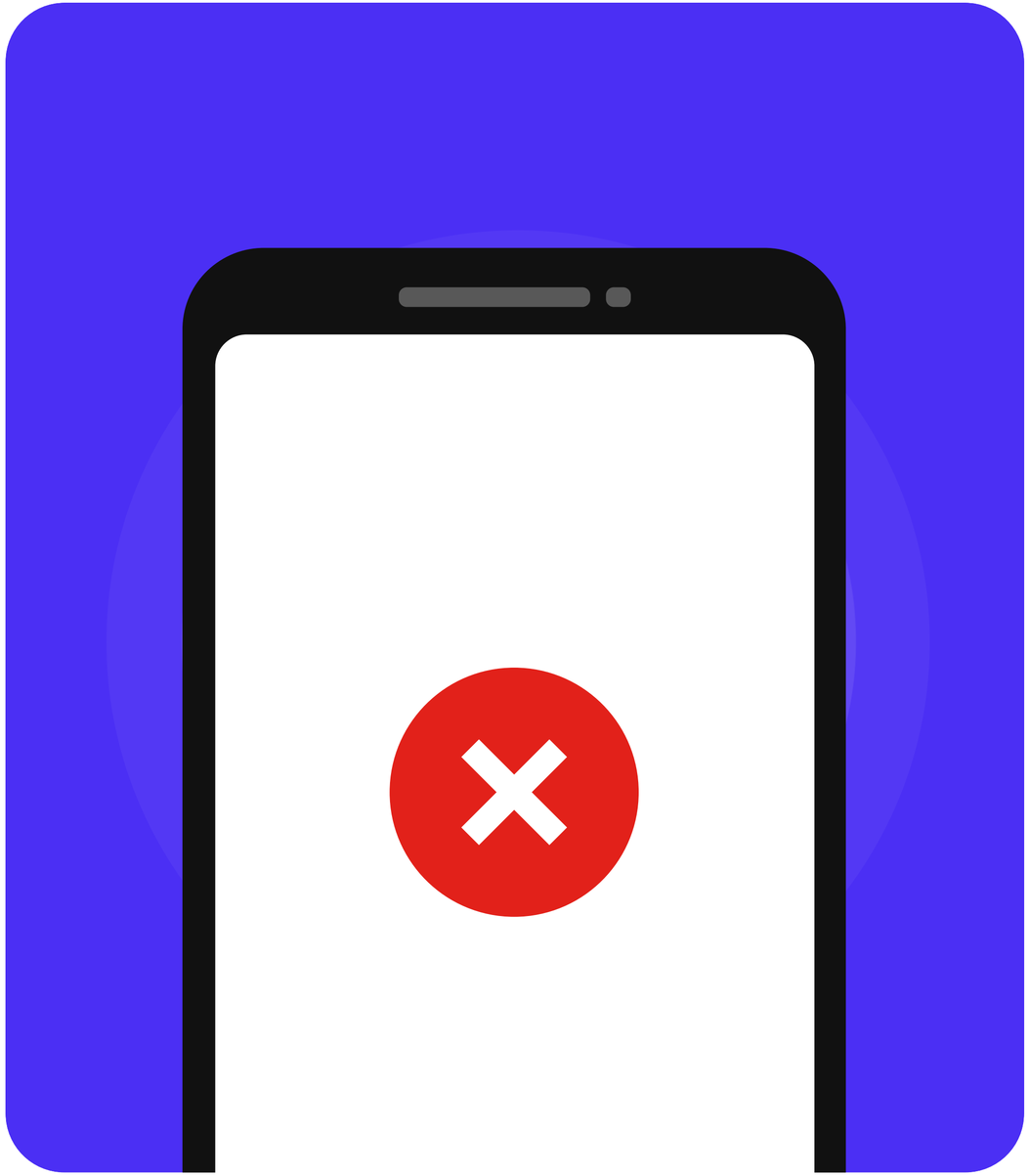
# Financial Abuse in Africa's Payment Systems- A Trust and Safety Issue



Trusted Tech
Africa Ltd

Financial abuse is a pervasive but often overlooked form of coercive control, particularly within the context of domestic violence. It involves tactics such as restricting access to funds, controlling financial resources, and using financial transactions to intimidate, harass, or manipulate victims. As digital ecosystems expand, financial abuse must be recognized as a form of online gender-based violence (OGBV) where digital tools are used to reinforce gendered power imbalances and harm vulnerable users.

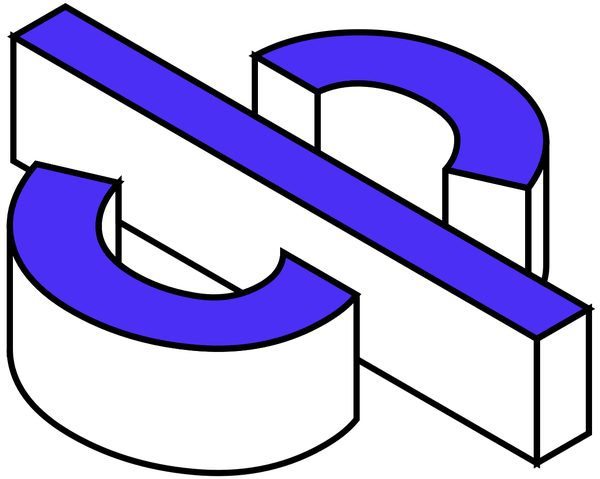
Recent evidence from Australia, where the Commonwealth Bank (CBA) detected over 400,000 abusive messages embedded in small financial transactions annually, calls attention to  how digital payment systems can be weaponized against vulnerable individuals. These cases highlight the urgent need for payment platforms to recognize financial abuse not merely as fraud or policy violations, but as serious trust and safety threats.

In Africa, the rise of digital financial platforms such as Opay, Moniepoint, MTN Mobile Money, and banking applications has been instrumental in expanding financial inclusion. However, the same technologies that empower millions also create new avenues for harm. The absence of advanced abuse detection mechanisms, lack of trauma-informed user support systems, and limited awareness. Without proactive trust and safety measures, digital payment platforms risk becoming silent enablers of gender-based violence online, leaving  victims of domestic violence and coercive control dangerously exposed to financial and emotional harm.

# Problem Statement

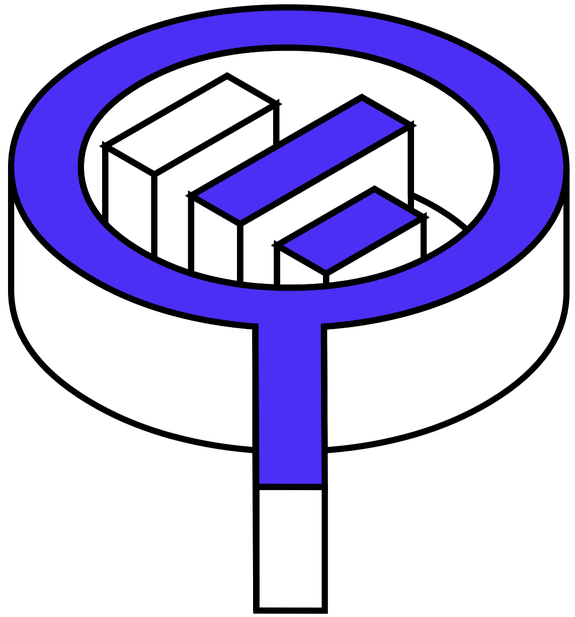
safety of users vulnerable to financial exploitation and abuse. Most platforms have security centers or protocols focused on fraud and scams, which are critical for financial system integrity. However, these mechanisms often overlook interpersonal or gender-based financial abuse where perpetrators misuse payment systems to maintain coercive control, stalk, intimidate, or harass victims especially women, this is a trust and safety issue because it directly threatens user well-being, platform integrity, and user confidence.

**This gap in user protection not only exposes vulnerable individuals to harm but also undermines broader user trust and platform integrity. Addressing financial abuse as a trust and safety issue is essential to building truly inclusive and secure digital economies in Africa.**



# Overview Of Research

**TrustedTech** Team conducted a research to understand how digital payment platforms across Africa may inadvertently enable financial abuse, coercive control, and gender-based online harms, particularly against women and other vulnerable users. The research aimed to evaluate trust and safety measures on leading platforms, identify gaps in user protection, and explore opportunities to co-create solutions that prioritize safety, dignity, and digital financial autonomy for all users.

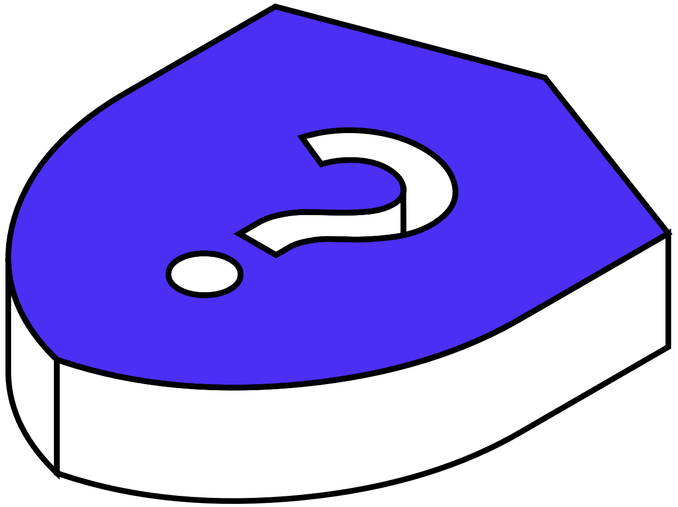


# Core Research Questions

1. How do African digital financial platforms currently enable or fail to prevent financial abuse and coercive control?

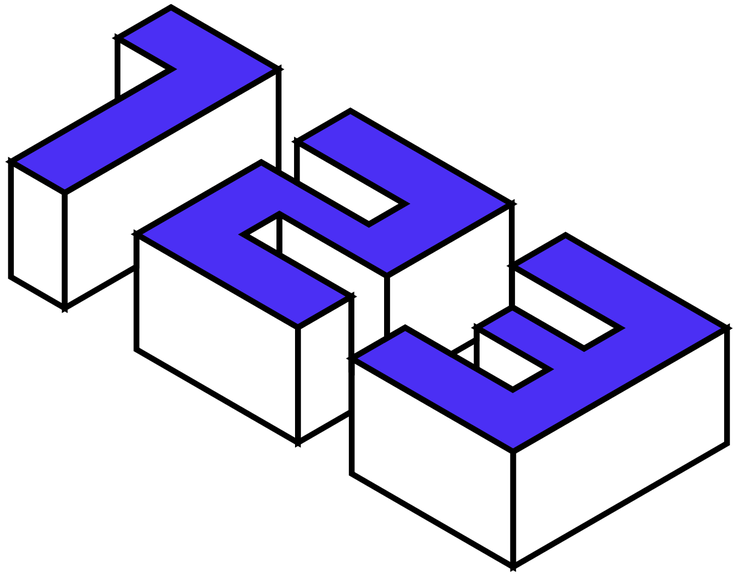
2. To what extent do existing trust and safety measures including user controls, reporting mechanisms, and platform policies explicitly address financial abuse, particularly in the context of gender-based and domestic violence?

3. What design, policy, or operational changes can these platforms adopt to better detect, prevent, and respond to financial abuse against vulnerable users?



# Methodology

This research combined platform review and red teaming methodologies to evaluate how selected African digital financial platforms address or fail to address the risks of financial abuse and coercive control. Red teaming, a recognized approach in trust and safety research, involves simulating harmful use cases to identify platform vulnerabilities, particularly when real-world data is scarce due to underreporting, stigma, or privacy concerns.

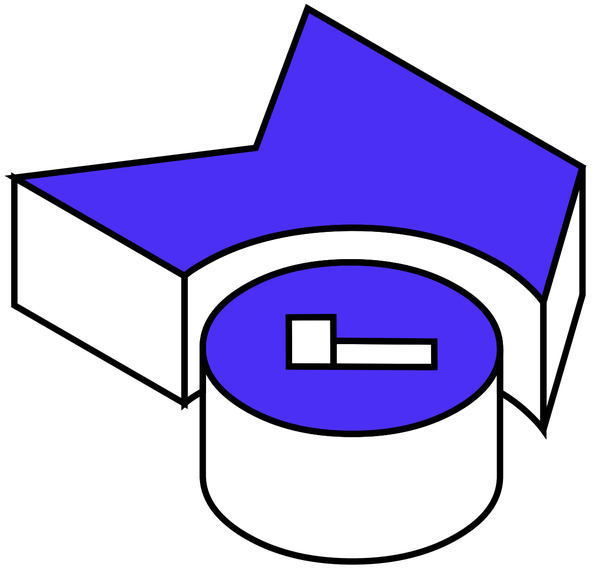


# Platform Selection

We focused on widely-used platforms that have driven significant financial inclusion across diverse African regions:

- Opay
- Moniepoint
- MTN Mobile Money (MoMo)

**These platforms were selected based on their market share, user base size, and relevance to low- and middle-income users, who are often most vulnerable to domestic violence and coercive control.**



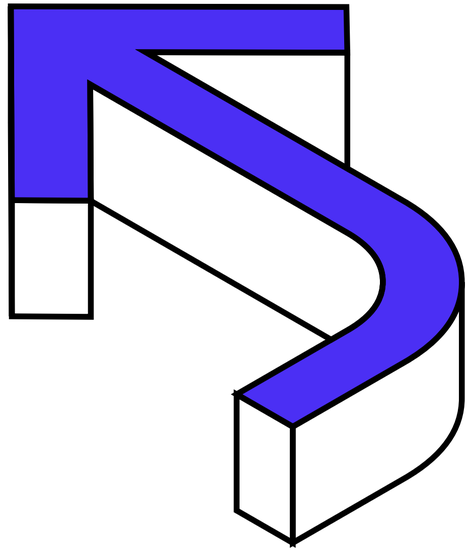
# Review Criteria

**Each platform was evaluated using the following trust and safety-focused criteria:**

- **User Privacy and Control Features:**
  - Ability to block or mute other users.
  - Ability to control who can send payments or messages.
- **Abuse Reporting Mechanisms:**
  - Existence of clear and accessible reporting channels for financial abuse.
  - Options for flagging abusive or suspicious transactions.
- **Authentication and Account Security:**
  - Default use of multi-factor authentication (MFA).
  - Options for secure recovery of accounts compromised by abusers.
- **Policy Recognition:**
  - Whether Terms of Service, Community Guidelines, or Help Center materials explicitly acknowledge financial abuse, harassment, or coercive control.
- **User Support Services:**
  - Availability of trauma-informed support (e.g., help for victims of financial abuse or domestic violence).
- **Detection and Prevention Systems:**
  - Presence (or absence) of proactive abuse detection (e.g., keyword filtering in transaction notes).

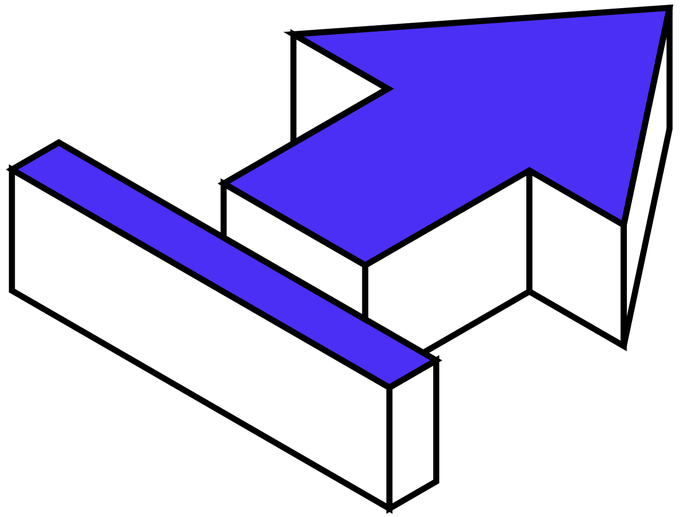
# Review Process

- Publicly available documentation (Terms of Service, Privacy Policies, User Guides) was analyzed.
- Platform apps were downloaded and tested to explore user functionalities related to blocking, reporting, and security settings.
- Where applicable, customer service channels were contacted to simulate a user experience report of suspected financial abuse.



# Limitations

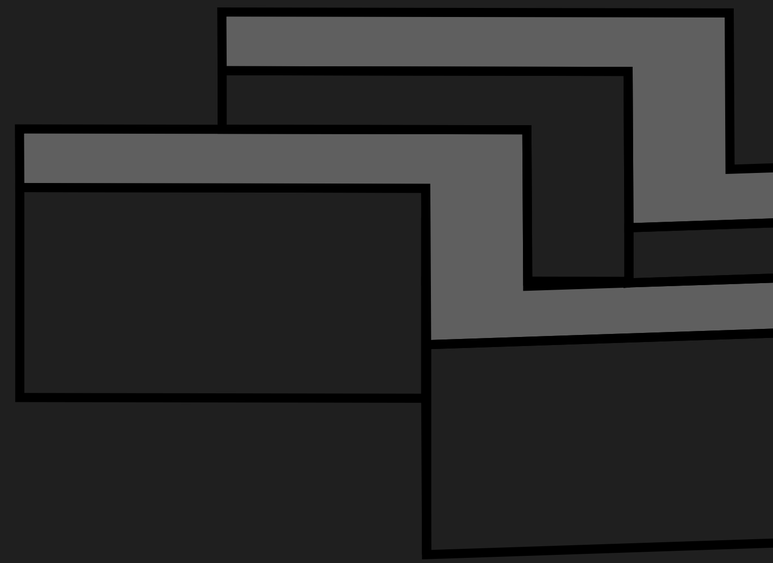
- Some platforms may have back-end abuse detection mechanisms not visible to public users.
- The review is based on documentation and app interface at the time of research; platform updates may occur afterward



# Findings

This section presents key insights from the platform review and red teaming exercises, structured around the core trust and safety criteria used in the methodology. Each platform is analyzed individually, followed by a cross-platform analysis to identify patterns, gaps, and opportunities for reform.

# Platform-Specific Summaries



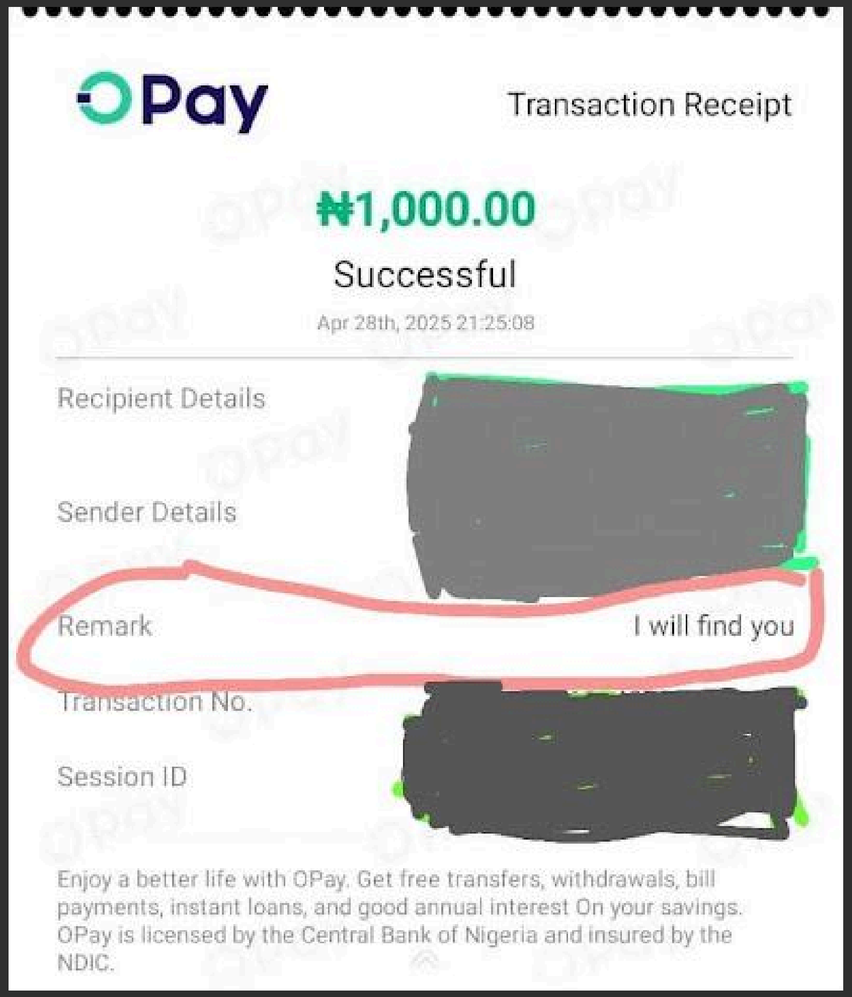
# Opay

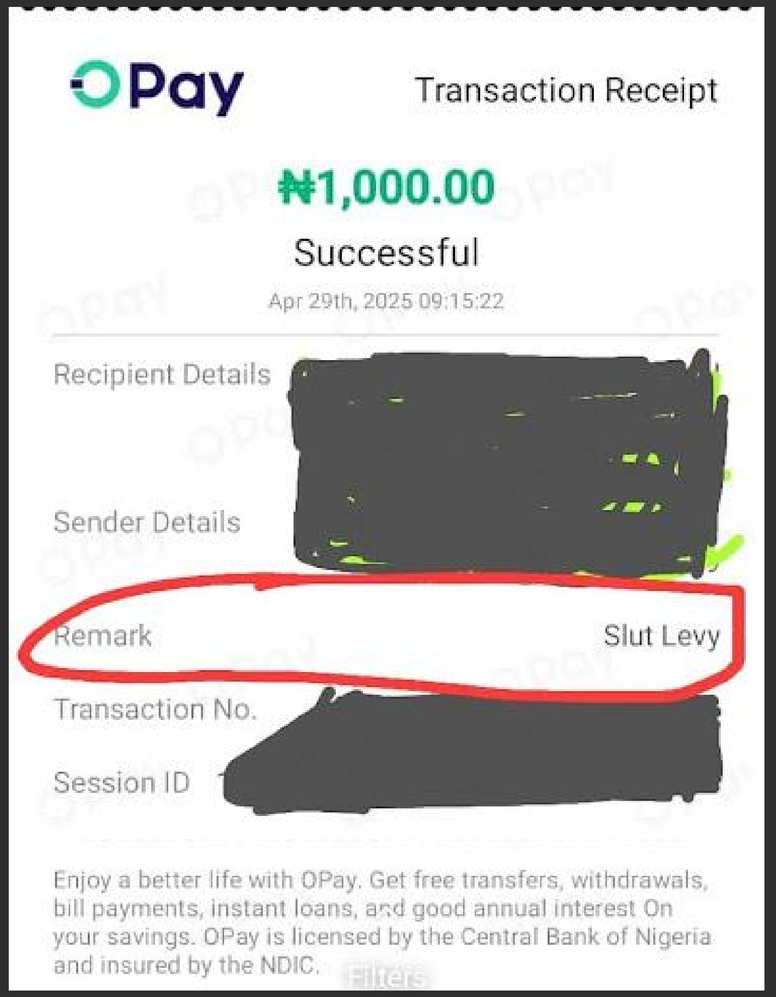
OPay is a prominent African fintech company established in 2018 and headquartered in Lagos, Nigeria. It has rapidly grown to become one of the continent's most widely used digital financial platforms. With over 50 million registered users and more than 10 million daily active users, OPay facilitates a broad range of services including digital wallets, peer-to-peer transfers, bill payments, airtime purchases, savings, lending, and point-of-sale (POS) services for merchants. The platform reportedly processes over $12 billion in transactions every month and supports a network of over 1 million merchants. While its operations are primarily concentrated in Nigeria and Egypt, OPay also has a presence in Pakistan and reported activity in other African countries such as South Africa, Kenya, and Ghana.

OPay has invested in a variety of security features to safeguard its users. These include a Transfer Protection Feature and a Night Guard tool, which enables users to restrict unauthorized transfers during designated hours. The Large Transaction Shield applies stricter verification protocols for high-value transactions, while the Report Scam feature provides a channel for users to flag account theft, erroneous transfers, and internet fraud. In addition, OPay offers user-facing security guides that educate customers on handling scams, lost devices, and password management.

As part of this research, our team conducted a trust and safety red teaming exercise on the OPay platform. In one scenario, we simulated a case of coercive messaging via small repeated transfers—an abuse tactic increasingly seen on digital payment platforms—to assess whether users had adequate options to block, report, or filter such interactions.

## Scenario: A team member simulated the experience of a survivor of domestic abuse  being targeted with multiple low-value transactions containing harassing messages.


OPay
Transaction Receipt
₦1,000.00
Successful
Apr 28th, 2025 21:25:08
Recipient Details
Sender Details
Remark
I will find you
Transaction No.
Session ID
Enjoy a better life with OPay. Get free transfers, withdrawals, bill payments, instant loans, and good annual interest On your savings. OPay is licensed by the Central Bank of Nigeria and insured by the NDIC.


OPay
Transaction Receipt
₦1,000.00
Successful
Apr 29th, 2025 09:15:22
Recipient Details
Sender Details
Remark
Slut Levy
Transaction No.
Session ID
Enjoy a better life with OPay. Get free transfers, withdrawals, bill payments, instant loans, and good annual interest On your savings. OPay is licensed by the Central Bank of Nigeria and insured by the NDIC.

# 1. Platform: Opay

## a. User Privacy and Control Features

- Can users block or restrict senders? — No
- Can users control who sends them money/ messages? — No filtering options

## b. Abuse Reporting Mechanisms

- Is there a reporting feature for abuse or harassment? — Customer service was a chatbot that already had preloaded responses for specific questions especially regarding fraud; no category for abuse or financial coercion

## c. Authentication and Account Security

- Multi-factor authentication (MFA) available? — Yes
- Secure recovery for compromised accounts? — Yes, but may require ID verification

## d. Policy Recognition of Abuse

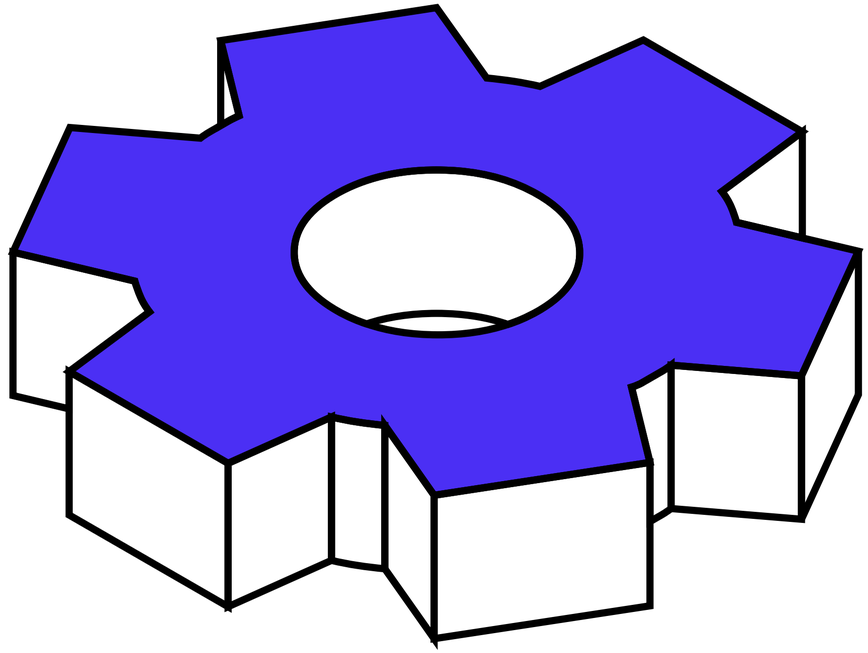
- Do Terms of Service acknowledge financial abuse or coercive control? — No
- Any support pages mentioning abuse? — No

## e. User Support Services

- Dedicated help for victims of abuse? — Not available

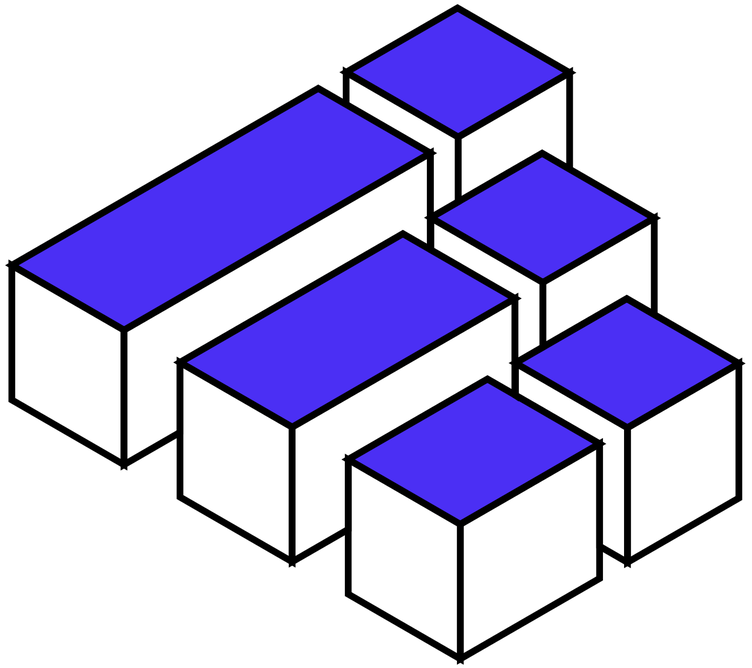
## f. Detection and Prevention Systems

- Keyword filtering or AI moderation for message notes? — Not present



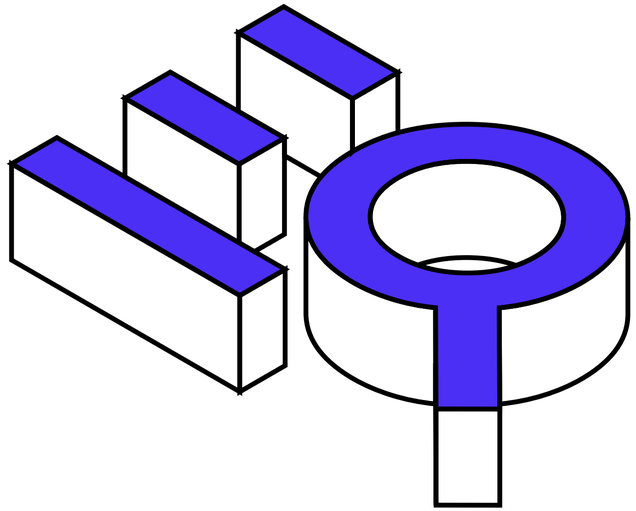
# Red Teaming Scenario Summary

Simulated coercive messaging test showed repeated abusive notes sent with micro-transfers. No mitigation options were found. Customer service was unresponsive to emotional safety concerns.



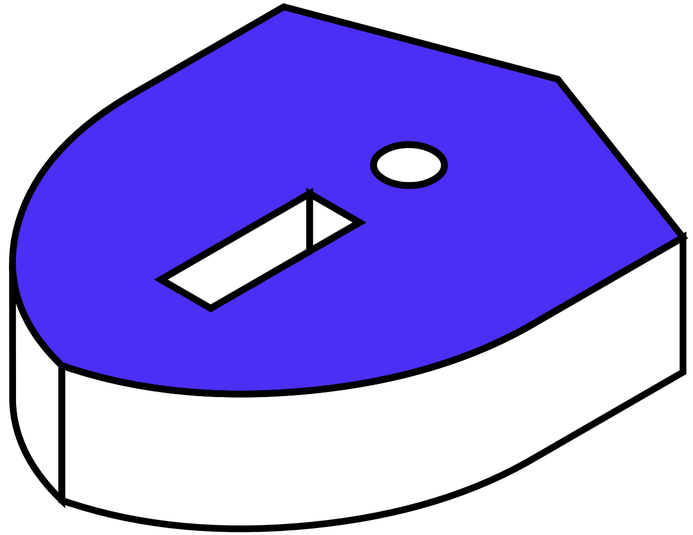
# Observation:

- No option for users to block or restrict who can send them the sender from initiating transactions.
- Transaction message notes were unfiltered, even when they contained language that could reasonably be flagged as threatening.
- Customer service was a chatbot that already had preloaded responses for specific questions especially regarding fraud
- No Abuse reporting channels specific to financial abuse.
- Staff training to recognize signs of financial abuse versus routine fraud.



# Recommendation:

- Build a financial abuse reporting category separate from fraud.
- Train Trust & Safety staff on trauma-informed response protocols.



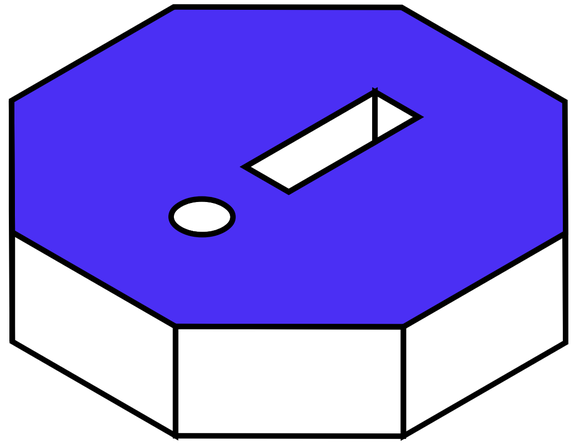
# Moniepoint

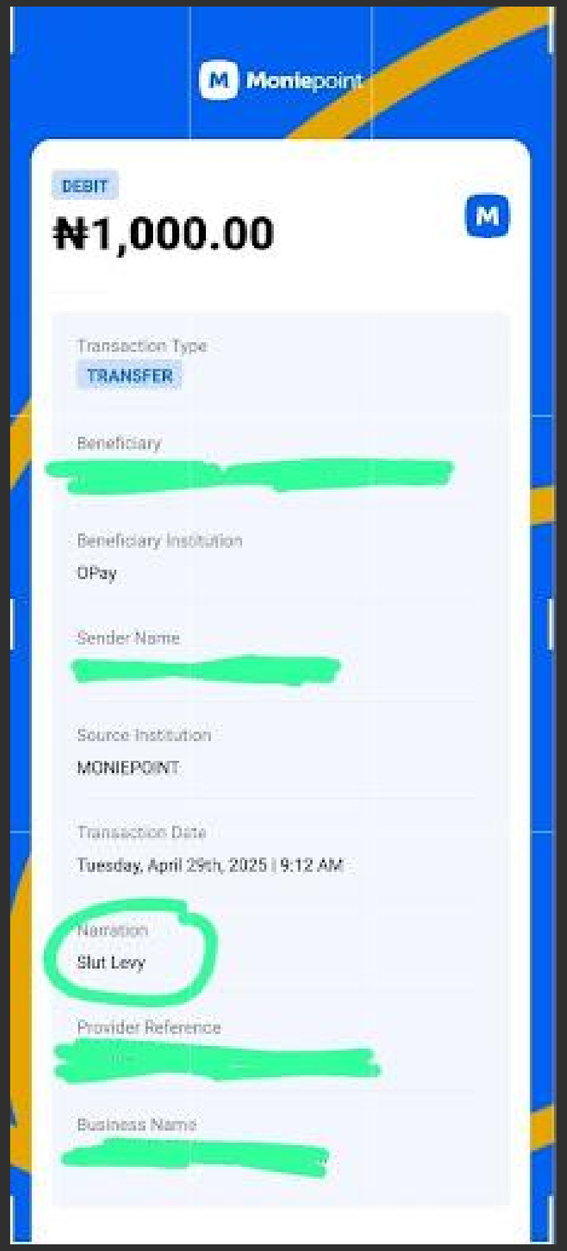
Moniepoint Inc., formerly known as TeamApt, is a Nigerian fintech company founded in 2015. Headquartered in Lagos, Nigeria, Moniepoint has evolved into an all-in-one financial ecosystem, offering services such as digital banking, payment processing, credit facilities, and business management tools. The company primarily serves small and medium-sized enterprises (SMEs) and individual consumers, aiming to enhance financial inclusion across Nigeria.
As of 2025, Moniepoint processes over 800 million transactions monthly, totaling more than $17 billion in transaction value. The platform supports over 10 million businesses and individuals, with its Point of Sale (POS) terminals handling a significant portion of Nigeria's POS transactions. Moniepoint's services are accessible across all 774 local government areas in Nigeria, making it a ubiquitous presence in the country's financial landscape.

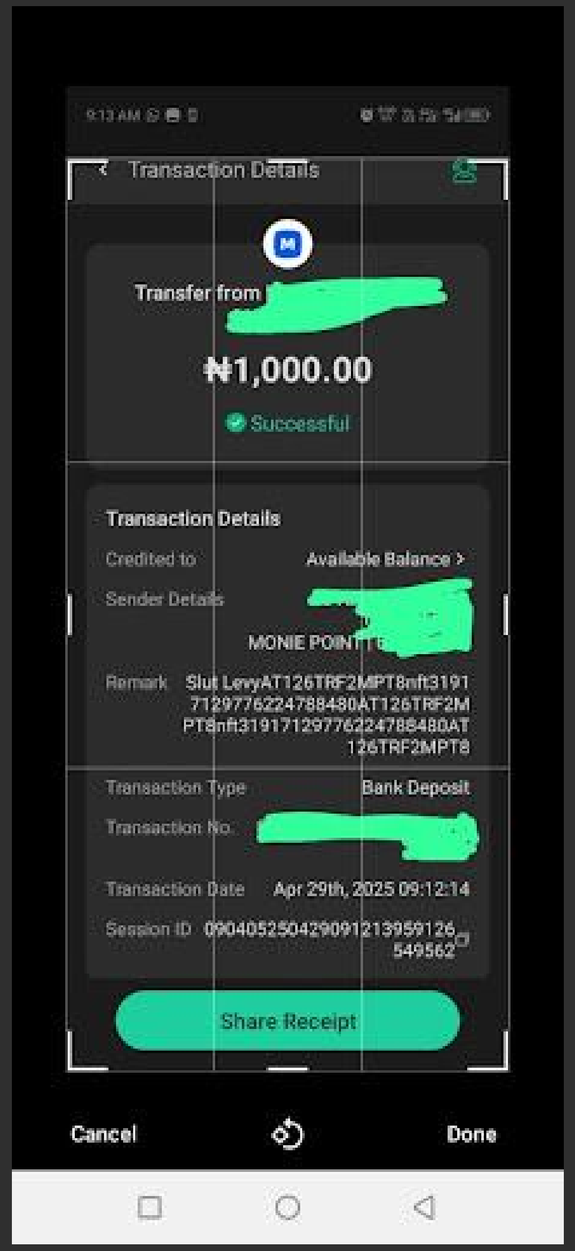
In October 2024, Moniepoint achieved "unicorn" status after raising $110 million in a Series C funding round led by Development Partners International, with participation from Google's Africa Investment Fund, Verod Capital, and Lightrock. This funding is intended to support the company's expansion across Africa and the development of comprehensive digital financial services, including foreign exchange and credit options.Moniepoint has also been recognized as Africa's fastest-growing fintech by the Financial Times for two consecutive years, reflecting its rapid growth and significant impact on the continent's financial services sector.In addition to its business-focused services, Moniepoint launched personal banking services in July 2023, further broadening its customer base and reinforcing its commitment to financial inclusion.

# Simulated Case: Absence of Abuse Reporting on Moniepoint

Scenario: A red team member simulated being a user targeted by a coordinated online group after sharing personal photos and opinions on a women's rights forum. Multiple users, as part of a mobbing campaign, sent small payments ranging from N1000 with degrading messages such as “Slut levy”, “This is all you’re worth”, and “We fund your shame.” The repeated transactions cluttered the user’s payment history, triggered emotional distress, and served as a form of financial harassment masked as legitimate use of the platform.




Moniepoint
DEBIT
₦1,000.00
Transaction Type
TRANSFER
Beneficiary
Beneficiary Institution
OPay
Sender Name
Source Institution
MONIEPOINT
Transaction Date
Tuesday, April 29th, 2025 | 9:12 AM
Narration
Slut Levy
Provider Reference
Business Name


Transaction Details
Transfer from
₦1,000.00
Successful
Transaction Details
Credited to
Available Balance >
Sender Details
MONIE POINT
Remark
Slut LevyAT126TRF2MPT8nft3191712977622478848OAT126TRF2MPT8nft319171297762247884 80AT126TRF2MPT8
Transaction Type
Bank Deposit
Transaction No.
Transaction Date
Apr 29th, 2025 09:12:14
Session ID
090405250429091213959126549562
Share Receipt
Cancel
Done

# 2. Platform: Moniepoint

## a. User Privacy and Control Features

- Can users block or restrict senders? — No
- Can users control who sends them money/ messages? — No filtering options

## b. Abuse Reporting Mechanisms

- Is there a reporting feature for abuse or harassment? — Customer service was a chatbot that already had preloaded responses for specific questions especially regarding fraud; no category for abuse or financial coercion

## c. Authentication and Account Security

- Multi-factor authentication (MFA) available? — Yes
- Secure recovery for compromised accounts? — Yes, but may require ID verification

## d. Policy Recognition of Abuse

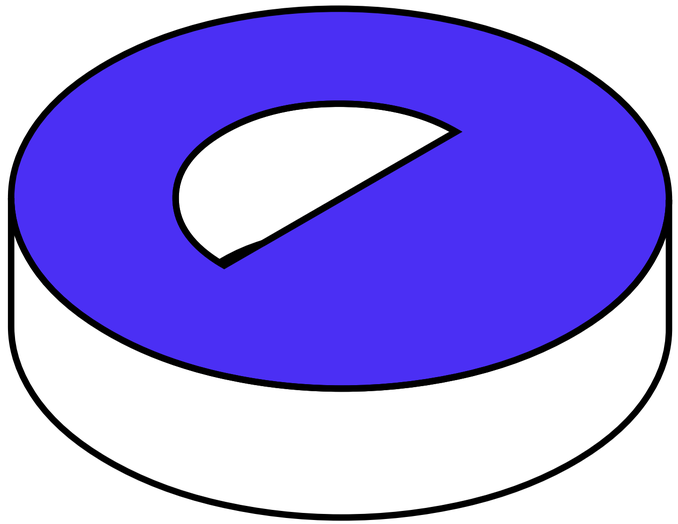
- Do Terms of Service acknowledge financial abuse or coercive control? — No
- Any support pages mentioning abuse? — No

## e. User Support Services

- Dedicated help for victims of abuse? — Not available

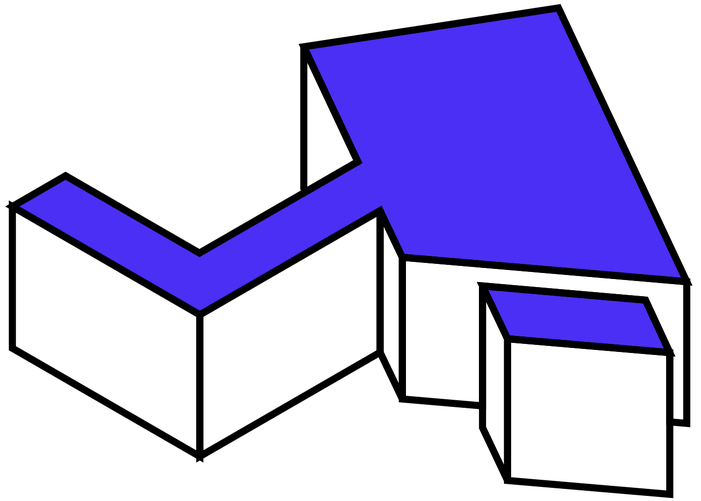
## f. Detection and Prevention Systems

- Keyword filtering or AI moderation for message notes? — Not present



# Observation:

- No dedicated abuse reporting category.
- No acknowledgement of financial abuse or gender-based violence in Help Center content.
- There is a long wait time to report abuse complaints



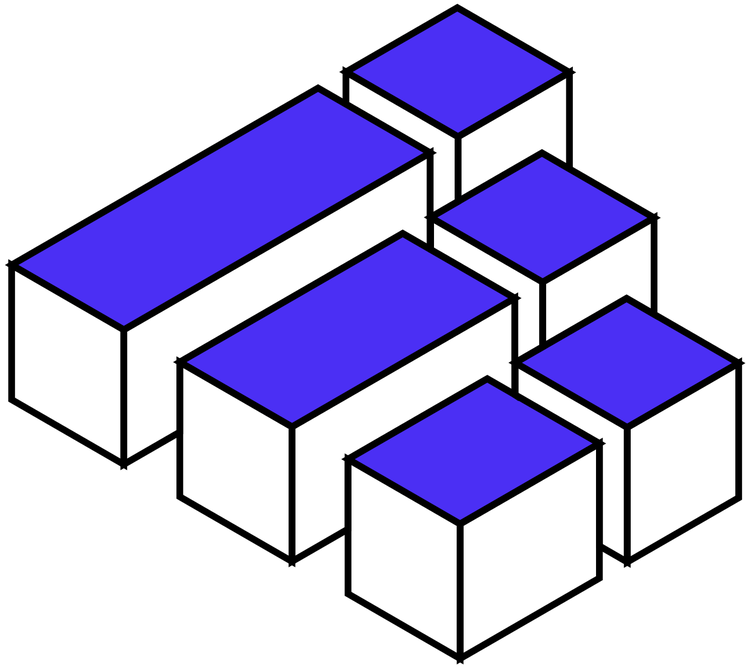
# Mobile Money

Financial and economic abuse – including controlling a partner's access to money and resources – is recognized under Ghana's Domestic Violence Act (2007) as a punishable form of domestic violence ugspace.ug.edu.gh. In Ghana, roughly 27.7% of women report experiencing domestic violence, highlighting how common abuse is ourhomelandghana.com. At the same time, digital finance has become ubiquitous: over 17 million Ghanaians use MTN's Mobile Money (MoMo) service mtn.com.gh. MoMo offers convenience and inclusion, especially for women (who can open wallets without a bank account), but its design and policies also present opportunities for misuse by abusive partners grameenfoundation.orggrameenfoundation.org. This report examines how MoMo's features, security, and practices can both empower users and leave them vulnerable to coercive financial control. We review MoMo's platform documentation and related research, then identify gaps and make recommendations to better protect women from financial abuse.

# Red Teaming
# Scenario Summary

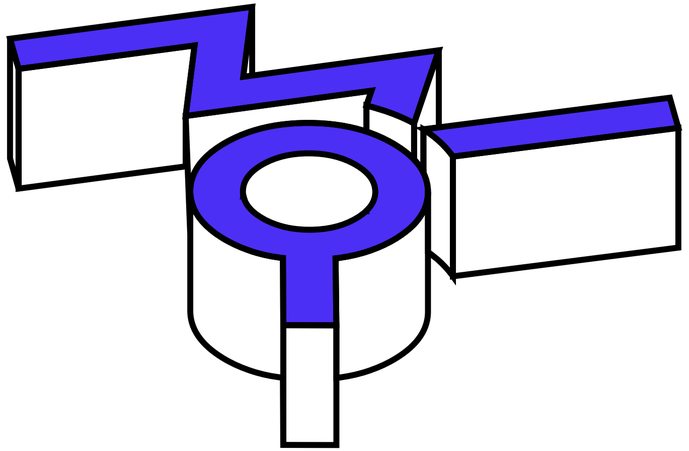
**Scenario Description:**

A red team member simulated being a user attempting to disengage from an abusive relationship. The simulated abuser sent GHS 5.38 with messages containing manipulative and threatening text such as “You’ll regret this” & "You'll regret this and I will find you.”



# Findings:

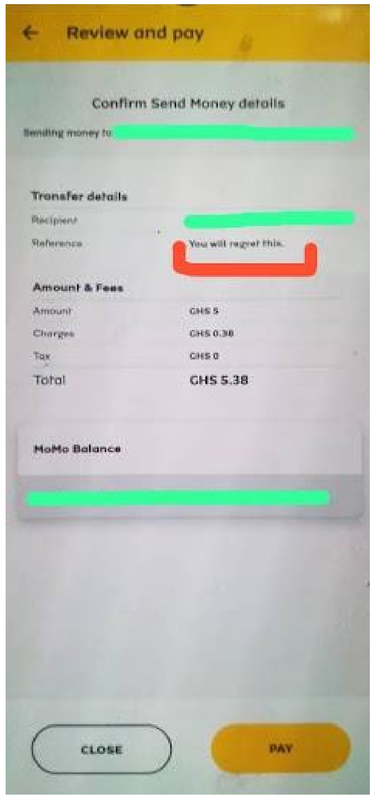
- The receiver has no way to block the sender.
- Harassing messages were delivered without restriction.
- No option was provided to report, mute, or flag these interactions.
- The emotional impact of being constantly re-targeted through a financial app was dismissed.

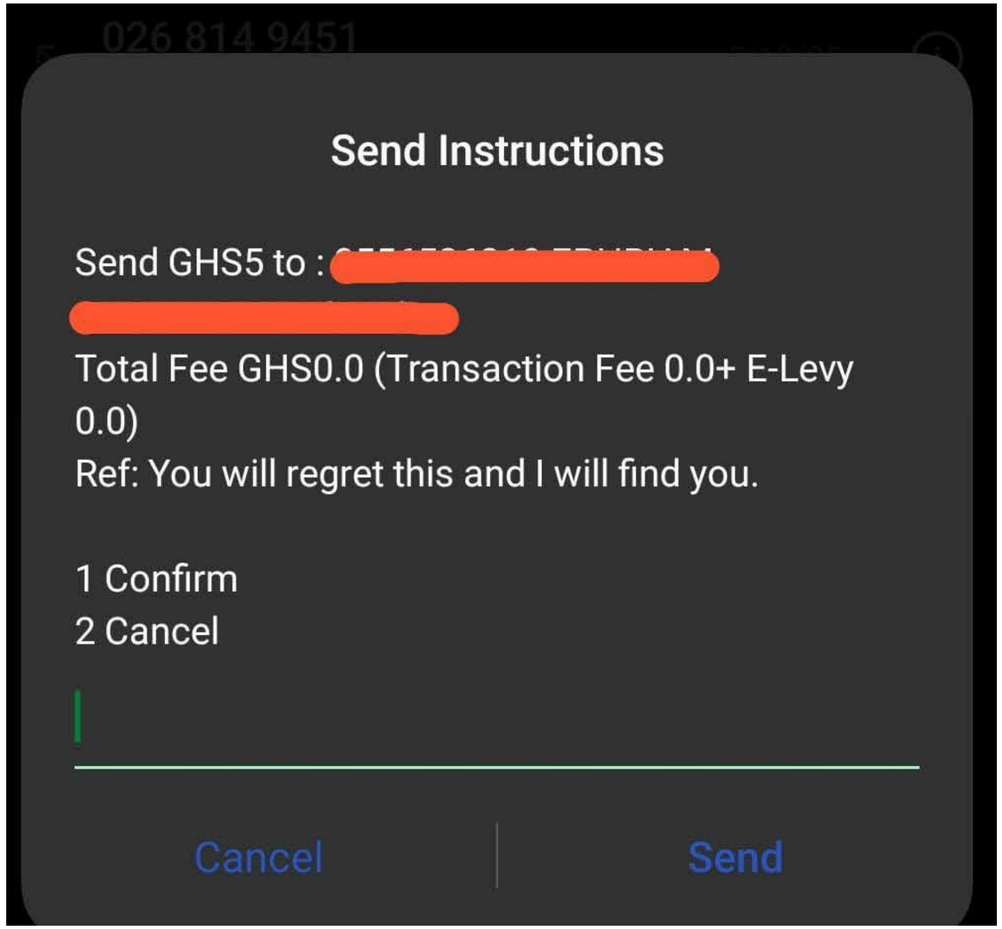


# Observation:

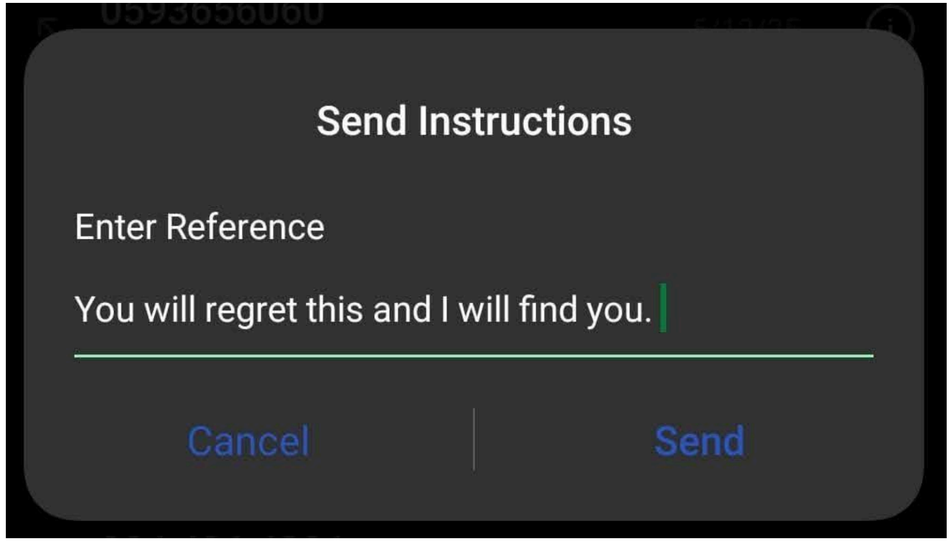
The Momo App currently lacks basic trust and safety protections against coercive financial abuse. It assumes all transfers are benevolent or purely transactional. The lack of sender controls, reporting mechanisms, and emotional safety design creates a serious vulnerability—especially for women and at-risk users in domestic violence contexts.
Below are screenshots of the both app and USSD of the transactions.

**NB: The MoMo app does not allow screenshots.**



Send Instructions
Send GHS5 to :
Total Fee GHS0.0 (Transaction Fee 0.0+ E-Levy 0.0)
Ref: You will regret this and I will find you.
1 Confirm
2 Cancel
Cancel
Send


Current Balance
Reference:
You will regret this and I will find you from
Transaction ID: 57529319934. TRANSACTION FEE: 0.00
7:51 p.m.


Send Instructions
Enter Reference
You will regret this and I will find you.
Cancel
Send

# 3. Platform: Momo App (MTN Ghana)

## a. User Privacy and Control Features

Can users block or restrict senders? — No
The Momo App does not provide users with the ability to block or restrict specific individuals from sending money or attaching messages. This leaves survivors of abuse vulnerable to repeated unwanted contact and coercive financial interactions.

- **Can users control who sends them money/messages? — No filtering options**

There are no visible privacy settings that allow users to whitelist or blacklist senders or to turn off receipt of messages attached to transactions.

## b. Abuse Reporting Mechanisms

**Is there a reporting feature for abuse or harassment? — No.**
The app does not have a built-in option to report abusive transaction messages. Customer support is general-purpose and lacks a specific category or form for harassment, abuse, or coercive behavior.

## c. Authentication and Account Security

**Multi-factor authentication (MFA) available? — Yes.**

- The platform uses PIN codes and SMS-based authentication, but this is primarily focused on financial fraud prevention—not behavioral or interpersonal abuse.

**Secure recovery for compromised accounts? —Partially.**

- Recovery via ID verification and customer service is possible, but the process may not prioritize safety in abuse contexts (e.g., abusive partner controlling account recovery).

## d. Policy Recognition of Abuse

**Do Terms of Service acknowledge financial abuse or coercive control? —No.**
There is no recognition of gender-based financial abuse, digital coercion, or misuse of the platform for interpersonal harm.

**Any support pages mentioning abuse? — No.**
Public-facing help resources do not mention coercive control, domestic abuse, or emotional safety risks in relation to financial transactions.

## e. User Support Services

**Dedicated help for victims of abuse? —Not available.**
There are no visible links to support resources for survivors of abuse, nor are there staff or processes trained to respond to safety-based misuse of the platform.

## f. Detection and Prevention Systems

**Keyword filtering or AI moderation for message notes? —Not present.**
The platform does not screen messages attached to transactions. Abusive or threatening language can be sent repeatedly via micro-transfers with no automated flagging or filtering.

# Recommendation:

1. **Implement Sender Blocking Features** – Allow users to block or restrict incoming transfers and messages from selected accounts.

2. **Add Abuse Reporting Options** – Introduce in-app abuse reporting specifically for harassment and coercive control through financial interactions.

3. **Message Filtering & Flagging** – Use simple keyword detection (e.g., threats, coercive language) to flag potential abuse patterns for review.

4. **Terms of Service Update** – Explicitly include language about financial abuse, coercive control, and behavioral misuse of the platform.

5. **Partner with Domestic Violence Organizations** – Provide help resources, survivor-informed training for support agents, and safety design improvements.

6. **Create a Privacy Mode** – Allow users to hide transaction messages or automatically decline low-value transfers under a set threshold.

# Cross-Platform Analysis

| Criteria | Opay | Moniepoint | MTN Momo |
|---|---|---|---|
| Block/Restrict Users | ❌ | ❌ | ❌ |
| Report Abuse | ❌ | ❌ | ❌ |
| MFA | ✅ | ✅ | ✅ |
| Abuse Acknowledged in Policy | ❌ | ❌ | ❌ |
| Victim Support Features | ❌ | ❌ | ❌ |
| Keyword/Message Filtering | ❌ | ❌ | ❌ |

(Legend: ✅ Yes | ❌ No | 🟠 Partial or unclear)

# Key Patterns and Gaps

- **Lack of User-Control Features:** The platforms do not allow users to block senders or filter transaction messages, leaving users exposed to ongoing harassment.
- **Policy Silence on Abuse:** No reviewed platform explicitly acknowledges financial abuse, coercive control, or online gender-based violence in their terms or user help resources.
- **Weak Reporting and Support:** Reporting flows are generic and not designed with abuse contexts in mind. Victims are often advised to ignore or endure.
- **Security ≠ Safety:** While platforms have robust anti-fraud measures (e.g., MFA, encryption), these do not translate to safety from interpersonal or gender-based abuse.

# Platform Review Checklist: Financial Abuse Safeguards in African Digital Payment Platforms

| Review Area | Checklist Questions | Scoring Guide (Yes / Partial / No / Not Found) |
|---|---|---|
| **1. User Privacy & Control** | Can users block or mute other users? | |
| | Can users restrict who can send them money or messages? | |
| **2. Abuse Reporting Mechanisms** | Is there a visible, accessible way to report abuse related to transactions? | |
| | Can users flag messages or transaction notes as abusive? | |
| | Do the Help Center or FAQs include steps for reporting abuse or coercion? | |
| **3. Authentication & Account Security** | Is multi-factor authentication (MFA) required or strongly recommended? | |
| | Are there account recovery options designed to protect victims of abuse (e.g. changing credentials securely)? | |
| **4. Platform Policy Recognition** | Do Terms of Service mention financial abuse, harassment, or coercive control? | |
| | Are there any policies on misuse of the platform for interpersonal abuse? | |
| **5. User Support Services** | Is there reference to support services for victims of domestic or gender-based violence? | |
| | Are customer service agents trained to recognize and respond to abuse-related complaints? | |
| **6. Detection & Prevention Systems** | Is there proactive monitoring for abusive or threatening language in transaction notes? | |
| | Are repeat micro-transactions (used for stalking/intimidation) flagged or limited? | |
| **7. User Experience Testing** | Are blocking/reporting functions easy to find and use in the app? | |
| | How did the platform respond to a simulated report of financial abuse? (Record response time, tone, usefulness) | |
| | | |

# Problem Statement

While African digital payment platforms have prioritized financial access, they have largely neglected the safety of users vulnerable to financial exploitation and abuse. Most platforms have security centers or protocols focused on fraud and scams, which are critical for financial system integrity. However, these mechanisms often overlook interpersonal or gender-based financial abuse where perpetrators misuse payment systems to maintain coercive control, stalk, intimidate, or harass victims especially women which is a trust and safety issue because it **directly threatens user well-being, platform integrity, and user confidence.**

This gap in user protection not only exposes vulnerable individuals to harm but also undermines broader user trust and platform integrity. Addressing financial abuse as a trust and safety issue is essential to building truly inclusive and secure digital economies in Africa.

**Specifically:**

**Exploitation and Coercion:**
Abusers can misuse payment platforms to **control, exploit, or stalk** individuals — e.g., by sending unwanted payments with threatening messages, stealing money via unauthorized access, or demanding repayments under duress.

**Loss of Trust:**
If users feel **unsafe financially** — because the platform allows harassment through money transfers, scams, or financial blackmail — they lose trust in the platform and may stop using it.

**Psychological Harm:**
Financial abuse isn't just economic; it causes fear, stress, shame, and trauma, especially for vulnerable groups (like domestic violence survivors). Platforms have a duty of care to protect against this.

**Fraud and Security Risks:**
Financial abuse often overlaps with **fraud, account takeovers**, and **money laundering** — major **trust and safety** concerns that can trigger legal penalties, reputational damage, and regulatory scrutiny.

**Inadequate Reporting Tools:**
If platforms lack ways for users to **report financial abuse** or **block bad actors**, it compounds harm and shows a failure to prioritize user safety.

**Power Imbalances:**
Without proper safeguards, payment platforms can **enable abusers to maintain financial control** over others, reinforcing broader cycles of abuse.

# Platform-Specific Summaries

### 1. Platform: Opay

#### a. User Privacy and Control Features

- ✅ Can users block or restrict senders? — No
- ✅ Can users control who sends them money/messages? — No filtering options

#### b. Abuse Reporting Mechanisms

- 🟠 Is there a reporting feature for abuse or harassment? — Generic complaint form; no category for abuse or financial coercion

#### c. Authentication and Account Security

- ✅ Multi-factor authentication (MFA) available? — Yes
- ✅ Secure recovery for compromised accounts? — Yes, but may require physical ID verification

### d. Policy Recognition of Abuse

- ❌ Do Terms of Service acknowledge financial abuse or coercive control? — No
- ❌ Any support pages mentioning abuse? — No

### e. User Support Services

- ❌ Dedicated help for victims of abuse? — Not available

### f. Detection and Prevention Systems

- ❌ Keyword filtering or AI moderation for message notes? — Not present

## Red Teaming Scenario Summary

Simulated coercive messaging test showed repeated abusive notes sent with micro-transfers. No mitigation options were found. Customer service was unresponsive to emotional safety concerns.

## 2. Platform: Moniepoint

### a. User Privacy and Control Features

- ✅ Can users block or restrict senders? — No
- ✅ Can users control who sends them money/messages? — No filtering options

### b. Abuse Reporting Mechanisms

- 🟠 Is there a reporting feature for abuse or harassment? — Generic complaint form; no category for abuse or financial coercion

### c. Authentication and Account Security

- ✅ Multi-factor authentication (MFA) available? — Yes
- ✅ Secure recovery for compromised accounts? — Yes, but may require physical ID verification

### d. Policy Recognition of Abuse

- ❌ Do Terms of Service acknowledge financial abuse or coercive control? — No
- ❌ Any support pages mentioning abuse? — No

### e. User Support Services

- ❌ Dedicated help for victims of abuse? — Not available

### f. Detection and Prevention Systems

- ❌ Keyword filtering or AI moderation for message notes? — Not present

## Red Teaming Scenario Summary

Simulated coercive messaging test showed repeated abusive notes sent with micro-transfers. No mitigation options were found. Customer service was unresponsive to emotional safety concerns.

### 3. Platform: Momo (MTN Ghana)

#### a. User Privacy and Control Features

- ✅ Can users block or restrict senders? — No
- ✅ Can users control who sends them money/messages? — No filtering options

#### b. Abuse Reporting Mechanisms

- 🟠 Is there a reporting feature for abuse or harassment? — Generic complaint form; no category for abuse or financial coercion

#### c. Authentication and Account Security

- ✅ Multi-factor authentication (MFA) available? — Yes
- ✅ Secure recovery for compromised accounts? — Yes, but may require physical ID verification

### d. Policy Recognition of Abuse

- ❌ Do Terms of Service acknowledge financial abuse or coercive control? — No
- ❌ Any support pages mentioning abuse? — No

### e. User Support Services

- ❌ Dedicated help for victims of abuse? — Not available

### f. Detection and Prevention Systems

- ❌ Keyword filtering or AI moderation for message notes? — Not present

## Red Teaming Scenario Summary

Simulated coercive messaging test showed repeated abusive notes sent with micro-transfers. No mitigation options were found. Customer service was unresponsive to emotional safety concerns.