Responsible Financial Systems (RFS)
Empowering Trust, Driving Inclusion

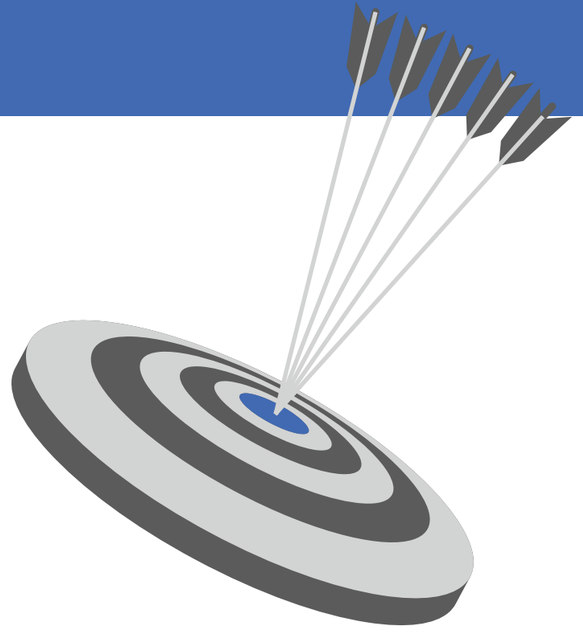
In this third edition of our consumer protection newsletter, we share informative insights from our latest publications and present the PREVENT framework. It serves as a practical checklist that service providers can use to strengthen consumer protection after fraud.

Moreover, this newsletter also features another cunning diary snippet from Kurkuri, our resident fraudster. Take on a fun challenge to get closer to the consumer protection landscape, one unjumble at a time.

Happy reading!

Our mission

At MSC, we seek to champion consumer protection and build a responsible and inclusive ecosystem. Through our RFS capability, we promote fair treatment, transparency, and user-centric design in the industry. Our research, advocacy, and capacity-building efforts advance consumer rights, enhance trust, and support sustainable inclusion for individuals and communities.



Our evolving framework

What are the ideal steps for resolution after a fraud occurs? The following framework outlines a structured approach to support and streamline the customer's post-fraud recovery journey.

Proactive communication

Are users informed in advance about risks, red flags, and response mechanisms?

Risk detection and reachability

Can the system detect suspicious activity early? Can users easily report fraud and get help?

Education and clarity

Are risks and next steps clearly explained at every touchpoint?

Victim support (Affective response)

Are affected users treated with empathy and respect throughout the resolution process?

Trust assurance (Trust rebuilding)

Are visible actions taken to restore and reinforce confidence in the system?

Nudges for secure behavior

Are users guided through behavioral nudges and reminders to adopt safer practices post-incident?

Escalation pathways (Case resolution)

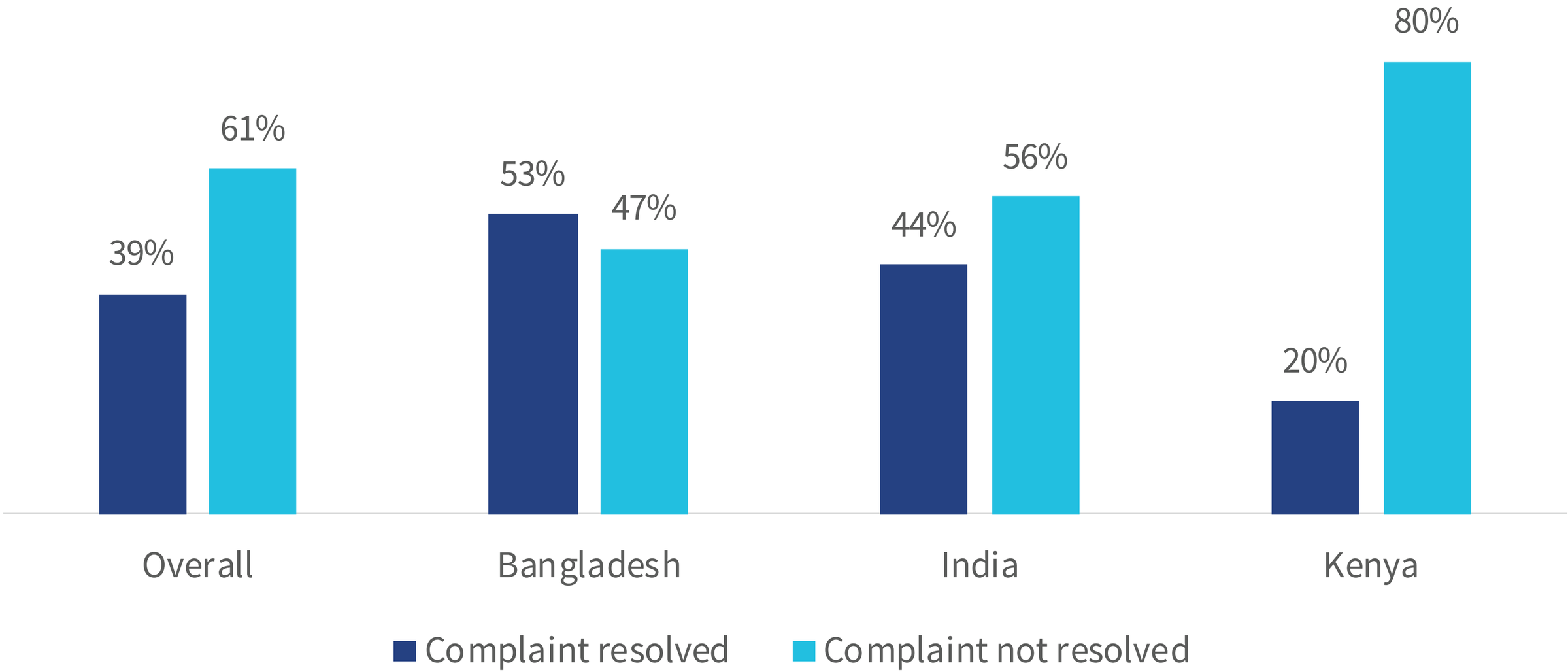
Is there a structured, timely process to resolve grievances and fraud cases?

The PREVENT framework consists of seven key elements: Proactive communication, Risk detection, Education and clarity, Victim support, Escalation pathways, Nudges for recovery, and Trust assurance. Together, these components ensure that users receive timely, structured responses to fraud and are protected before disaster strikes.

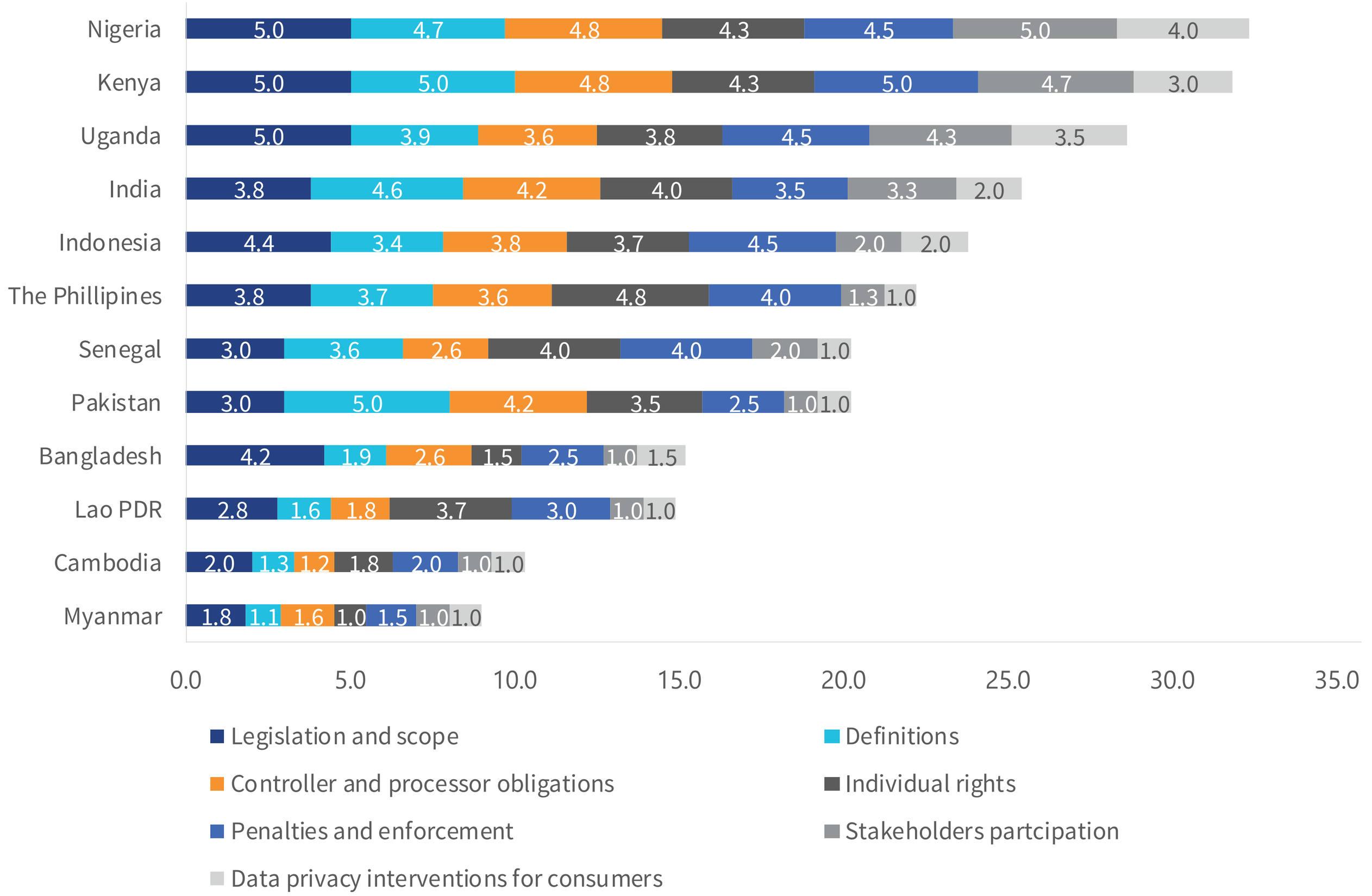
The PREVENT framework focuses on anticipation and mitigation, not just reaction. PREVENT integrates proactive detection with empathetic communication and behavioral shifts to empower organizations to build long-term trust, resilience, and safety in digital systems.

MSC's key research insights

Complaint resolution - a cross country comparison



Our three-country analysis from the report, **Mind the Gap**, shows that 60% of respondents who filed a complaint did not see any resolution. More specifically, Kenya has the poorest complaint resolution among the three countries, with 80% unresolved cases, followed by India with 56% and Bangladesh with 47%.



Our multicountry analysis of **data protection** in Africa and Asia evaluates countries' data protection policies and guidelines. It focuses on key pillars, such as legislation and scope, controller and process obligations, penalties and enforcement, data privacy interventions, definitions, individual rights, and stakeholder participation.

The scores for Asian and African countries across these pillars reveal a mixed performance. Some countries, such as Nigeria and India, perform well across all pillars. Other countries, such as the Philippines and Senegal, lag in specific areas, such as consumer data privacy protection, stakeholder participation, and clearly defined obligations for data controllers and processors. A few countries, such as Cambodia and Myanmar, lag in most pillars and need to strengthen their data protection systems significantly.

Latest publication

Toward a trusted digital nation: A multicountry analysis on data protection in Africa and Asia

Building LMI communities' confidence in digital financial services: A behavioral science approach

Mind the gap: Closing the loopholes in consumer protection in digital financial services

Building trust by design: Eliminating dark patterns in digital financial services

Building trust by design: Eliminating dark patterns in digital financial services

Dear diary,

Yours truly AKA Rizqi Kurkuri landed in Jakarta last month. And today, he became both a child in crisis and a FinTech visionary. Two identities, one SIM card. Oh, what a deliciously strange dance it has been!

It began, as always, with a message. I crafted it the way I always do, short, urgent, full of motherly guilt: "*Ma, aku butuh pula, darurat, nanti aku jelasin, ini no temen aku*." ("Mom, I need phone credit, it is an emergency, I will explain later, this is my friend's number"). An old trick, still oddly effective. Four messages out, and within 10 minutes, two transfers had landed. No questions, no hesitation. Just pure, maternal panic. It warms the heart. Or would, if I had one.

But it was not just *pula* I was after today. The real con began at noon. You see, after I had impersonated the child, I shape-shifted into an investment guru, complete with a fake Bappebti license and a Telegram channel called "Robot untung 2025" ("Profit bot 2025").

Why this combination, you ask? Because I have discovered something, dear diary. The reflex that makes a mother send pula without hesitation is the reflex that makes a retiree sink their savings into a robo trading platform that promises 3% daily returns. It is not greed. It is love, fear, and the desperate hope that technology will save them.

So, I wove the story: A passive income bot, crypto-backed, with a government "certificate", expertly forged using Canva. I hosted a webinar where I showed dashboards complete with green arrows, growing balances, and motivational quotes like, "*Uang tidur pun bisa bekerja.*" ("Even sleeping money can work for you.")

By mid-afternoon, an *ibu-ibu* from Bandung messaged me. Her daughter had warned her it might be a scam. I reassured her gently, "Ma'am, those rumors are spread by jealous people who could not follow simple withdrawal steps." She paused, and almost like déjà vu, she typed, "*Anak saya tetap bilang hati-hati. Tapi saya percaya kamu*." ("My child still says to be careful. But I trust you.") She sent five million rupiah. I sent her a PDF receipt, which was branded and completely fake.

As I switched off for the day, it hit me. Is it not ironic, dear diary? In the morning, I was a child. In the evening, I had become someone who robbed mothers blind. So goes the circle of scams.

Yes, today I made money. But more importantly, I proved a theory: The strongest scams do not rely on code or malware; they prey on love, fear, and trust. The most vulnerable systems are human.

Until later, when I test another theory.

Yours cunningly,
Kurkuri

Digital Arrest

Can You catch the Fraudster?

A fraud has just been reported in the system.
Use the clues below to figure out which digital behavior triggered the red flag.

Can you spot the suspicious activity?

1. The user changed their registered mobile number twice in 24 hours.
2. A transaction attempt was made from a new device at 3 A.M.
3. OTP verification failed four times in a row.
4. The account was accessed from two different states within 10 minutes.
5. The user reported no awareness of any of these actions.

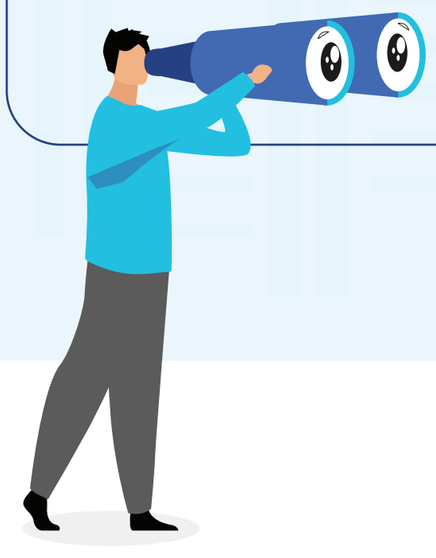
A. Geo-location mismatch

B. Unusual device behavior

C. Failed authentication pattern

D. SIM swap attempt

E. Credential compromise



Answer Key: 1-D, 2-E , 3-B, 4-A, 5-C