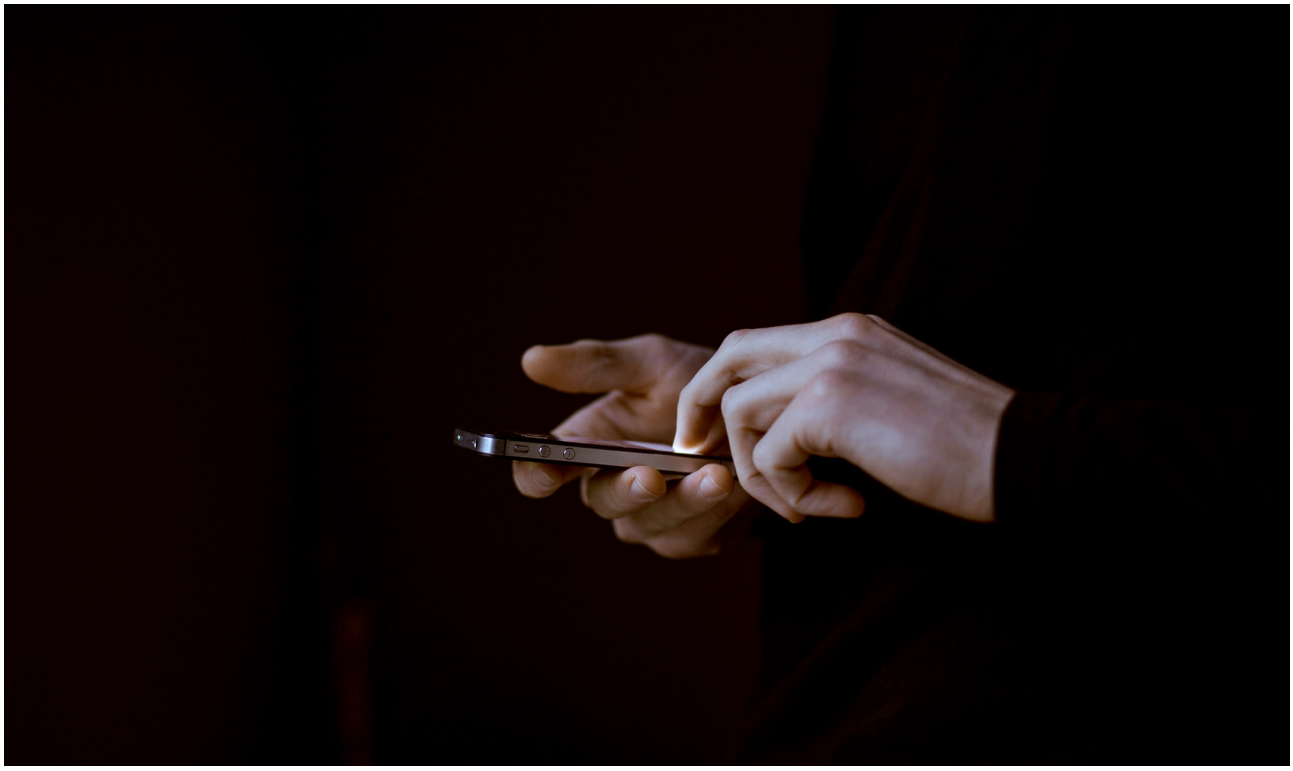


Mobile money and financial crime



Andrew Dornbierer
Asset Recovery Specialist

The amount of money flowing through mobile payment systems such as M-Pesa, MTN Mobile Money and Orange Money has exploded, in part due to covid-19 lockdowns. Should we be worried about the use of mobile money for financial crimes? While many think the amounts involved are too small to matter, others say the systems are open to abuse by organised crime or accuse them of enabling illegal currency trading.

Here are the basics of how mobile money systems could be abused for corruption and money laundering. Drawing on on-the-ground experience in Sub-Saharan Africa, we also outline how law enforcement officers can take advantage of this widespread payment method to catch corruption and money laundering schemes and prove them in court.

The what, how and why of mobile payments

For many individuals and businesses in countries with low banking penetration, particularly in Africa and Asia, mobile money systems have replaced both cash and bank accounts.

Instead of paying with cash at shops, market stalls and restaurants, customers can simply transfer payment from their mobile phone. This means no need to carry lots of cash around and worry about it being stolen. People can also lend and send money instantly by phone, which is useful for urban workers to send money back to their families in faraway villages.

As larger companies have come on board, many people now pay bills for energy, water and TV subscriptions via mobile. Companies have even started paying wages via the platforms. And the possibilities of mobile payment are expanding quickly. Most providers now offer additional services like cash withdrawals, transfers to bank accounts and international transfers.

Why is mobile payment so popular in Sub-Saharan Africa?

Sub-Saharan Africa is estimated to account for over 60 percent of the USD 690 billion in mobile money transactions carried out globally in 2019. This is partly because, in a region with a large informal economy and low penetration of formal banking, the barrier to opening a mobile money account is very low.

There are different models of mobile payment system, which are usually provided by either banks or telecoms companies. For basic telecoms-led systems, the user just needs a SIM card, a working mobile phone and an account with a provider. Sending money can be as simple as entering a phone number and the amount to transfer. The provider takes a small fee for each transaction.

This ease and speed make mobile payment systems perfect for micro-payments and small business owners. The industry is credited with enabling millions of people without a bank account to access financial markets for the first time.

Traceable cash and lifestyle snapshots

In countries where mobile payment systems are widely used, financial investigators potentially have a rich source of information at their fingertips. Records obtained from providers track all transactions related to a mobile number, such as sending, receiving, loading cash onto the account or withdrawing it. The mobile numbers are in turn linked to the individuals or businesses that registered the account – although these can of course be false names and shell companies.

Investigators can look at these records to get a good snapshot of a person's lifestyle. Where do they shop and eat out? How much do they spend and what kinds of shops do they spend it on? Are they paying for the most expensive cable TV package – perhaps for more than one property?

This information can provide indirect evidence of corruption by showing a discrepancy between a person's standard of living and their declared

income. It can also be used as direct evidence for cases of unexplained wealth, otherwise known as illicit enrichment.

Revealing new leads

As well as giving a picture of a suspect's lifestyle, mobile payment records can give investigators vital new leads and help uncover hidden assets. If a suspect is paying a cable TV bill, the investigator can obtain the address linked to that account from the cable provider. Perhaps they're paying more than one cable TV or electricity bill. How many properties do they own, even if not in their name?

These records can also help uncover networks of people potentially involved in petty corruption schemes by providing a picture of how individuals in these networks shared kickbacks amongst themselves or passed profits up the line.

Financial crime risks

Mobile money systems can be abused to launder money in a similar way to bank accounts. A person can easily and quickly set up multiple different accounts under their own or false names and transfer money between them to throw investigators off the track. They can also withdraw cash and upload it again to a different account. Platforms that allow users to convert mobile money into cryptocurrency and vice versa also exist, such as Kenya's BitPesa. Do these simple things multiple times and you get a very tangled money chain.

Another trick is to set up a business that accepts mobile payments and have fake customers paying money to this fake business. This mechanism is nothing new, but the use of mobile money makes it simpler and lowers the risk of getting caught.

Suspects involved in more serious crimes and corruption schemes often throw that chain across the border by transferring money internationally. Then, investigators have the same challenges of international cooperation to obtain information on those financial transactions as with any other cross-border investigation.

Slipping under the radar

Mobile money payment systems typically limit the amount of money that can be transferred in one transaction or day to a few hundred dollars. Many also limit the amount of money that an account can hold at any one time. This makes it unlikely that a mobile payment or account will trigger a suspicious transaction report to a financial intelligence unit, even if the mobile payment provider is included as a reporting entity in that country's legislation.

For criminals, it is easy to bypass know-your-customer (KYC) due diligence checks by purchasing multiple SIM cards using false or photocopied IDs, or by committing identity fraud. Access to black market SIM cards is certainly possible. For instance in 2019, Kenyan authorities seized 40,000 SIM cards

and several mobile phones in a raid on two apartments.

With multiple SIM cards and mobile payment accounts, it is then easy to transfer large amounts of money in lots of small individual payments. In a 2013 mobile money fraud case involving MTN Uganda, for example, around USD 850,000 was stolen in seven smaller transactions and transferred to 138 user accounts before being withdrawn in cash or tokens. Two years earlier in the case of Uganda vs Ssentongo, employees at the same company stole around USD 2.4 billion over six months by exploiting weaknesses in KYC processes and IT systems.

Transnational organised crime groups are known to use sophisticated networks of accounts to transfer the payments and proceeds of their crimes quickly across borders in multiple small transactions.

Fighting back through financial investigation

Despite the prevalence of mobile money platforms and their potential abuse for corruption and money laundering, many financial investigation agencies don't yet systematically include this in their investigation protocols. They should.

Mobile payment records can reveal a wealth of information about a suspect's lifestyle, income, assets and networks. Like any other piece of financial evidence, these records should be accepted without issue in courts.

Moreover, a more systematic, targeted focus on mobile payments – along with other relevant new payment products and services such as internet-based payment services and cryptocurrencies – will help strengthen a country's resilience to money laundering and terrorist financing. For more on this, see guidance from the Financial Action Task Force (FATF) including the 2013 Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services and the 2017 Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion.

The systematic exploration of mobile payment records is among the good practices that our experts at the International Centre for Asset Recovery are working to embed in standard financial investigation processes in our partner agencies, in countries where this is a relevant avenue for investigation.

Published on 28 July 2020

https://www.baselgovernance.org/blog/andrew-dornbierers-quick-guide-mobile-money-and-financial-crimes