

Report | January 2026

(Digital Hundi)

ShadowRemit

**Malicious Google Play Apps used for
illegal money transfer**

Analysis by CTM360



**INDUSTRY**
Financial Services**COUNTRY**
Bangladesh**REGION**
ASIA**DATE**
Jan, 2026

OVERVIEW :

CTM360 **observed continued and evolving activity** consistent with a known Malicious Android apps targeting remittance and money-transfer users with a **primary focus on Bangladeshi expatriate** communities. Informal remittance systems such as **Hundi/Hawala** have long been used across South Asia, and have increasingly been digitized through malicious Android apps, fake marketplaces, and localized social engineering. Similar campaigns continue to re-emerge with evolving variants and distribution methods.

A sample of the reviewed infrastructure included [PlayPraetor](#)-style **Google Play Store impersonation pages** used to distribute unauthorized APKs via **side-loading mechanisms** outside Google Play, bypassing official platform security controls.

These impersonation pages closely mimic legitimate Google Play listings and promote the applications as trusted remittance services using strong financial incentive messaging such as "**zero fees**," "**instant transfers**," **improved exchange rates**, and reward-style offers (e.g., **cashback**) to encourage installation and payment activity.

Following installation, victims are guided through payment workflows that route funds to local beneficiary endpoints, reflecting a **digitized Hundi/Hawala-style** settlement model involving intermediary domestic accounts and informal payout channels. This approach can bypass regulated remittance corridors and aligns with mule-account collection patterns.

Key Findings

- **WebHunt** identified a sample of **100+** such APK distribution pages, notably featuring PlayPraetor-styled Google Play impersonation templates.
- Victims are instructed to send payments to beneficiary accounts/eWallet endpoints and provide **transaction screenshots** as proof for verification
- **In one reviewed infrastructure**, an exposed C2 management server was observed showing **300+ registered users** and reflected a high volume of transaction activity.
- **Open directory listings and C2 management server** were observed exposing sensitive end-user content including **credit and debit card data, passport scans, ID cards, visa stickers, and transaction receipts**.

This report is based on the findings of a sample cases detected by CTM360, however we extrapolate this fraud cases to be much higher and impacting users in other geographies.

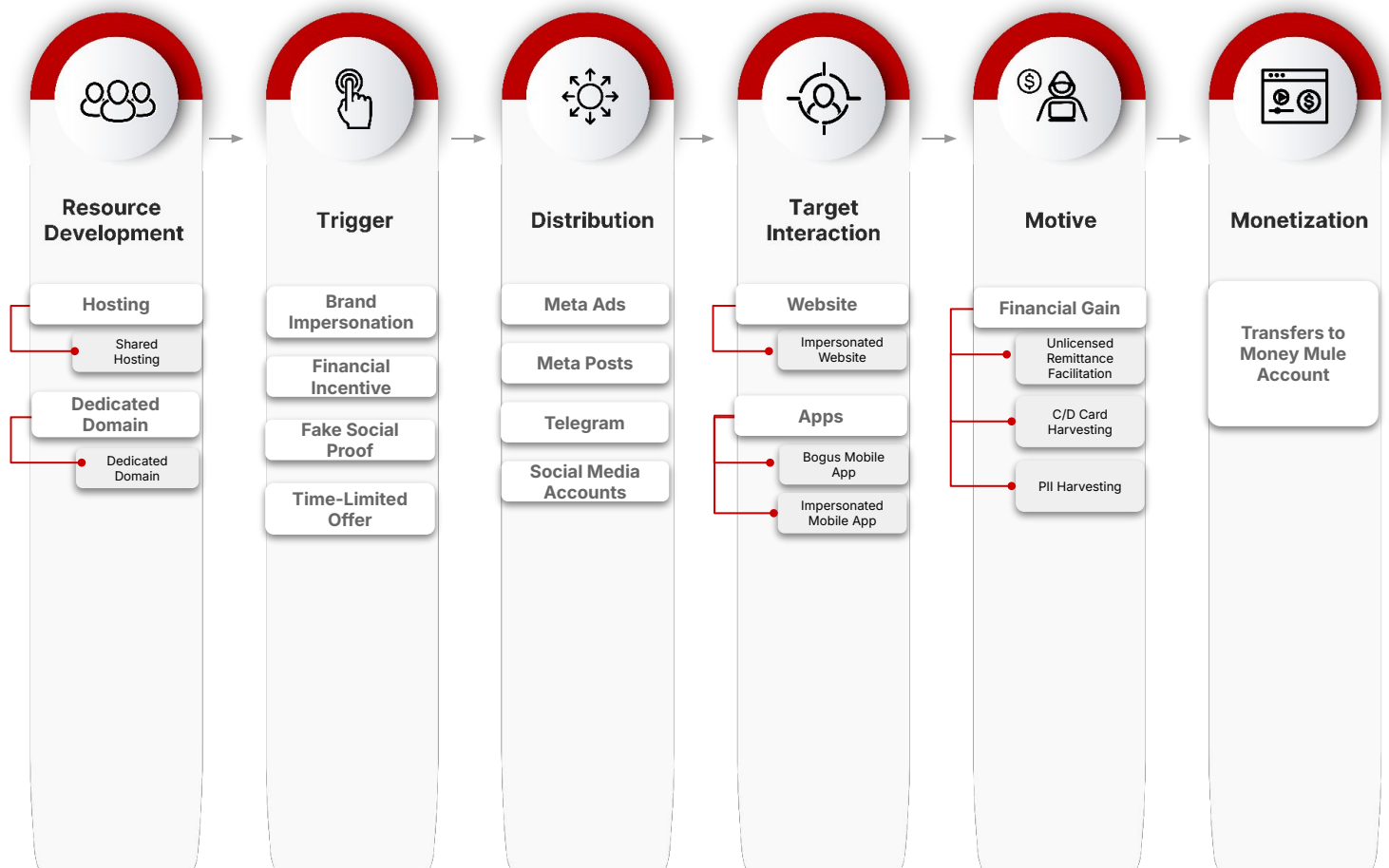
FRAUD STAGES:

CTM360 Fraud Navigator

CTM360 Fraud Navigator, inspired by the MITRE framework, is an analytical model used to map observed fraud activity and illustrate how threat actors progress through distinct operational stages. Fraud Navigator categorizes common fraud techniques and provides insight into typical patterns of malicious behavior across six key stages: Resource Development, Trigger, Distribution, Target Interaction, Motive, and Monetization. These stages are commonly represented in two phases: Phase 1 (white) and Phase 2 (grey).

This Fraud Navigator has been mapped to the observed fraud campaign to provide insight into its lifecycle, including key techniques, entry points, and objectives. By breaking the campaign down across these stages, the framework enables a clearer understanding of how the activity evolves and where preventive or disruption measures can be most effectively applied.

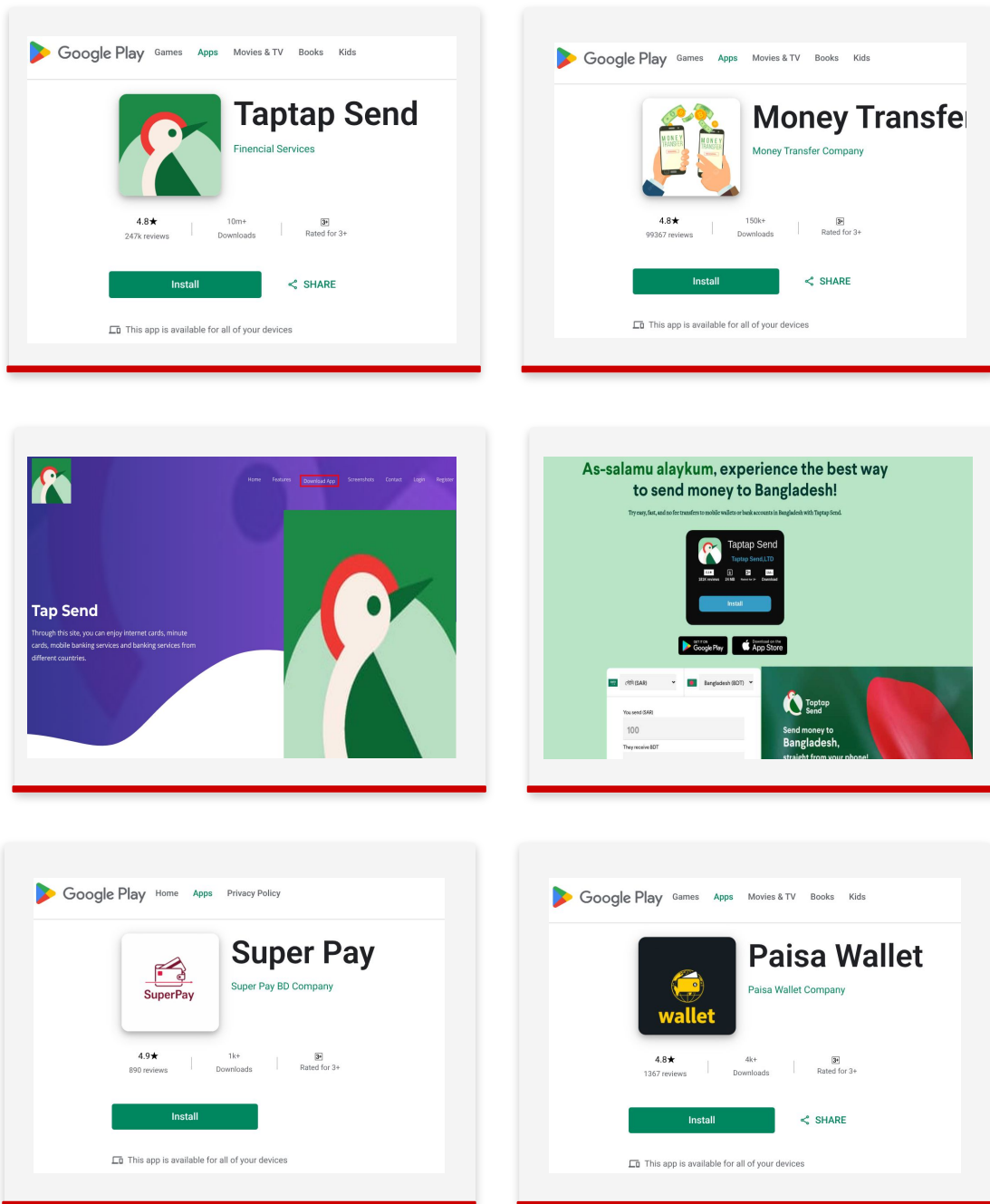
Based on our experience, PlayPraetor-style impersonation infrastructure is frequently reused across fraud operations, with domains and APK variants updated over time to evade takedowns and maintain distribution.



ShadowRemit - Fraud Navigator

CTM360 Observations

The sample screenshots below illustrate a subset of the identified Google Play Store impersonation pages used to distribute unauthorized money-transfer/remittance applications.



Source: CTM360 Webhunt

CTM360 Observations

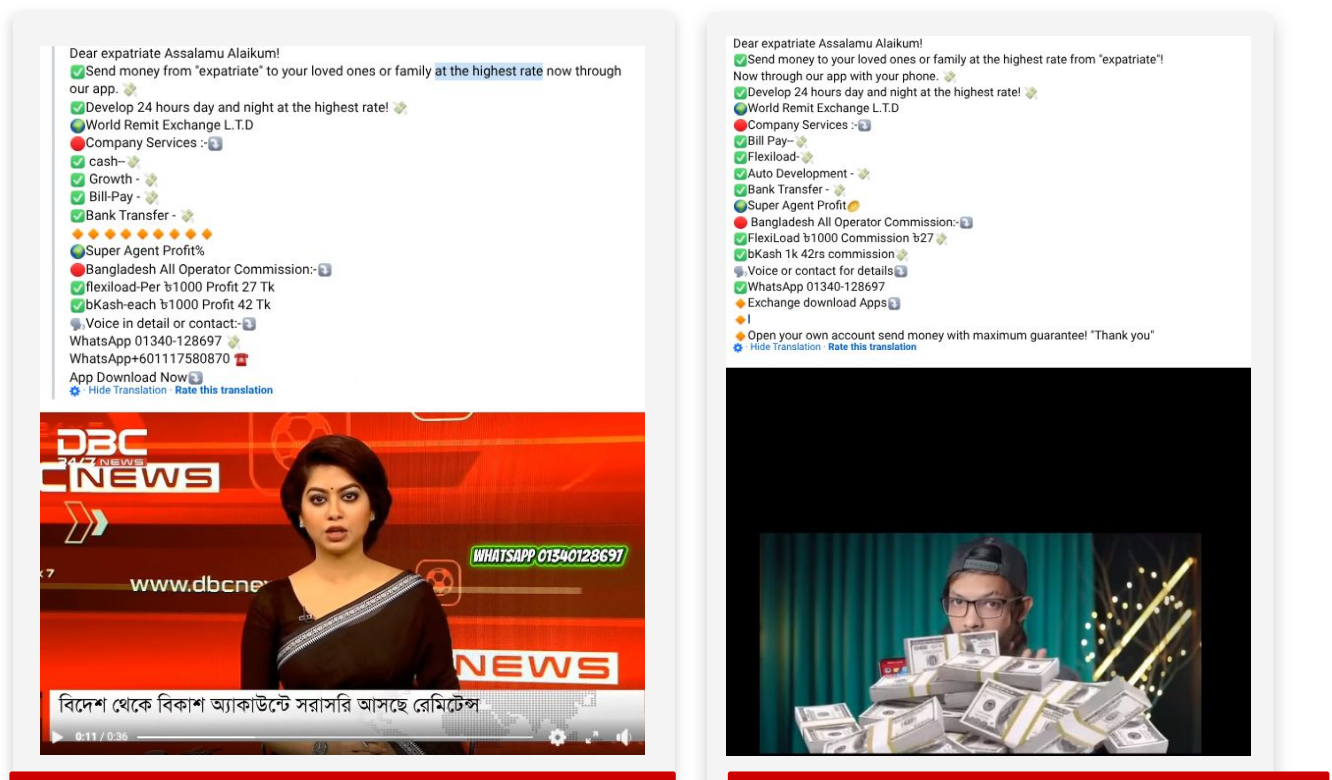
Resource Development

The actors leveraged **dedicated domains hosted on shared infrastructure** to support APK distribution pages and supporting backend services. The infrastructure also frequently included a C2 **management server**, serving as a centralized interface for administering the application ecosystem.

In **some instances**, to increase credibility and drive installations, the actors hosted Android APKs on webpages crafted to mimic authentic **Google Play Store listings**. These pages replicated trusted Play Store design elements (branding, logos, and layout), encouraging victims to download APKs directly and thereby bypass Google Play's built-in security controls.

Trigger

The primary trigger technique relied on **financial incentive messaging**, promoting offers such as "**zero fees**", "**instant transfers**" and **better exchange rates** to attract users seeking low-cost remittance options. These promotions are reinforced with reward-style incentives (e.g., cashback offers, scratch cards, and in-app rewards) to encourage installation and continued payment activity.



Fake social media posts promoting the app with "highest rate" claims.

CTM360 Observations

Distribution

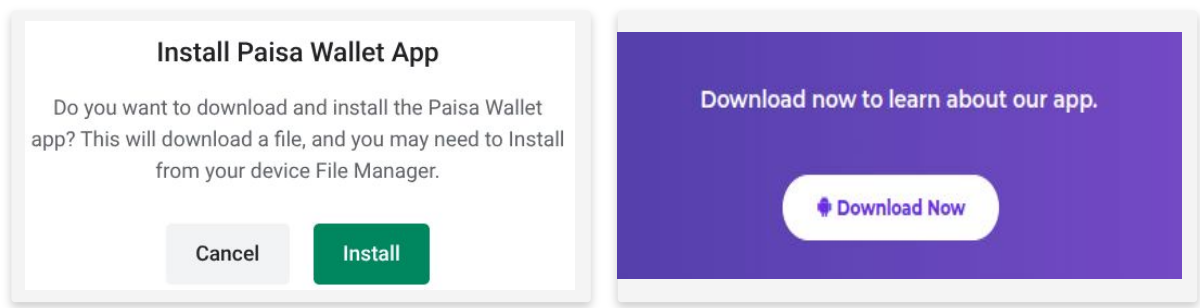
Download links were circulated through **social media advertisements, promotional posts, and Telegram channels**, which served as primary traffic drivers into the impersonation ecosystem. These distribution methods redirected victims to fake **Google Play Store pages** promoting "Money Transfer" applications and hosting unauthorized APK downloads. The ads and messages were designed to maximize reach and exploit user trust, ultimately tricking users into clicking the links and downloading APKs from fraudulent domains.



Fake social media posts promoting the app with "highest rate" claims.

Target Interaction

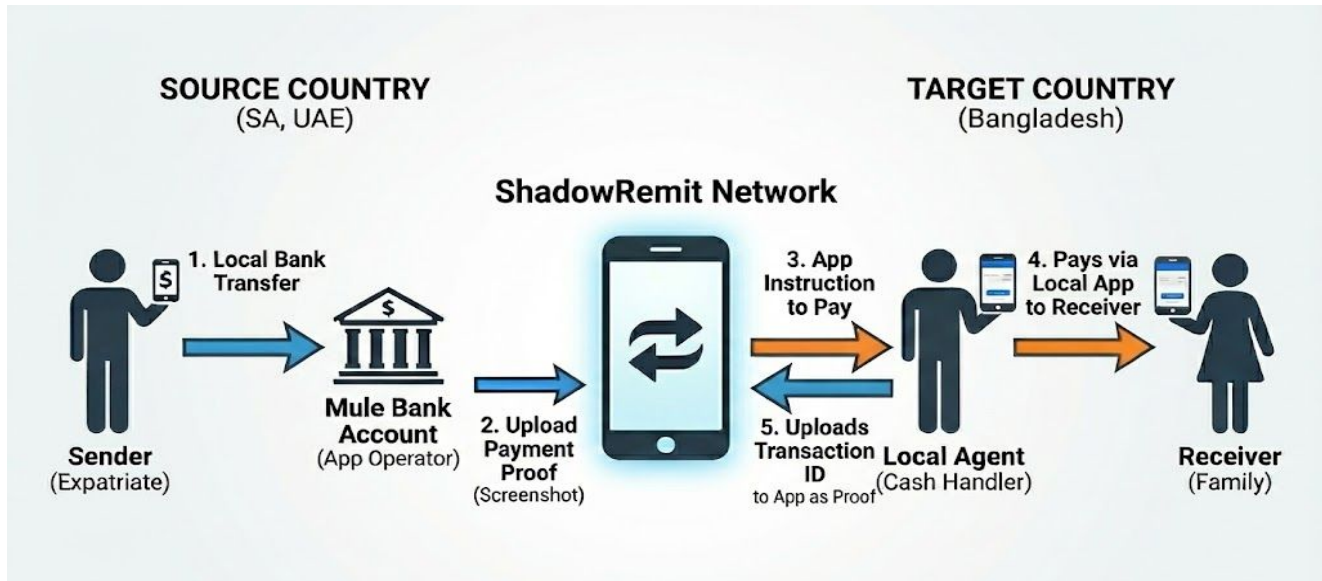
Victims were directed to fraudulent download pages advertising money-transfer/remittance applications. In some instances, the download experience closely mimicked a legitimate Google Play Store listing, featuring familiar branding elements, icons, and layout. In other cases, APKs were delivered through custom landing pages that hosted direct download links without Play Store impersonation. In both scenarios, victims were prompted to download and install an APK via side-loading mechanisms outside the Google Play ecosystem, bypassing official platform security controls.



Following installation, victims were guided to interact with the application and proceed through payment workflows, resulting in transfers to beneficiary accounts/eWallet endpoints associated with the operation.

Suspected Settlement Workflow (a sample case-study)

Unlike legitimate remittance applications that rely on regulated international transfer corridors, the observed payment flow appears consistent with an **informal netting-off settlement model** commonly associated with **Hundi/Hawala-style networks**. In this model, funds are collected domestically in the source country and corresponding payouts are arranged domestically in the target country, without using regulated cross-border transfer rails.



Local Collection (Source Country)

- The victim initiates a transfer request in the application (e.g., sending funds to a beneficiary in another country).
- The app displays a local beneficiary account or IBAN within the victim's country (e.g., a domestic bank account or eWallet endpoint).
- The victim transfers funds using domestic rails (e.g., bank transfer, local wallet top-up).
- The victim uploads a transaction screenshot/receipt as proof of payment, indicating a verification step before further processing.

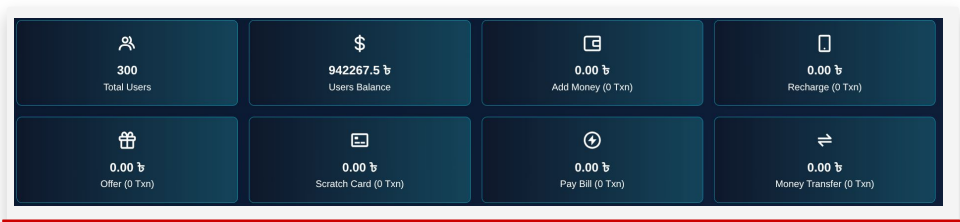
Local Payout (Target Country)

- Following receipt verification, operators coordinate with counterpart handlers in the destination country.
- The beneficiary receives the equivalent amount in local currency via domestic payment methods (e.g., bank transfer, mobile wallet, or cash handover).

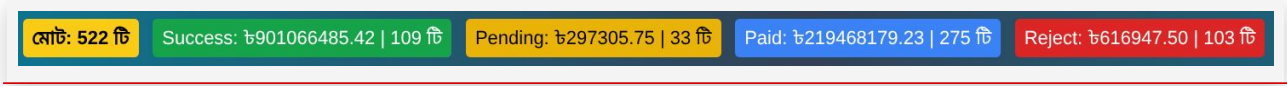
Further Analysis

In **one reviewed sample (APK and associated website infrastructure)**, CTM360 identified an embedded C2 management server. The C2 Server in this instance exposed operational metrics including:

- A sample of **300+** total registered users
- Aggregated wallet balance indicator
- Modules for money handling and services including Add Money, Money Transfer, Bank, Pay Bill, etc.



From the same C2 Server, a transaction history view was observed containing **500+ transaction records**, with entries dating from **01/09/2025** to **31/12/2025**, and categorized across multiple transaction states (e.g., Success, Paid, Pending, Rejected).



The dataset reflected a **high volume of transaction activity** within the ecosystem, however, CTM360 observed indicators consistent with **test entries**. As such, the figures presented in the C2 server may **not accurately represent genuine remittance volume or confirmed user activity**.

Two primary transaction directions were observed:

- **Receive flows**, aligned with Add Money operations
- **Send flows**, aligned with Money Transfer operations (onward transfer)

521	240	Send	3,230.00	Success	13-12-2025 07:23:55 PM	0132	Pin-6932	Money Transfer	Account Type: Personal
515	266	Receive	199,512.00	Success	12-12-2025 09:39:58 PM	7039	AODUUHLYZD	W Paisa Wallet	Loan + Cashback
497	257	Receive	100.00	Success	10-12-2025 12:22:16 AM	5925	HJVPQRPDSA	W Paisa Wallet	refund
490	240	Send	600.00	Success	01-12-2025 08:31:04 PM	5857	IUDVMBHWAT	W Paisa Wallet	0
486	238	Send	400.00	Success	30-11-2025 02:14:02 PM	0163	4456	Money Transfer	Account Type: Personal

Further Analysis

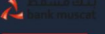
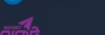
Sensitive Data Exposure

Additionally, within the reviewed sample's web infrastructure, open directory listings were identified. These directories exposed sensitive and high-risk content, including:

- Credit/Debit card data
- Passport scans
- Personal photographs
- ID card scans
- GCC country visa sticker scans
- Transaction receipts

	1766950788_1614.jpg	2.2 MB		1766457703_3974.jpg	156 KB
	1766950440_4463.jpg	5.2 MB		1766085223_6454.jpg	138 KB
	1766950436_2280.jpg	5.2 MB		1766084086_7305.jpg	138 KB
	1766867823_8540.jpg	964 KB		1766083979_8110.jpg	138 KB
	1766867816_6369.jpg	964 KB		1766070771_8355.jpg	138 KB
	1766867657_7367.jpg	45 KB		1766067450_8700.jpg	138 KB
	1766867290_4524.jpg	4 MB		1766066195_3449.jpg	138 KB
	1766867239_5435.jpg	4 MB		1766064124_3163.jpg	138 KB
	1766867066_2650.jpg	45 KB		1766064022_4927.jpg	138 KB
	1766783523_7550.jpg	278 KB		1765979440_9668.jpg	364 KB

Additionally, multiple payment-accepting accounts were configured within the C2 management server. These appear to represent beneficiary bank and eWallet endpoints used for payment collection and may indicate the use of intermediary accounts consistent with mule-account patterns.

ID	Name	Number	Holder	District	Branch	Image	Type	Action
33	REMITTANCE	0161	Paisa Remit Ltd	GLOBAL	eWallet		Bank	এডিট ডিলিট
32	om OMAN om	0211	MUSCAT BANK	Oman	all		Bank	এডিট ডিলিট
31	mv MALDIVES mv	7730	Bank of Maldives	Paisa Bank	Maldives		Bank	এডিট ডিলিট
30	ae DUBAI ae	0190	MASHREQ BANK	Global	All		Bank	এডিট ডিলিট
29	sa SAUDI A Bsa	0770		u2426778151	MD HOSSAIN		Bank	এডিট ডিলিট
25	bKash Remittance	0132	eWallet	bangladesh	Global		Mobile	এডিট ডিলিট
24	mv MALAYSIA mv	1643	May Bank (Agent Auto)	Touch N Go Duit Now, RHB, AmBank, CLIB	Paisa Remit Ltd		Bank	এডিট ডিলিট
23	mv MALAYSIA mv	1317	Touch N Go	Duit Now All Banking Transfar	Global		Bank	এডিট ডিলিট
19	✈️ eWallet bKash ✈️	0188	Paisa wallet	Global	AUTO		Mobile	এডিট ডিলিট
18	qa QATAR qa 2	8448	Paisa Wallet	Doha	Qtr		Bank	এডিট ডিলিট
14	🚀 Rocket	0161	Paisa Remit Ltd	Global	eWallet		Mobile	এডিট ডিলিট
10	🌿 Nagod Personal	0140	Paisa Remit Ltd	.	.n		Mobile	এডিট ডিলিট +

Further Analysis

Fraudulent Documentation

In addition to identity documents and transaction artifacts, CTM360 observed **Bangladesh eTrade (BD eTrade) license certificate samples** embedded within **one of the reviewed applications**. The certificates appeared to be forged, intended to **increase perceived legitimacy and user trust**, support onboarding, or facilitate **fraudulent verification workflows**.

Upon investigating the certificate content and associated details, the **original referenced certificate** was found to be **unrelated** to the application and its purported remittance services, suggesting deliberate **reuse or manipulation of official-style documentation for deception**.

Dhaka North City Corporation
www.dncc.gov.bd

E-Trade License

Details of license issue
Date of Issue :03/09/2024
Time of issue :18:34:06

License No. :

Pursuant to section 10 of the Standard Tax Schedule, 2016 made by the Government under the powers conferred by section 84 of the Local Government (City Corporations) Act, 2009 (Act No. 60 of 2009), Business, Professional, This trade license is issued in favor of the following person/organizations for the purpose of collection of taxes imposed on professions or industrial establishments.

1. Business name	: Ramit Wadati Limited	Word	Word	30
2. Name of Owner	: Abul Kalam Talukder			
3. Father's name	: Abul Mohit Talukder			
4. Mother's name	: Rowshan Ara			
5. Nature of business	: Limited Company			
6. Type of business	: Remittance provider			
7. Business address B. Region/DNCC's	: House 42, Road No 04, Gulshan Avenue, Dhaka			
8. Website	: WWW			
9. NID/Passport/Birth Registration No. Mobile No		TIN/BEN No:		
		E-mail:		
10. Financial Year	: 2024-2025 [New]	Date of Commencement of		03/09/2024
11. Current Address/Owner Holding No.		Business Permanent Address of Proprietor		
	: 48	RODING NO		
	: Road No	: Road No		
	: Village / Mohala	: Village / Mohala		
	: Post Code	: Post Code		
	: 1207	: 1207		
	: Police station	: Police station		
	: District	: District		
	: Division	: Division		
12. Model Schedule, Serial No. 13 of 2016, Trade License Fee (New/Renewal)		Signboard Tax (Informatives) : VAT Book Value		
	: 200089699	Form		96000
	: 0 : 0 : 0 : 0.00	Firm Other Fees		79008
		Due ()		27089
		amendment Fee		590759.00
		Chapter		417784.00
		sanctioned		

This trade license expires on 30 June, 2025

Licensing and Advertising Supervisor

Do the work

Fake E-Trade License Certificate

Dhaka North City Corporation
www.dncc.gov.bd

E-Trade License

Issue date :05/01/2026
Time of issue :19:12:22

License No. :

This trade license is issued in favour of the person/organization mentioned below for the purpose of collecting tax imposed on business, profession, profession or industrial establishment as per Section 10 of the Model Tax Schedule, 2016, prepared by the Government under the powers conferred by Section 84 of the Local Government (City Corporation) Act, 2009 (Act No. 60 of 2009).

1. Business name	:		
2. Name of the owner of the organization	:		
3. Father/Husband's Name	:		
4. Mother's name	:		
5. Nature of business	:	Limited company	
6. Business type	:	IT, Import, Export Management Business, Consultancy, Developer, News Media, First Class Contractor, Export, Real Estate, Suppliers (Excluding Flammables and Chemicals)	
7. Organization address	:		
8. Region/Market Branch Area	:	Ward / Market:	
9. NID/Passport/Birth Number: No. Phone	:	BIN No.:	
	:	Email:	@gmail.com
10. Financial year	:	Business start date:	03/09/2024
11. Owner's current address	:	Owner's permanent address	
	:	Holding No.	
	:	Road No.	
	:	Village / Neighborhood	
	:	Postcode	
	:	Police station	
	:	District	
	:	Category	
12. Trade License/Renewal Fee (Annual)	:		
	:	License/renewal fee	2000
	:	Surcharge	0
	:	Income tax / Withholding tax	0
	:	Due ()	0
	:	Amendment fee	0.00
	:	Signboard tax	960
	:	VAT	444
	:	Book price	270
	:	Form fee	0.00
	:	Other fees	500.00
	:	Total	4174.00

This trade license is valid until June 30, 2025.

Licensing and Advertising Supervisor

Tax officer

Genuine E-Trade License Certificate



Potential Risks & Recommendations

Based on the observed platform functionality and the presence of multiple configured beneficiary accounts (bank accounts, eWallet numbers, and IBAN endpoints), the ecosystem appears to support illicit fund collection and may facilitate illegal fund transfer activity, including unlicensed remittance operations. As such, it presents several risks, including:

- **Money laundering & mule account abuse:** Multiple bank/eWallet/IBAN endpoints suggest mule-account facilitation, enabling criminals to collect and redistribute funds while obscuring transaction origins.
- **Illegal/unlicensed remittance operations:** The platform may be used to bypass regulated remittance channels, avoiding licensing requirements, transaction limits, and AML/KYC obligations.
- **Fraud & direct financial loss:** Users may transfer funds to operator-controlled accounts with no assurance of payout, increasing likelihood of fraud-driven financial loss.
- **Sanctions & regulatory evasion:** Informal cross-border routing may enable transfers to restricted or sanctioned entities, with limited screening controls increasing compliance and sanctions exposure.
- **Identity & payment data exploitation:** Exposure of sensitive data including identity documents (passports/IDs/visas), transaction receipts, and stored credit/debit card information creates risk of identity theft, account takeover, payment fraud, and document forgery.

Recommendations :

- Escalate to AML / Financial Crime teams to review mule-account indicators and assess potential links to illegal remittance settlement networks.
- Block, monitor, and track associated domains linked to PlayPay/PlayPraetor impersonation infrastructure, including at country level where applicable.
- Assess victim impact exposure where possible, particularly relating to identity documents leaked via open directories; recommend preventive monitoring or outreach if victims can be identified.

References:

<https://www.thefinancetoday.net/article/economy/19617/Digital-hundi-acts-behind-remittance-shortfall>

<https://www.bssnews.net/others/319525>

<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/fake-android-money-transfer-app-targeting-bengali-speaking-users/>

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

Disclaimer

The information contained in this document is meant to provide general guidance and brief information to the intended recipient pertaining to the incident and recommended action. Therefore, this information is provided "as is" without warranties of any kind, express or implied, including accuracy, timeliness, and completeness. Consequently, under NO condition shall CTM360®, its related partners, directors, principals, agents, or employees be liable for any direct, indirect, accidental, special, exemplary, punitive, consequential, or other damages or claims whatsoever including, but not limited to loss of data, loss in profits/business, network disruption...etc., arising out of or in connection with this advisory.

