ITU Digital Financial Services Security
Episode #8 – Knowledge Sharing
"GSMA Mobile Money Fraud Management Insights"

- José Carlos Sobreira, Director Risk, Fraud and Security at Unitel Angola &
GSMA Africa Fraud and Security Group (AFASG) Chair

AGENDA

1. The GSMA Study Methodology
2. The Mobile Money Fraud Context (Introduction)
3. Main Trends in Mobile Money Fraud
4. Mitigation of Mobile Money Fraud
5. Collaboration with Law Enforcement Authorities
6. Future Outlook on Mobile Money Fraud (Key Take Aways)

1. The GSMA Study Methodology

GSMA Employed a Comprehensive Methodology to Collect Data from Several Sources

1. Geographic Coverage

The study consulted **stakeholders from 34 countries across Africa, Asia, and Latin America**, which have significant mobile money deployments.

2. Stakeholder Involvement

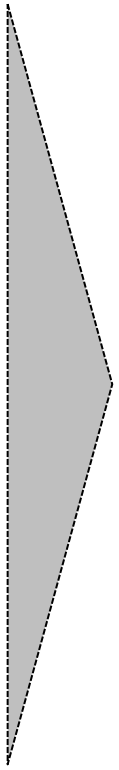
Engagement of a wide diverse range of **stakeholders, including Mobile Operators, Financial Institutions, Technical Providers, Fintech's, and Regulators**.

3. Survey Baseline, Followed By Interviews

GSMA designed and distributed **surveys/questions to the stakeholders** within the mobile money ecosystem, **complemented with in-depth interviews,** conducted to key personnel such as Risk Managers, Fraud Managers, and Senior Executives, from Mobile Operators.

4. Focus Groups Consultation

Focus Groups discussions were organized to gather collective insights from groups of stakeholders.



5. Analysis of Case Studies and Data

Collected and **analyzed fraud case studies from various mobile operators,** which illustrated specific instances of Mobile Money Fraud and the mitigation actions taken.

6. Literature Review

The study also included a **comprehensive review of existing literature on Mobile Money Fraud**, including academic papers, industry reports, and regulatory documents.

7. Specific Entities Consultations

Consultations made with **Regulatory Bodies, Law Enforcement Agencies, and Consumer Protection Organizations**, were also part of the methodology.

8. Validation with Panel Expert

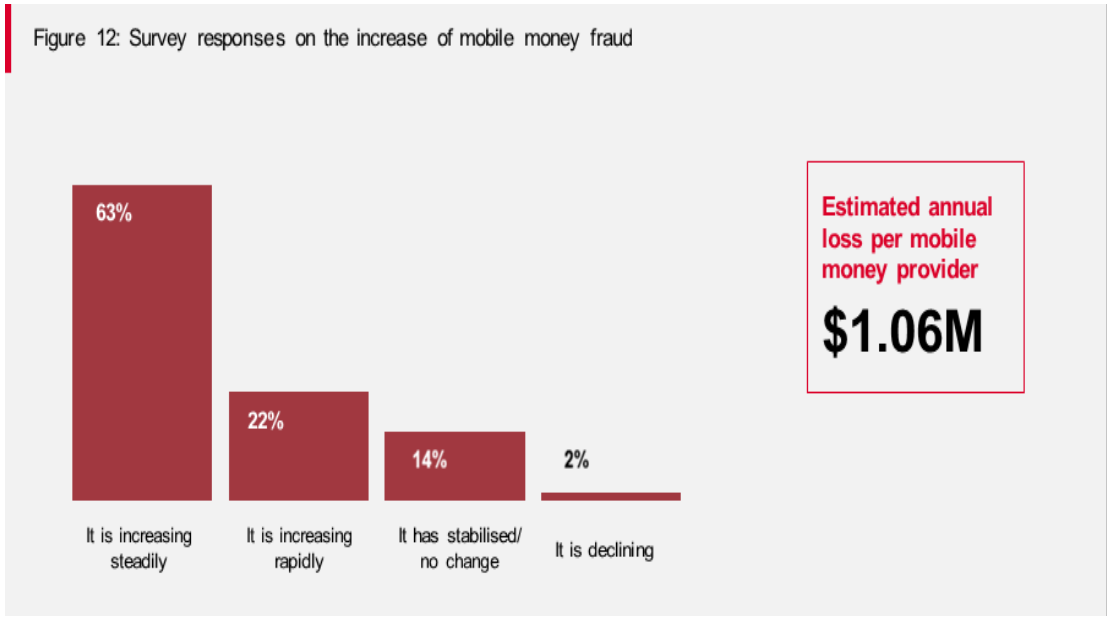
A **validation with panels** consisting of experts in Mobile Money, Cybersecurity, and Fraud Prevention were convened to review the study findings.

2. The Mobile Money Fraud Context (Introduction)

- **The Mobile Money Industry has experienced exponential growth, evidenced by the:**
  - The ***addition of 800 million customers in just five years***, half of which (400M Accounts), occurred during the COVID-19 Pandemic
  - ***Reached USD$1.26 Trillion in transaction value*** with 1.6 Billion Registered Accounts by 2022
  - ***88% increase in Mobile and Online Transactions***, cited as the most significant contributor to the rise in fraud
- **The acceleration was particularly notable during the COVID-19 Pandemic and after it by the:**
  - ***Dramatic shift towards mobile cashless payments***, particularly through Digital Financial Channels/Services, providing more opportunities for fraudulent activities
  - This growth has been also accompanied by a ***substantial increase in Mobile Money Application Transactions***
- **Mobile Money users in Africa are particularly vulnerable to fraud due to lower digital literacy and service unique features**
  - *Service* Availability; Velocity of Funds; Distance Between Victims and Perpetrators; Ecosystem Complexity and Multi-Staged Fraud Scams

2. The Mobile Money Fraud Context (Introduction – Cont.)

GSMA **2024 Mobile Money Financial Impacts and Trends**



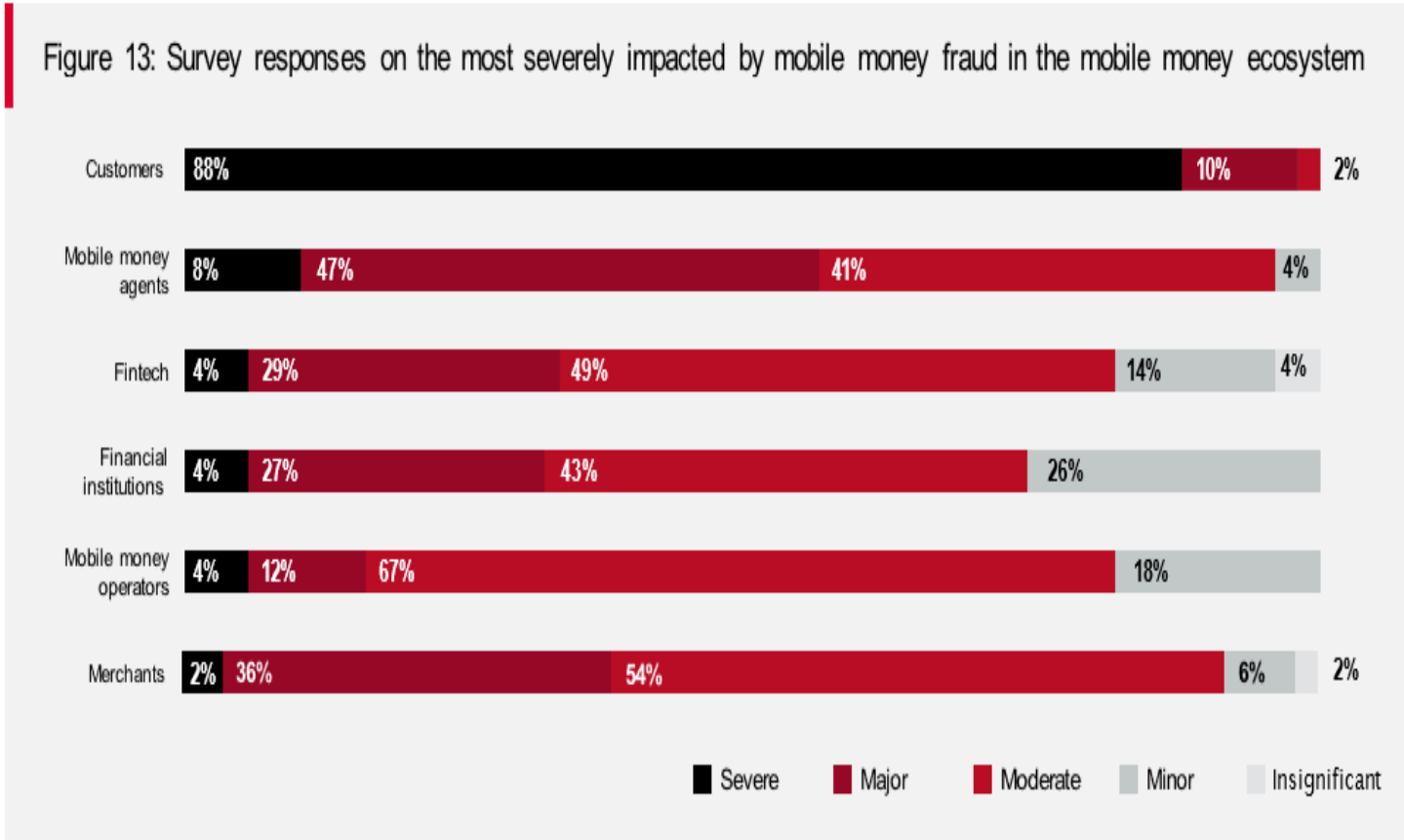
Mobile Money Financial Impacts and Trends

- The average annual loss due to Mobile Money Fraud (MMF) per provider is estimated at USD$1.06 million.
- This ***loss represents a small percentage (0.03%) of the average transaction volume per provider***, highlighting the massive scale of mobile money operations.
- ***63% of respondents perceive that MMF is increasing steadily***.
- ***22% indicate that it is increasing rapidly.***
- ***Only 14% see fraud as stabilized with no change***
- ***A mere 2% believe it is declining.***

GSMA

2. The Mobile Money Fraud Context (Introduction – Cont.)

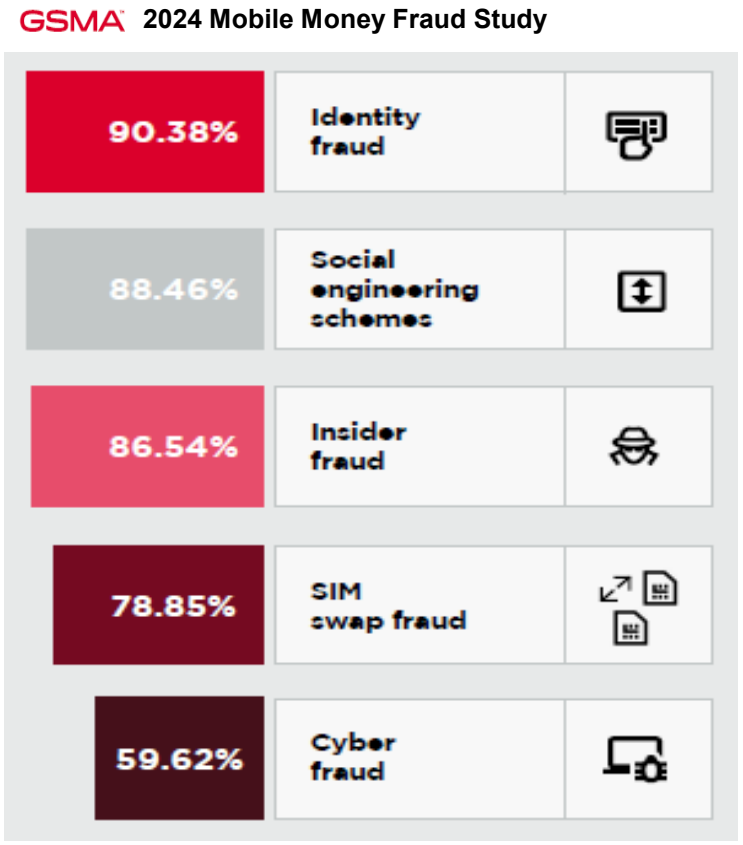
GSMA **2024 Players Most Impacted by Mobile Money Fraud**



The players most impacted by Mobile Money Fraud, are ranked as follows:

1. ***Customers,*** experience the most severe impact, with a significant majority (88%) reporting "Severe Effects" and (10%) "Major Disruptions".
2. ***Agents,*** also face substantial impacts, with (8%) of "Severe Effects" and (47%) of "Major Disruptions" (total of highest impacts at 55%).
3. ***Merchants,*** report a "Major Impact" (36%) and a "Moderate Impact" (54%), but a total of highest impacts at 38%.
4. **Fintech,** companies face mostly Moderate (49%) to Major (29%) impacts, but a total of highest impacts at 33%.
5. ***Financial Institutions,*** similar to Fintech's face mostly Moderate (43%) to Major (27%) impacts, but a total of highest impacts at 31%.
6. ***Mobile Operators,*** although equipped with robust systems and processes to handle fraud, report a predominant "Moderate Impact" (67%). Total of highest impacts at 16%

3. Main Trends in Mobile Money Fraud

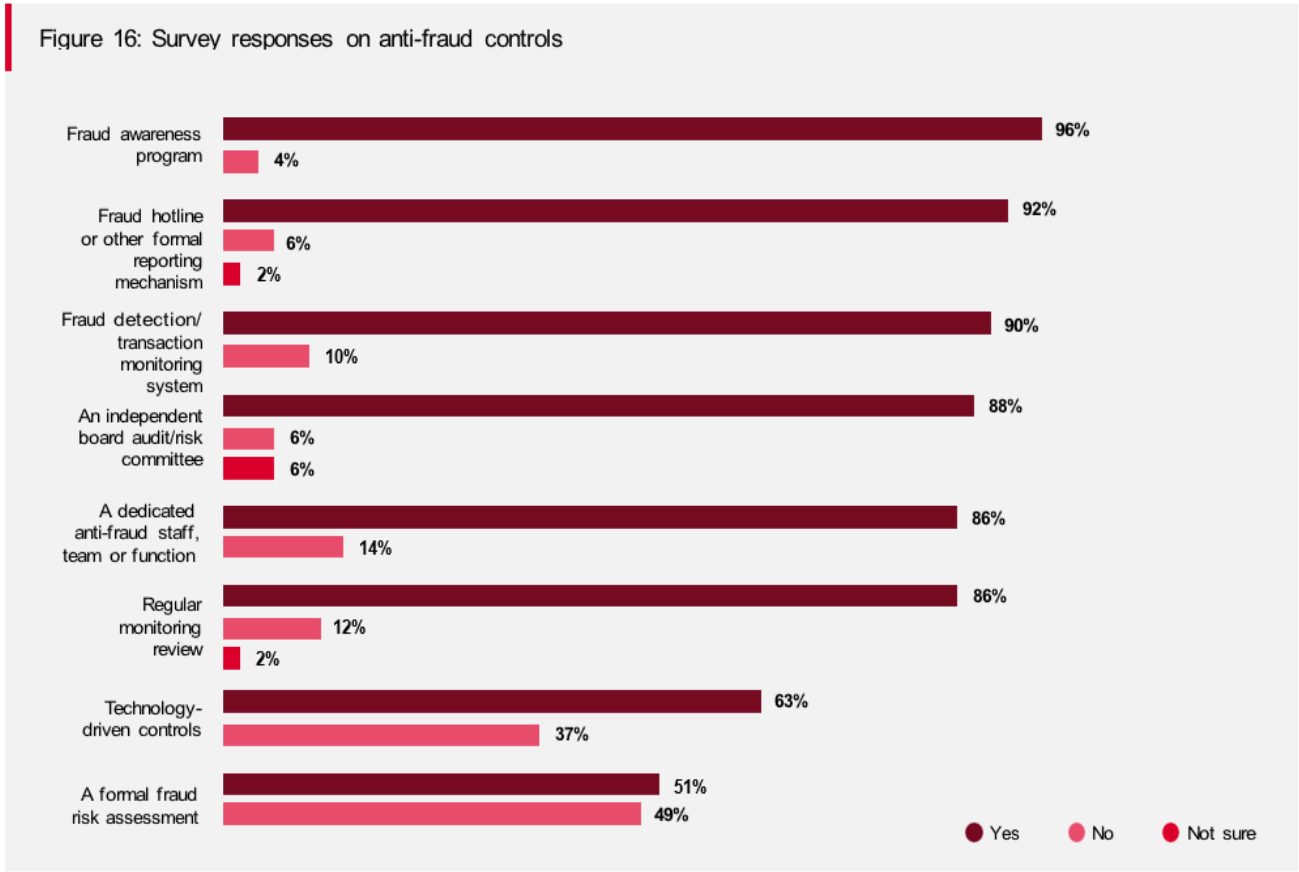


Mobile Money Most Prevalent Fraud Scams

- ***Identity Fraud (90%)*** - This type of "Impersonation Fraud" is seen as the most prevalent, where fraudsters use stolen or fake identities to commit fraud.
- ***Social Engineering Scams (88%)*** - These schemes involve manipulating or tricking people into divulging confidential or personal information that may be used for fraudulent purposes.
- ***Insider Fraud (86%)*** - This fraud is committed by individuals within the organization who have access to sensitive information and systems. It involves collusion between insiders (employees) and external parties (fraudsters), making it harder to detect and prevent.
- ***SIM Swap Fraud (79%)*** - Another type of "Impersonation Fraud", where the fraudster obtains a duplicate SIM Card from the victim's phone number to hijack personal and financial information. Highly prevalent in countries like Kenya and Mozambique at M-Pesa Service. https://restofworld.org/2023/mpesa-sim-swap-fraud/
- ***Cyber Fraud (60%)*** – Cyber-Attacks against the Mobile Money Service, the Platform and the Customers (Hacking, Phishing, Smishing, DDoS, etc), with the purpose to carry out fraud.
- ***Commissions Fraud (56%)*** - Typically involves Agents manipulating transactions (Arbitrage), breaching KYC or creating fake accounts to earn illegitimate commissions or incentives.

4. Mitigation Mobile Money Fraud

2024 The Extent of General Anti-Fraud Controls Implemented



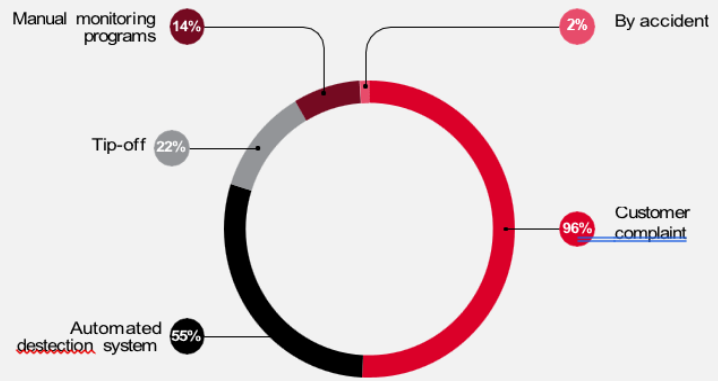
The General Anti-Fraud Controls implemented are:

1. **Fraud Awareness Program**
   - 96% have a “Fraud Awareness Program” in place
2. **Fraud Hotline or Other Formal Reporting Mechanism**
   - 92% have a “Red Hotline” to report fraud suspicious or incidents
3. **Fraud Detection/Transaction Monitoring System**
   - 90% use Transaction Monitoring Systems
4. **Independent Board Audit/Risk Committee**
   - 88% have an independent committee for Audit and Risk oversight
5. **Dedicated Anti-Fraud Staff, Team, or Function**
   - 86% have dedicated teams for anti-fraud activities
6. **Regular Monitoring Review**
   - 86% conduct regular monitoring reviews to ensure process improvements
7. **Technology-Driven Controls**
   - 63% use technology-driven controls, to enhance fraud detection/prevention
8. **Formal Fraud Risk Assessment**
   - 51% have a formal Fraud Risk Assessment in place and 49% do not have

4. Mitigation Mobile Money Fraud (Cont.)

GSMA 2024 Channels to Detect Fraud

Figure 17: Survey responses on fraud detection in organisations



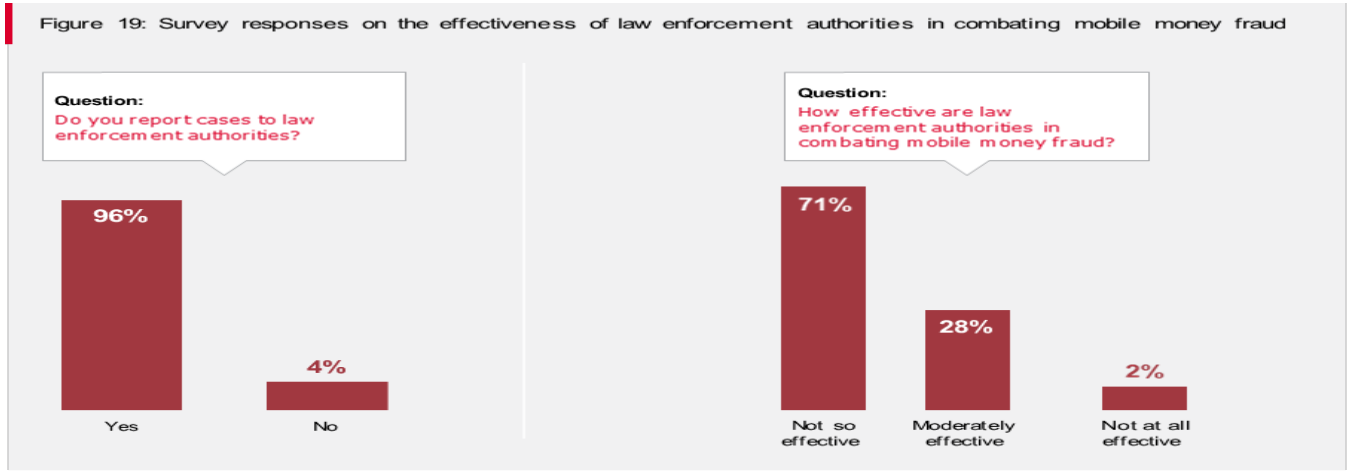
Effectiveness of Anti-Fraud Controls Implemented

The Role of General Detection Channels implemented

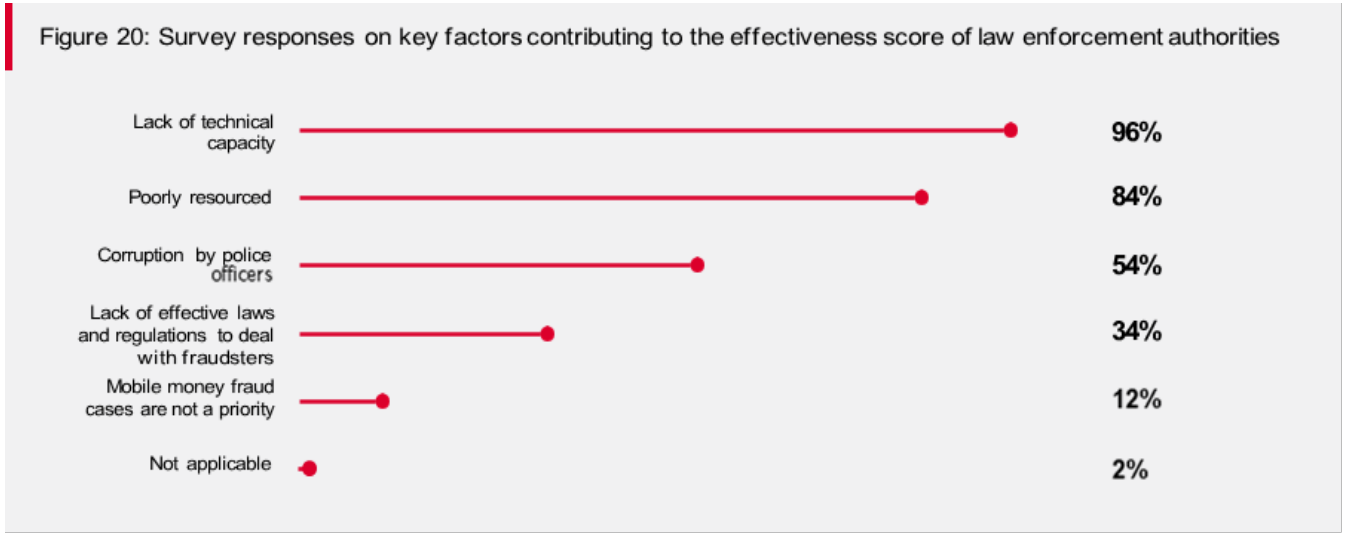
1. **Customer Complaints (96%)**
   - Nearly all fraud detection comes through customer complaints
2. **Automated Detection Systems (55%)**
   - Over half of the fraud is also detected through automated systems
3. **Tip-Offs (22%)**
   - Tips from internal/external sources represent a significant portion of fraud detected
4. **Manual Monitoring Programs (14%)**
   - Manual checks and reviews still play a role, though smaller, in detecting fraud
5. **Detection by Accident (2%)**
   - Small fraction of fraud is detected accidentally (routine checks or unrelated investigations)

5. Collaboration with Law Enforcement Authorities

GSMA **2024 Effectiveness of Law Enforcement**



GSMA **2024 Reasons Behind Effectiveness of Law Enforcement**



About the Reporting and Effectiveness Rate of Law Enforcement Agencies

1. **Reporting to Law Enforcement**
   - A vast majority (96%) report cases of Mobile Money Fraud to Law Enforcement Authorities.
2. **Effectiveness of Law Enforcement**
   - A significant majority (71%) perceive Law Enforcement as "not so effective" in combating Mobile Money Fraud.
   - Another 28% view Law Enforcement's efforts as "moderately effective," indicating some level of success.
   - Only a small fraction (2%) consider Law Enforcement to be "not at all effective,"

Reason Behind Effectiveness of Law Enforcement Agencies

1. **Lack of Technical Capacity (96%)**
2. **Poorly Resourced (84%)**
3. **Corruption Within the Police Force (54%)**
4. **Inadequate Legal Frameworks (34%)**
5. **Mobile Money Fraud Not a Priority (12%)**

GSMA

6. Future Outlook on Mobile Money Fraud (Key Take Aways)

1. A total of **85% of respondents believe that fraud trends are expected to increase**, due to evolving technology and new business models.
2. As technology advances, we can **expect increasingly sophisticated scams involving Artificial Intelligence and Deep Fakes**. As a response the Mobile Money Industry is likely to see:
    - A significant **growth in the adoption of AI and Blockchain technologies, to prevent/detect fraud** and to secure transactions
    - The **adoption of Biometric Verification** (Fingerprint, Facial Recognition, and Voice Authentication) will become more common
3. As **Mobile Money Systems become more integrated with International Payment Systems**, the scope for **cross-border fraud** will increase.
4. As **more Financial Services are delivered - such as Overdraft, Micro Loans and Saving products -** fraudsters will have **new opportunities to exploit** these additional vectors.
5. As fraud schemes become more sophisticated, **educating consumers about the risks and signs of fraud will become even more important.**
6. With **stricter Data Protection Regulations coming into force globally**, Mobile Money Providers will need to ensure **Compliance with Privacy Laws**.
7. There will be a **greater need for collaboration** among Mobile Money Operators, Financial Institutions, Technology Providers, and Regulators.

THANK YOU