Mitigating common fraud risks

Best practices for the mobile money industry

Mobile Money

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

The GSMA's Mobile Money programme works to accelerate the development of the mobile money ecosystem for the underserved.

For more information, please contact us:

Web: www.gsma.com/mobilemoney

Twitter: @GSMAMobileMoney

Email: mobilemoney@gsma.com

Published December 2019

Author
Saad Farooq, Senior Advocacy Manager, Mobile Money

THE MOBILE MONEY PROGRAMME IS SUPPORTED BY THE MILL & MELINDA GATES FOUNDATION, THE MASTERCARD FOUNDATION, AND OMIDYAR NETWORK

Contents

Executive summary

This paper is the second in a series of GSMA publications on the risks of fraud within mobile money.[1] Our first paper recommended a risk management framework to manage frauds mainly linked to transaction reversals, payroll processing, customer registrations, and split transactions.[2] As mobile money ecosystems evolve, new fraud risks have surfaced. This paper looks at fraud typologies that significantly impact mobile money users, such as identity theft, SIM swap and SMS fraud. This paper goes a step beyond the implementation of risk management controls that providers have typically employed, and recommends approaches to mitigate the risks of these frauds.

1 Other organisations have published papers on preventing frauds by improving internal controls and risk management initiatives. Different frameworks including STRIDE and DREAD have been recommended.
2 Gilman, L. and Joyce, M. (2012). Managing the risk of fraud in mobile money. GSMA.

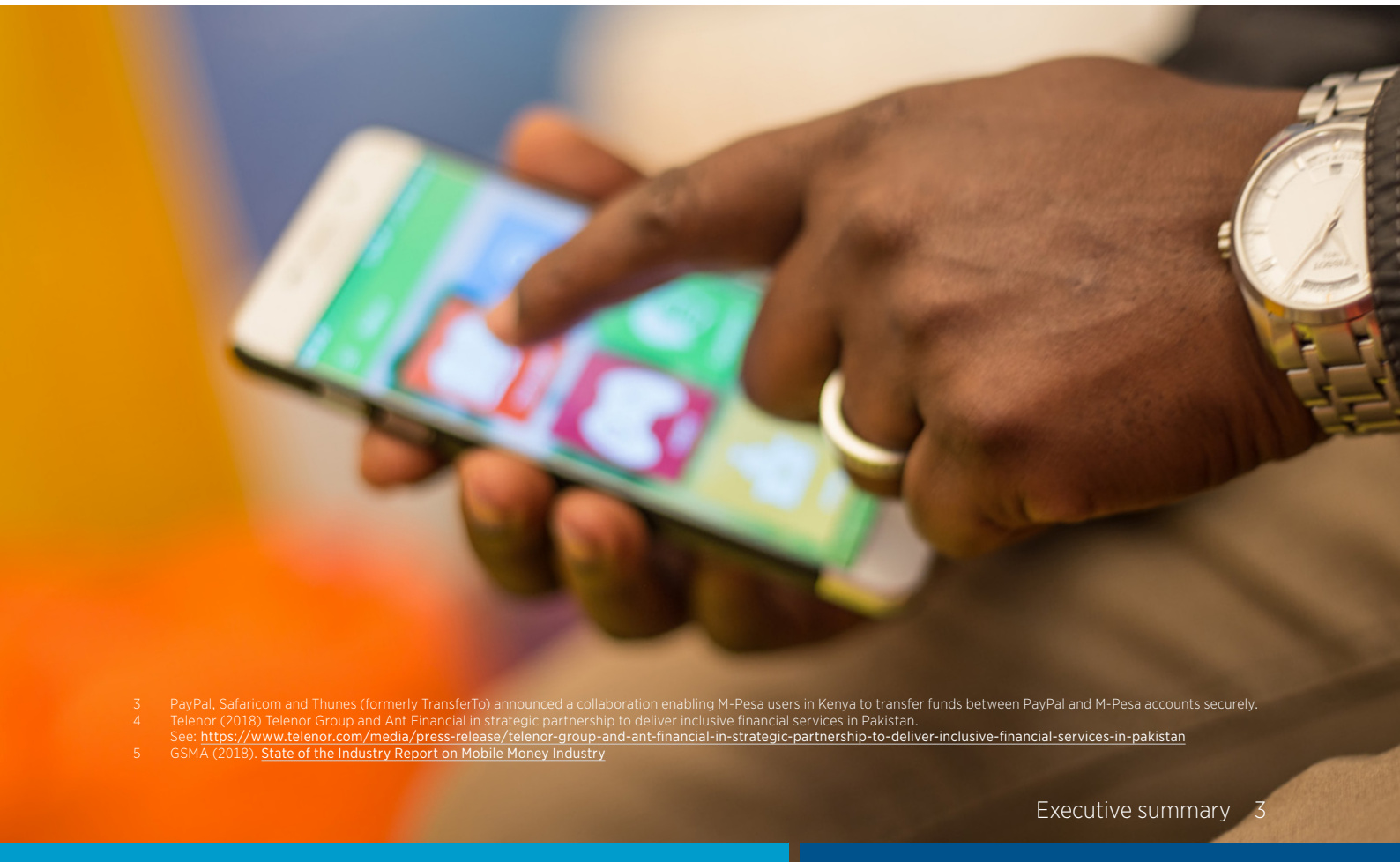
Introduction

For over a decade, mobile money has transformed access to financial services around the world. The mobile money ecosystem continues to expand, bringing in new partnerships and opportunities for providers, and new services for customers.

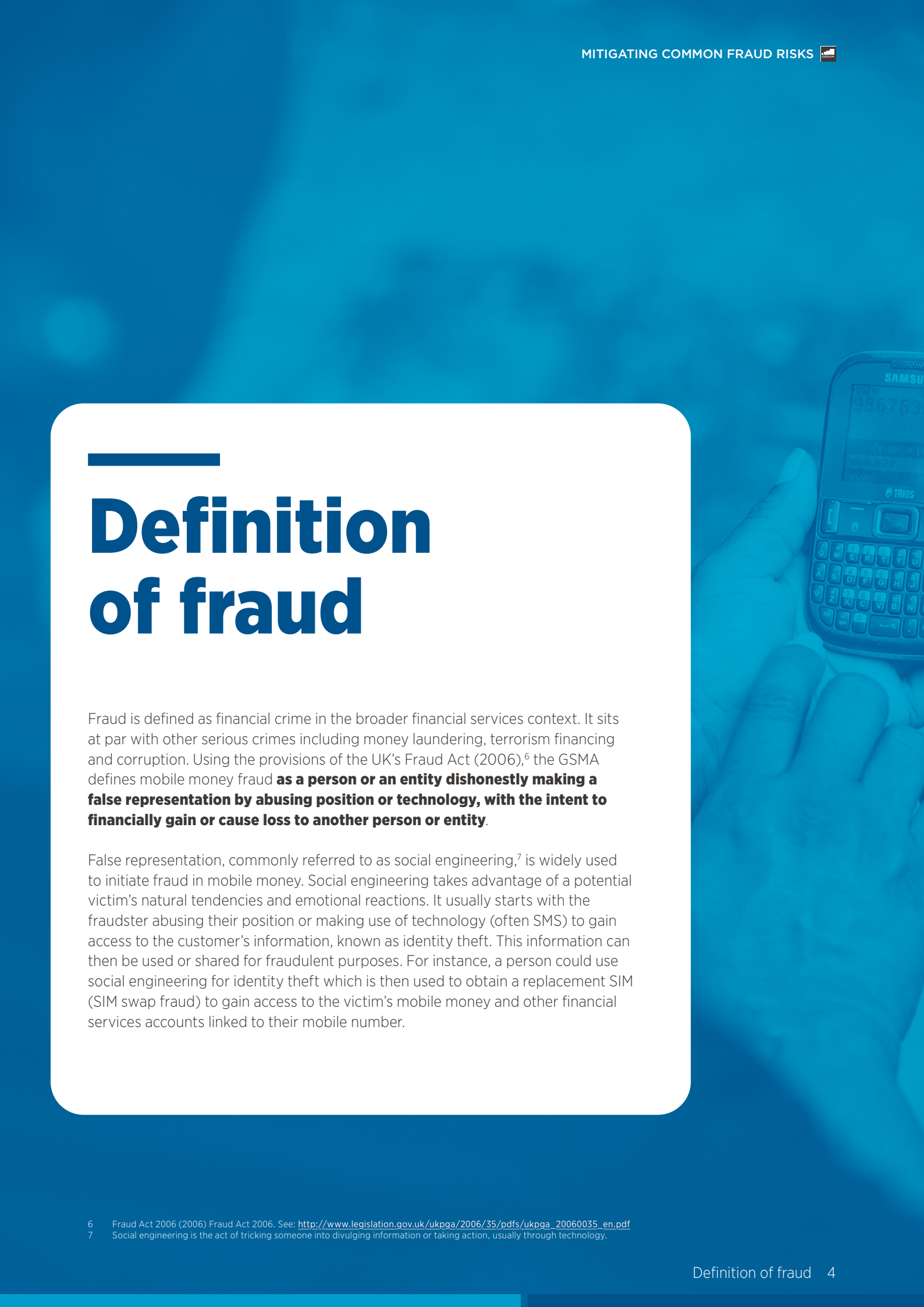
Operators are pursuing new investments and strategic partnerships to leverage data and innovative financial technologies, and to develop robust and interoperable payments systems to support a range of use cases and financial products. Examples include the PayPal and M-Pesa collaboration in Kenya[3] and Ant Financial's investment in Telenor Bank to deliver inclusive financial services in Pakistan.[4]

By providing new products and services to customers, these partnerships are catalysing the growth of the industry and increasing financial inclusion. Almost a billion people use mobile money to transact over $1.3 billion daily.[5]

While this growth over the last 10 years has created a significant economic and social impact on the lives of those living in poverty, the nature of financial fraud continues to evolve. Those with malign intentions have targeted mobile money providers and customers to steal personal information and money. As well as the financial loss and emotional stress caused to affected customers, providers also risk reputational damage. An understanding of the most common and impactful frauds within mobile money—and the best practices required to mitigate these—play a key role in continuing to provide safe and reliable services for the future.



3 PayPal, Safaricom and Thunes (formerly TransferTo) announced a collaboration enabling M-Pesa users in Kenya to transfer funds between PayPal and M-Pesa accounts securely.
4 Telenor (2018) Telenor Group and Ant Financial in strategic partnership to deliver inclusive financial services in Pakistan. See: https://www.telenor.com/media/press-release/telenor-group-and-ant-financial-in-strategic-partnership-to-deliver-inclusive-financial-services-in-pakistan
5 GSMA (2018). State of the Industry Report on Mobile Money Industry



Definition of fraud

Fraud is defined as financial crime in the broader financial services context. It sits at par with other serious crimes including money laundering, terrorism financing and corruption. Using the provisions of the UK's Fraud Act (2006),[6] the GSMA defines mobile money fraud **as a person or an entity dishonestly making a false representation by abusing position or technology, with the intent to financially gain or cause loss to another person or entity**.

False representation, commonly referred to as social engineering,[7] is widely used to initiate fraud in mobile money. Social engineering takes advantage of a potential victim's natural tendencies and emotional reactions. It usually starts with the fraudster abusing their position or making use of technology (often SMS) to gain access to the customer's information, known as identity theft. This information can then be used or shared for fraudulent purposes. For instance, a person could use social engineering for identity theft which is then used to obtain a replacement SIM (SIM swap fraud) to gain access to the victim's mobile money and other financial services accounts linked to their mobile number.

6 Fraud Act 2006 (2006) Fraud Act 2006. See: http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf
7 Social engineering is the act of tricking someone into divulging information or taking action, usually through technology.

Common frauds and recommendations

Different types of fraud are prevalent across the spectrum of mobile money services, yet some have a larger impact than others.

While mobile money providers should have mechanisms in place to mitigate the risks arising from all fraud, following a risk-based approach implies placing greater emphasis on those with the largest impact. As part of the research for this report, the GSMA worked with mobile operators, mobile money providers and regulators to understand the most common frauds across different countries and to provide recommendations to address these.

Identity theft

Identity theft occurs when personal information that can be used to identify someone is stolen. For instance, this can happen when technology is used to view or retrieve a person's identity details, through collusion with a rogue agent or an employee of a mobile money provider.

Identity theft can also happen as a result of data breaches, unsecure internet browsing on a mobile phone, malware activity, and smishing/SMS scams. In countries where feature phones are the dominant mobile device, smishing/SMS fraud is the most common method to steal identity information by directly targeting the end users.

Despite large scale investments in information security systems, identity theft remains a major problem worldwide. For example, a data security incident at the largest bank in the US exposed the names, addresses, telephone numbers and emails of almost two-thirds of US households in 2014.[8] In the UK, the number of reported identity theft cases over a 10 year period increased by 125 per cent to 175,000 in 2017.[9] More recently, a large mobile operator suffered a data breach that exposed the personal data of 11.5 million customers. Such incidents suggest that while investing in data privacy controls is important to manage the threats of data breaches and identity thefts, these alone are not enough.

Recommendations

Investments in state-of-the-art systems should be supplemented by best practices:

- Incorporating 'privacy by design' and implementing best practice[10] cybersecurity frameworks to strengthen systems will act as a barrier to identity theft;
- Increasing collaboration among industry players to share near real-time information on data breaches and related incidents (subject to data privacy laws) will limit the scale of losses as a result of identity thefts;
- Proactively educating customers on the latest techniques being used by fraudsters to steal identity information will alert customers to not reveal personal information; and
- Reporting data breaches (providers) and identity theft (customers) immediately to law enforcement agencies will limit exposure.

Identity theft is a common prerequisite to other serious unlawful activities such as fraudulent SIM swaps. To mitigate the risks of identity theft and associated frauds, it is important to look at these frauds in tandem, as one often leads to another.

8 Financial Times (2018). HSBC customers hit by data breach in US business. See: https://www.ft.com/content/ded1f64c-e1ea-11e8-a6e5-792428919cee
9 Independent (2018). ID theft levels soar as criminals set their sights on new targets. See: https://www.independent.co.uk/money/spend-save/id-theft-criminals-identity-fraud-increase-mobile-phones-credit-cards-a8311481.html
10 GSMA (2019). GSMA Mobile Money Certification Principles. See: https://www.gsma.com/mobilefordevelopment/resources/gsma-mobile-money-certification-principles/. Maina, J. (2018). Guidelines on mobile money data protection. GSMA.

SMS scams

Smishing (also known as SMS phishing) is one of the most common methods used to steal personal information such as account numbers, PINs and other identification details from a customer. Smishing scams compromise the target's mobile phone through SMS messages, stealing their personal data once the user clicks on the text link in the message.

Smishing frauds are also committed through bulk SMS campaigns, often via international SMS gateways where large groups of mobile customers are targeted with text messages that seem to originate from legitimate companies, including the mobile operator. The information is used for various illegal purposes, including:

- Asking the customer to transfer funds from their mobile money account to a fraudster with a fake promise (such as a reward);
- Gaining access to mobile money and other financial services accounts of customers via SIM swap to gain access to customer funds;
- Gaining access to the victim's social media and other accounts; and
- Selling the victim's personal information to others.

Smishing messages are designed to look genuine, and often copy the format used by the organisation, including using their branding and logo. Once the victim clicks on the link in the SMS, they are directed to a fake website that looks like the real one, but has a slightly different address. For example, if the legitimate site is 'www.mobilemoneyprovider.com.', the scammer may use an address like 'www.mobilemuneyprovider.com'. The victim is then tricked into revealing personal information or transfering money from a mobile money or a financial service account to the fraudster.

A common example of a smishing fraud is the Nigerian 419 Scam.[11] Victims are usually contacted by SMS with an incentive to trick them into revealing personal information or transfering money. For instance, the fraudster could pretend to be in urgent need of medical aid, asking the victim to transfer funds to their mobile money account for a life-saving treatment. In other cases, fraudsters can try to scam money from victims as fees and charges on the pretense of needing to transfer larger sums of money overseas. Fraudsters may also request the victim's bank account details to facilitate these transfers and subsequently use this information for fraudulent purposes. Depending on the scale of the fraud, it may be several weeks before the customer realises that they have been scammed, and the funds transferred from their mobile money account are lost.

In these situations, the customer may try to hold the mobile money provider liable for the loss of funds. However, the question of liability is not straightforward. Whether the provider is financially liable or not depends on several aspects, such as whether there was negligence on the part of the victim in transferring money or revealing their personal details. Nonetheless, this creates reputational liabilities for providers, which can lead to an erosion of user trust. Therefore, managing these frauds remains in the best interest of providers, regardless of liability.

Recommendations

The following recommendations will play an important part in mitigating risks of SMS fraud:

- Raising awareness and educating customers on protecting personal information (including name, date of birth, address and PIN, etc.) should become routine practice, e.g. using SMS reminders, warning notices at agent locations etc;
- Informing customers on what to do in situations where personal information is compromised, e.g. immediately calling the financial service provider or mobile operator (as appropriate) and reporting the matter to the police;
- Employees and agents should be trained, tested and routinely monitored to ensure that they don't unwittingly release customers' personal information. Policies and systems should be updated to reflect greater safeguarding of personal data, e.g. the four eyes principle;[12]
- Providers should jointly hold capacity building and training for law enforcement agencies to enable them to deal with such incidents promptly; and
- Investment in local SMS firewalls to enable providers to detect and address fraud committed through bulk SMS campaigns via international SMS gateways should be prioritised in high risk markets.

11 These scams are often known as 'Nigerian 419' scams because they started in Nigeria. The '419' part of the name comes from the section of Nigeria's Criminal Code which outlaws the practice. These scams now originate worldwide.

12 The four-eyes principle means that a certain activity, i.e. a decision, transaction, etc., must be approved by at least two people. This controlling mechanism is used to facilitate delegation of authority and increase transparency.

SIM swap

SIM swap is a legitimate service offered by mobile operators to customers to replace their existing SIM with a new one. A SIM swap may be required in the following circumstances:

- A SIM is lost, stolen or damaged;
- A different sized SIM is needed for a new device; and
- The customer is porting out their number onto a different network.

While SIM swap is a necessary and useful service, it has inspired some to obtain and utilise the replacement SIM card to gain access to users' financial services accounts. Two-factor authentication is commonly used by financial institutions to provide safe and secure services to customers. One of the most common two-factor authentication methods sends one-time passwords to the account holder's mobile number. If a SIM swap is obtained successfully, it enables the fraudster to receive authentication messages, calls and one-time passwords from the financial service provider of the victim. This allows those carrying out fraudulent activity to send money from the banking and mobile money accounts of the victim.

While SIM swap fraud is a global phenomena, it is most frequently observed in developing countries. Service providers are making capital investments to ensure their fraud controls are in line with the perceived threats in their markets, as well as investing in employee and agent training to reduce the risk of fraud. The impact of SIM swap fraud has the potential to become more significant as the industry evolves and the nature of partnerships becomes more complex.

Recommendations

To supplement existing efforts, the GSMA makes the following recommendations:

- In countries where SIM swap fraud threat is high, SIM swaps should be carried out at the mobile operator's sales centre after proper due diligence. Where this is not feasible, or in countries where the risk is low, SIM swap should be carried out only at accredited dealers. In this case, access to the mobile money account and other linked financial services accounts should be restricted for up to 48 hours;[13]
- In countries where both SIM and national identity registrations are mandatory, customers should be required to provide identification documents. These should be authenticated before a replacement SIM card is issued.[14] Where such authentication mechanisms are not available, a photograph of the customer should be captured to deter fraudsters;
- Mobile operators and financial service providers should jointly develop a mechanism for proactively sharing information related to SIM swaps without compromising customer data. This should include sharing internal mobile subscriber identity (IMSI) and International Mobile Equipment Identity (IMEI) data and static alerts each time a SIM replacement is carried out. The telecoms regulator should ensure the IMSI data is made available to relevant stakeholders in line with the data protection regulations and without cost; and
- Regulators should encourage creating and sharing a watchlist of identified perpetrateurs of fraud among mobile operators and financial service providers (while respecting data protection laws) to help others identify possible fraudulent activity. Those on the watchlist should also be reported to law enforcement agencies.

13 This will give the customer adequate time to contact the MNO if the SIM swap was fraudulent and also ensure that the customer's money in the linked financial services accounts remains safe for 48 hours.
14 Pakistan suffered high instances of SIM swap fraud until SIM registration and national ID authentication were mandated by the Government.

Why regulation alone is not enough

Regulators are increasingly focusing on fraud prevention.[15] While regulations require providers to design and implement effective anti-fraud controls, these often do not provide guidance on what a comprehensive fraud management programme should encompass. This is because the more prescriptive a fraud regulation is, the more likely it is to become quickly outdated.

Given the dynamic and fast evolving nature of fraud, it is largely left to the providers to determine what might constitute appropriate mitigation.In addition to the recommendations in this paper, financial service providers should also look to adhere to international best practices, guidelines and frameworks. The GSMA has recently published a cybersecurity governance framework for mobile money providers. This looks at the "people", "technology", and "process" aspects and gives recommendations to mitigate the risks arising from each element in an effort to strengthen internal controls.[16]

Another example of a comprehensive risk management framework is the GSMA Mobile Money Certification,[17] which defines and promotes excellence in the provision of mobile money services. The Certification represents a strong proactive move by the mobile money industry, demonstrating its commitment to Anti Money Laundering / Combating the Financing of Terrorism (AML/CFT) and to delivering safe and fair services to customers. The Certification comprises almost 300 criteria, which go beyond regulation in terms of detail and scope, establishing an aspirational bar of excellence that providers should aim to achieve to mitigate the risks of fraud in mobile money.

In parallel, it is important for providers across different sectors to strengthen their collaboration in the fight against fraud. In Zambia for instance, the local GSM Association has agreed with the Banker's Association to work together to manage fraud issues under the oversight of the telecom and financial sector regulators.

15 Examples include the Central Bank of Kenya, and the State Bank of Pakistan.
16 Maina, J. (2019) Cybersecurity: A governance framework for mobile money providers. GSMA.
17 GSMA (2019). GSMA Mobile Money Certification. See: http://www.gsma.com/mmc

Way forward

When mobile money users lose funds fraudulently, it can lead to an erosion of trust in digital financial services and can prompt a move back to using cash, undoing the gains achieved in financial inclusion and undermining the attainment of global development goals.[18]

In addition, it creates liability and reputational losses for both mobile operators and financial service providers. While financial service providers can compensate customers for the loss of their money, the reputational losses suffered by providers are the hardest to recover due to the long-lasting negative perception that is created.

Managing fraud should remain an important objective going forward as the continued adoption of mobile money depends on customer's perception of how safe their money is in the mobile money account. Mobile money providers should continue to make investments in technology, resources and training to respond to fraud threats, and regularly review whether existing controls are effectively aligned with emerging fraud threats. Implementing the recommendations and frameworks referenced in this paper will bring the industry a step closer to providing safe and secure services.

18 Lopez, M. (2019) Harnessing the power of mobile money to achieve the Sustainable Development Goals. GSMA.

Appendix

Glossary

Mobile number portability

Mobile number portability is a regulated facility which allows customers to keep their numbers when changing mobile network operator.[19]

Smishing

"Smishing refers to phishing attacks that involve the use of messages sent using SMS (Short Message Service). False text messages are received by would-be victims, who in turn either reply directly or visit a phishing web site."[20]

Social engineering

"Social engineering is a form of techniques employed by cybercriminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites."[21]

19 OFCOM (2018). Number Portability. See: https://www.trendmicro.com/vinfo/us/security/definition/smishing
20 Trend Micro (2019). Smishing. See: https://www.trendmicro.com/vinfo/us/security/definition/smishing
21 Kaspersky (2019). Social Engineering – Definition. See: https://www.kaspersky.co.uk/resource-center/definitions/what-is-social-engineering

gsma.com/mobilemoney

For more information on GSMA Mobile Money, visit gsma.com/mobilemoney

GSMA Head Office
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601