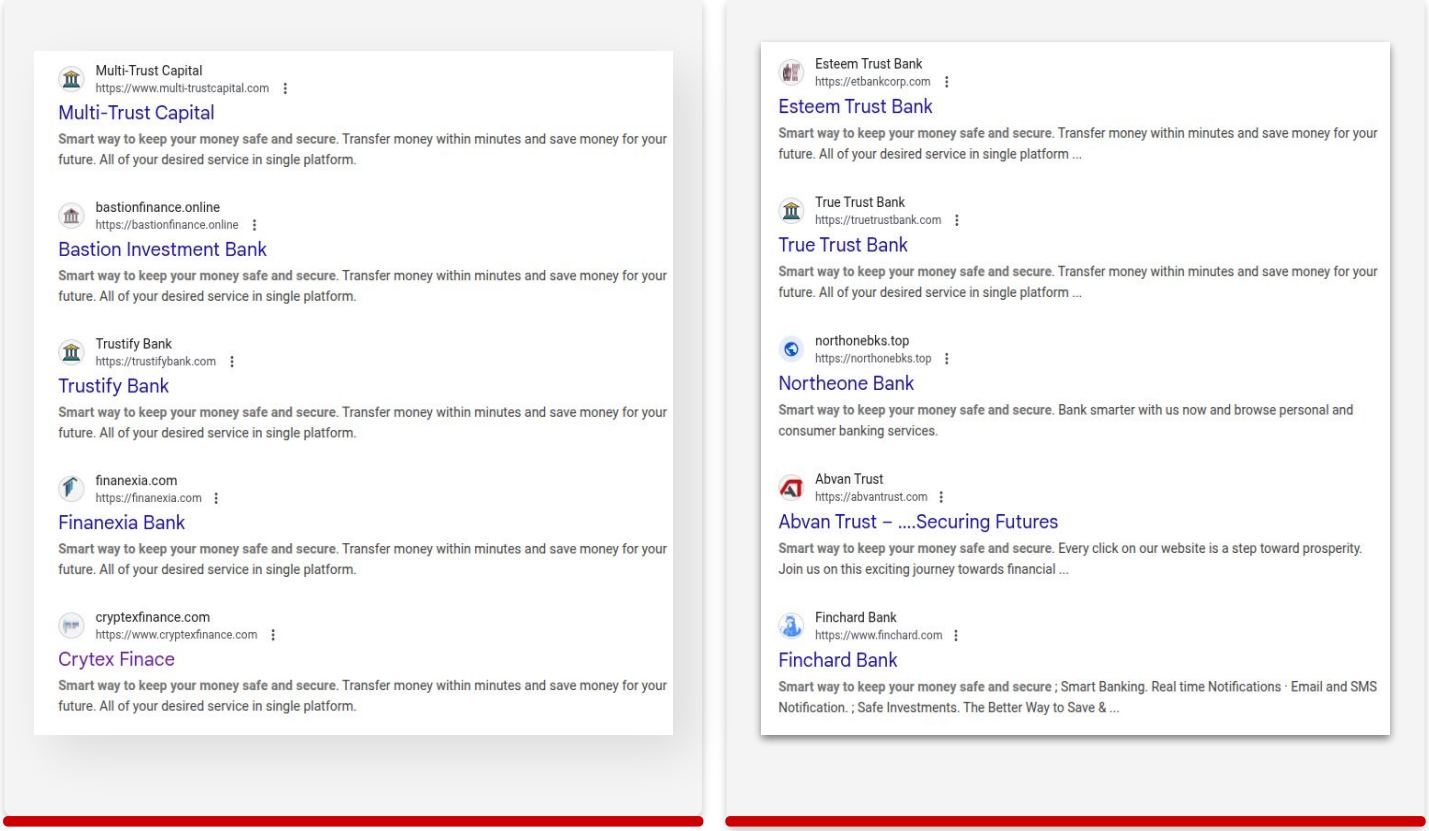


Figure 1 & 2: Fraudulent SEO practices utilize by Fake Banks

Case Statistics

Brief stats on CTM360 observations

Key Exploitation Factors:

- **Trusted domains & reputations:** Fake bank phishing campaigns frequently rely on domains registered under credible-sounding TLDs such as **.com or .net** that closely resemble legitimate banking names.
- **Shared hosting Abuse:** Threat Actor often exploit shared hosting environments, where multiple customers' websites reside on the same server or IP range. This allows malicious activity, such as phishing sites, to blend in with legitimate traffic.

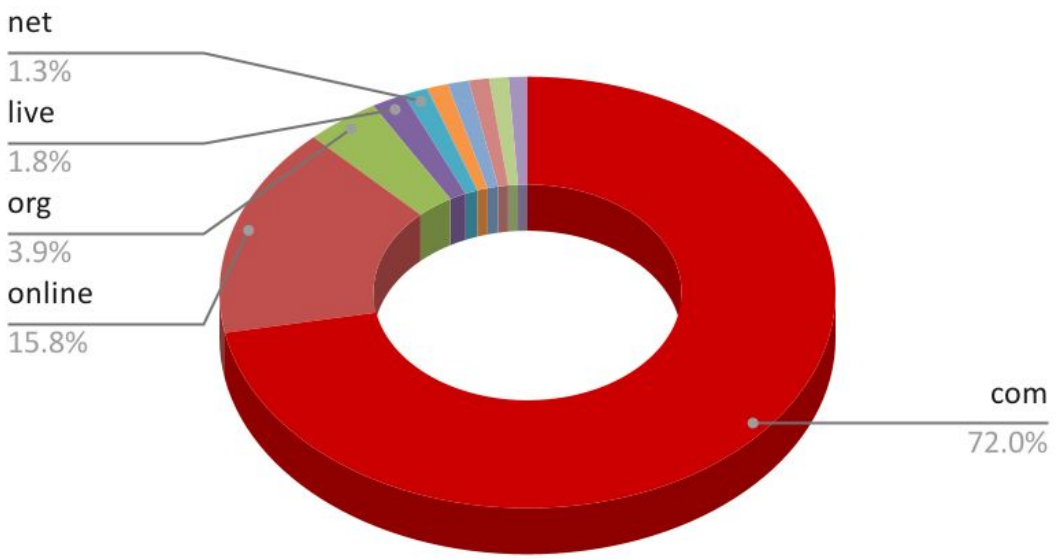


Figure 1: Chart highlighting various platforms used to host the Fake sites

CTM360 Observations: Structure and Workflow of Fake Bank Ecosystem

Stage 4: PII Harvesting and Monetization

PII harvesting and monetization are carried out through fake bank frauds that lure victims via convincing websites and fraudulent KYC (account registration) processes. Victims are asked to submit personal details, identity documents, and in some cases live selfies, while attackers build trust through fabricated approval and verification stages before requesting activation or processing fees.

Key Points:

- Fake KYC processes used to collect personal and identity data
- Submission of identity documents and live selfies for false verification
- Fabricated approval workflows to establish legitimacy and trust
- Activation or processing fees demanded as part of the fraud

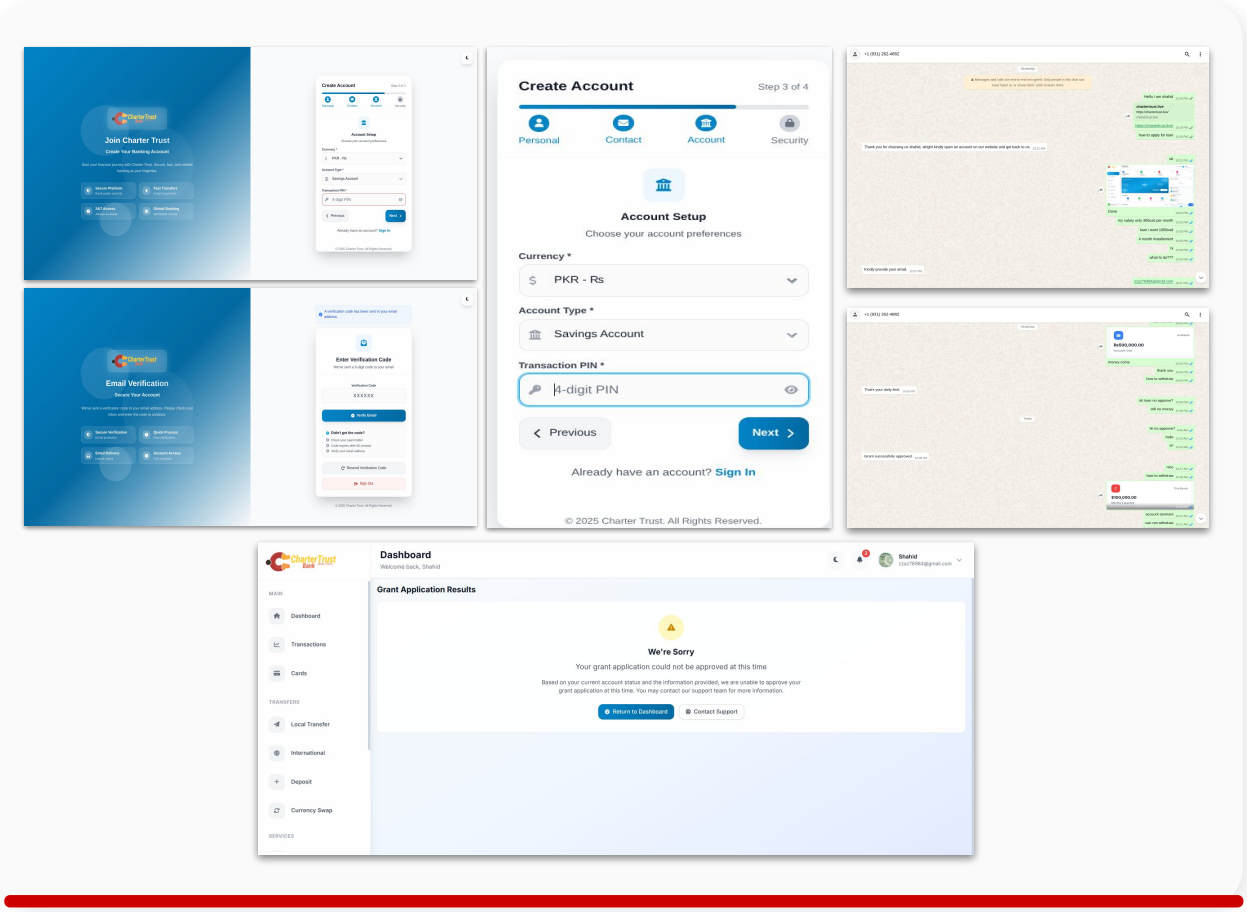


Figure: PII Harvesting and Monetization

CTM360 Observations: Structure and Workflow of Fake Bank Ecosystem

Stage 5 & 6: Motive & Monetization

Deposit Theft:

A critical lure occurs through live chat or WhatsApp, where victims are pressured to proceed with payments using urgency and reassurance tactics. The monetization methods are structured as follows:

- **PayPal:** As an alternative payment method, attackers redirect them to use PayPal, instructing payments to a specified email address via the **Friends and Family option**, which bypasses buyer protection and significantly reduces the likelihood of fund recovery.
- **Cryptocurrency wallets:** Victims are directed to deposit funds via cryptocurrency wallets, where the irreversible nature of blockchain transactions enables attackers to receive payments while significantly hindering fund recovery and transaction tracing.

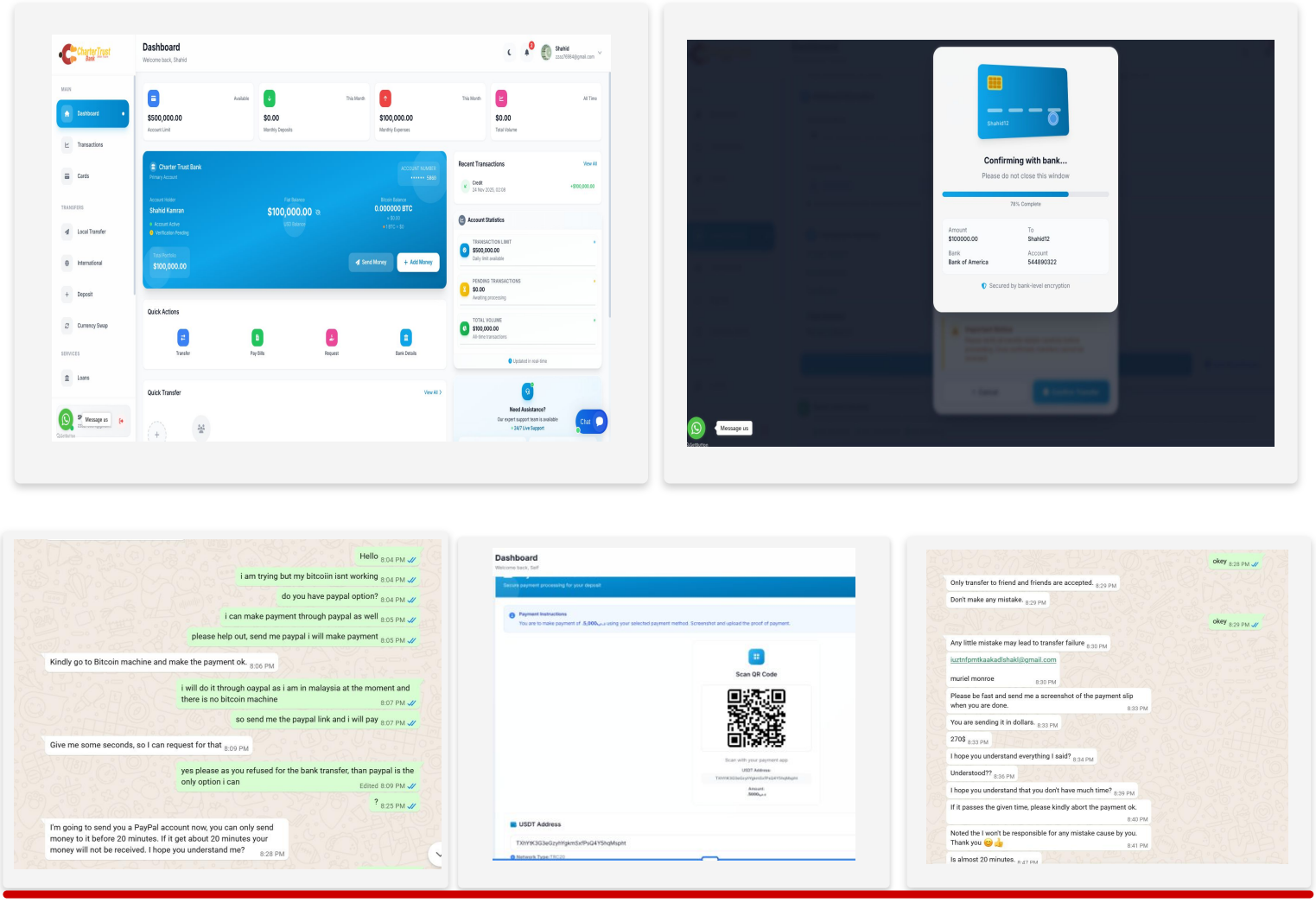


Figure: Fake Banks Monetization Stage

ABOUT US

CTM360 is a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and unlimited managed takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence.

CONTACT US:

+973 77 360 360

info@ctm360.com

www.ctm360.com

21st Floor, East Tower Bahrain Financial Harbour, Kingdom of Bahrain

CTM360®