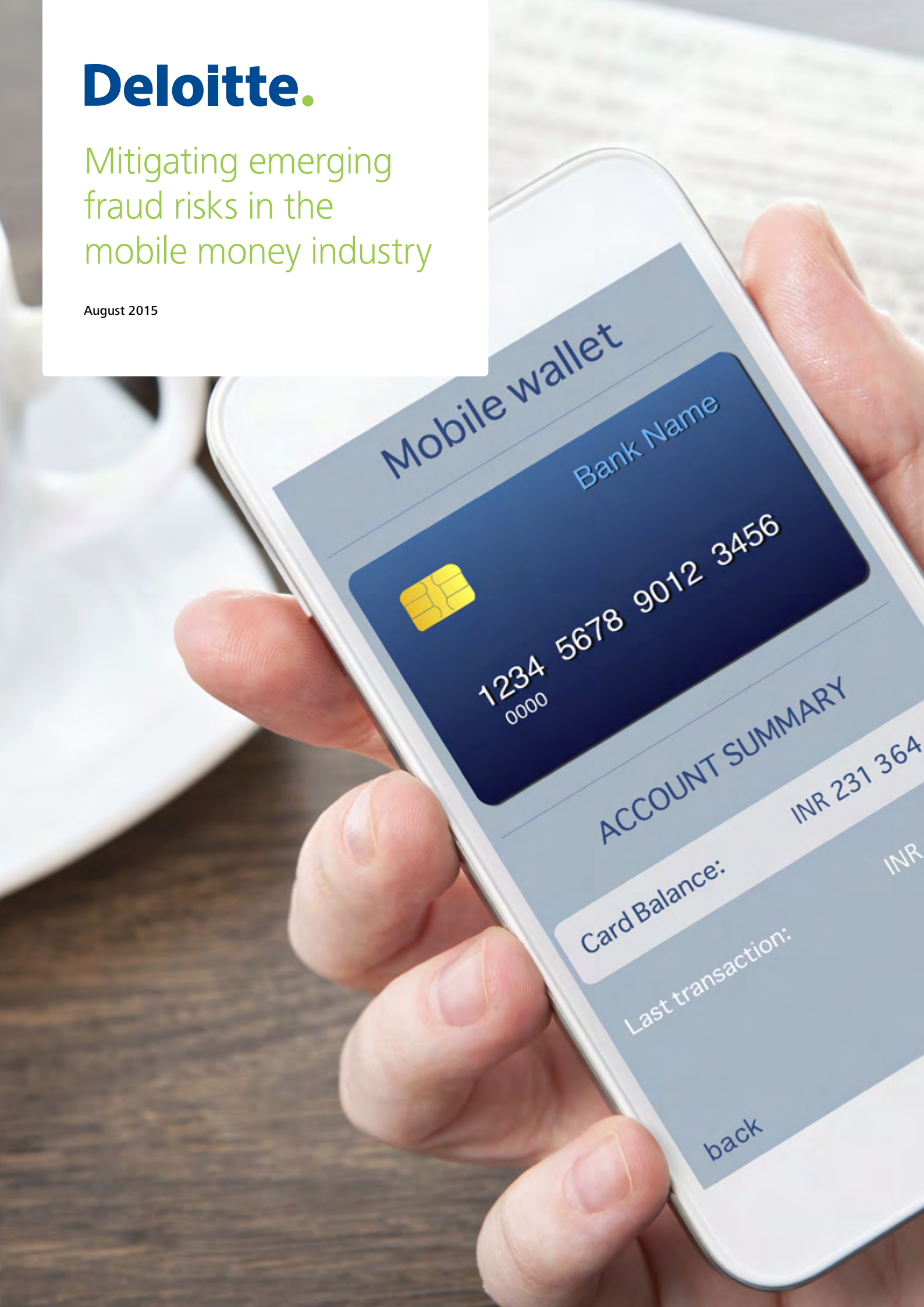
Deloitte.

Mitigating emerging fraud risks in the mobile money industry

August 2015



A Point of View

Introduction

The growth of the mobile subscriber base in India, currently over 980 million subscriber[1], has enabled the provision of communication, entertainment and information based services via mobile applications to subscribers. Mobile applications are increasingly paving the way for organizations in sectors such as public utilities and government organizations (m-governance), financial institutions (m-commerce), health care organizations (m-health), to deliver reliable services to a large audience without the need to physically visit a local office.

A report by ASSOCHAM and Deloitte released in 2015 indicated that mobile applications downloads in India have grown by 75 percent (CAGR) in the last three years, perhaps accompanied by the growth of smartphone penetration in India[2]. It is also observed that the fastest growing categories in mobile application development are social networking, e/m-commerce, gaming and entertainment.

E-commerce players for instance have realized the ability to better target customers on a mobile platform and leading ecommerce companies today derive a large proportion of their sales from mobile applications.

All leading banks in in India have their own mobile applications that customers can use to transact. Around 17million[3] Indians already use mobile banking. Considering that mobile penetration today covers around 73 percent[4] of India's population it is an incentive for banks to leverage mobile banking services as part of the financial inclusion agenda and reach out to around 41 percent[5] of India's households that remain unbanked, yet can access mobile applications.

While mobile wallet penetration in India is expected to rise to global levels, there is also a likelihood that the fraud risks witnessed in mature markets, may impact India in the near future. While the Reserve Bank of India ('RBI') has been updating the rules associated with flow of money in the virtual economy on a periodic basis, this alone may be inadequate to ward off fraud.

To tackle fraud in mobile transactions, it is important to understand the prevalent mobile transaction models and the inherent fraud risks that these models may be susceptible to. Accordingly, organizations using mobile transactions will have to devise specific controls to manage the risk of fraud.

---

1 Source: http://telecom.economictimes.indiatimes.com/news/industry/indias-telecom-subscriber-base-reaches-98-73-crore-in-february/46882582

2 Current smartphone penetration in India stands at 13.4% up from 10% in 2014, according to a report by Smartphone APAC Market Forecast 2014 – 2018: http://www.dazeinfo.com/2014/06/22/smartphone-apac-market-forecast-2014-2018-india-china-australia-japan-growth/

3 http://www.businessstandard.com/article/ finance/1-72-cr-customersusing-mobile-bankingfacilities-112121400624_1. Html

4 Source:http://country.eiu.com/ArticleIndustry.aspx?articleid=782421662&Country=India&topic=Industry&subtopic=Telecommunications

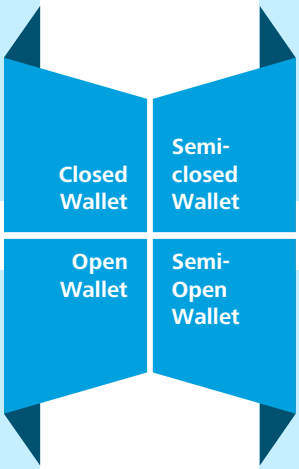
5 RBI, http://rbi.org.in/ scripts/BS_speechesvie

Understanding the mobile wallet eco system and transaction models

The RBI, that governs mobile payments in India, has allowed for the existence of four types of payment services[6] (called 'wallet'):

In a closed wallet model the flow of money is one-directional – one can only deposit money, but not withdraw it. Money present in a closed wallet can be used (like a prepaid card) for availing the services from a specific vendor/ service provider until one is left with no balance.

In a semi-closed wallet the flow of money is bidirectional. One can deposit money into the wallet as well as withdraw it, similar to a bank account. However, no cash based transactions (such as withdrawing or depositing cash) are permitted. In line with this facility, the RBI has clearly defined avenues for using semi-closed wallet models.



Open wallets are the most versatile among the prevalent wallet models in India. They can be used for purchase of goods and services and also permit cash withdrawal at ATMs.

Semi open wallets, while facilitating bidirectional flow of money, can also be used for purchase of goods and services at any credit/ debit card accepting merchant locations. This model does not permit cash withdrawal or redemption by the holder. A gift card issued by a bank is an example of semi-open wallet.

Given the regulatory requirements around end use and withdrawal guidelines, the Closed and Semi-Closed Wallet models have grown significantly in the last few years in India contributing up to INR 2700 crore in transaction value[7]. Globally, some countries also allow peer to peer money transfer and cash out activity via mobile payment models. However, this is presently restricted in India given the RBI's stringent view on Know Your Customer and Anti Money Laundering regulations.

[6] In line with the Payment and Settlement System Act 2007, later modified in 2014
[7] Source: http://www.financialexpress.com/article/personal-finance/e-wallets-money-on-the-move/28571/

Fraud risks around mobile wallets

Globally fraud loss in the telecom industry is in excess of 2 percent[8] of total revenues, which is close to USD 46 Billion. The industry estimates fraud losses due to mobile wallet fraud to also be around 2-3 percent of the revenues generated by mobile money services, although there is limited information available on this topic.

There are fraud risks that exist in every mobile money service around the world, however they can differ based on market dynamics. It is therefore prudent to determine key fraud risks across touch points in the mobile payment ecosystem that may impact the Indian market. The below table highlights the key globally observed fraud risks, that are likely to impact India in the future as the domestic market grows.

Frauds by customers/ external entities

Frauds	Common root causes
Phishing Fraud Fraudsters dupe customers through phone calls/SMS/ emails to share sensitive information such as PINs/Passwords that may result in embezzlement of virtual money from the wallet. The customer may also transfer virtual money himself under false promises or schemes. This may also happen with agents/retailer who own trust accounts and perform cash in/cash out transactions.	• Inadequate customer awareness around information sharing • Customer data theft, that are used by fraudsters to gain customers/agents confidence
Intrusion/ Cyber Attack: Fraudsters hacks into the mobile money platform and manipulate wallets to gain benefit	• Inadequate IT Securities/ Cyber Securities • Understanding on architecture and gaps shared through insiders
Benefits through misconduct Regular customers discover product or application flaws that can provide benefits to them in a specific scenario and they repeatedly simulate the same scenarios to exploit these limitations. E.g. • Transaction failures for specific scenarios results in wallet/ account getting credited without corresponding debit from the other side • Referral bonus on already registered customers • Avail bonus on refill of wallet, without actually recharging /refilling • Avail discount on same merchant transaction	• Inadequate governance on software development lifecycle (SDLC) and inadequate user acceptance testing (UAT) covering all possible fraud scenarios. • Insider information on design flaw. The design flaw can be intentionally introduced or overlooked by the internal stake holders with intent to carry out fraud. • Limitation on consequence management when customers perpetrate fraud • Inadequate data analytics capability to detect such anomalies on real time/near real time basis
Access to Wallet through unauthorized SIM SWAP Fraudster may impersonate and furnish fake documents to effect a SIM swap. Since most of the wallets are linked to MSISDN, the fraudster gains access to wallet of the subscriber and can embezzle the funds. This could be a serious concern for OTT players as they do not have control on SIM swap since they do not own the network.	• Inadequate validation and control on SIM swap (Chances of this occurring in India are low, unless otherwise an insider colludes with the subscriber) • Limited alternate controls such as application password, IMEI registration, especially for select OTT based players.
Fake KYC Customers can furnish fake KYC documents to gain access to premium wallets that allows higher transaction value (transfer and cash out). This may help facilitate money laundering.	• Inadequate validation of KYC documents. While the RBI has prescribed strict KYC norms and monitoring, the effectiveness of complying with these norms may be limited.

[8] CFCA Global fraud loss survey 2012

Frauds by Internal stake holders – Agents, Employees and Third Party Vendors

Frauds	Common root causes
Commission frauds by agents Agents introduce fake accounts to gain higher registration commissions Agents perform split transactions to gain higher transaction commissions	• Weak process of account onboarding and transactions management • Inadequate data analytics to identify red flags around commissions
Application manipulation by authorized user Employees having admin / super-user access can perform unauthorized transactions like: • Pseudo virtual money generation on select wallets. • Virtual money value embezzlement from wallets • SIM /MSISDN Swap or recycle • Fraudulent reversals • AML threshold manipulation • Report manipulation • Logs manipulation • Ghost wallets	• Inadequate Segregation of Duties (SOD) or violation of SOD and user privileges. • Inadequate policies on password sharing and other information security • Inadequate service assurance governance and control • Limited preventive and detective controls through data analytics. E.g. reconciliations not carried out for both virtual and physical books of account.

As is evident from the above table, the key root causes, even for the external frauds, are a result of internal control failures around governance, IT and continuous monitoring.

Identifying the risk of fraud from the perspective of all the stakeholders involved can provide the mobile money service provider an end-to-end understanding of the risks that need to be managed.

Mitigating mobile wallet fraud risks

In our experience there is limited amount of information around frauds reported by Indian mobile payments companies. Consequently it is possible that wallet service providers are likely to have little firsthand information on red flags and fraud schemes to circumvent these imminent risks. Further, the mobile payments industry is largely at a nascent stage in India and organizations are more focused on building a user base than perhaps looking into fraud control measures.

It is observed that the mobile platform adoption rates in India are much faster than in other parts of the world. It is therefore likely that this surge in adoption rates may be accompanied by a spate of fraud risks. Organizations need to start building comprehensive measures to counter impending fraud risks.

In our experience, each stakeholder in the mobile wallet value chain tends to look at risks in isolation, limiting the preventive measures to their immediate area of operations. Some of the key mitigation measures are listed below:

Controls to mitigate fraud	Extent of Preparedness by multiple system operators (MSO[9])	Extent of preparedness by Over the top service provider (OTT[10])	Extent of preparedness by Bank
Customer and Agents awareness program	🟡	🔴	🟢
IT Securities – Encryptions and other security features	🟢	🟢	🟢
User Access controls	🟡	🟡	🟢
KYC Controls	🟡	🟡	🟢
Preventive business rules - AML Violation controls, High Value transaction monitoring	🟢	🟢	🟢
Reconciliation on Virtual Money vs Trust Account	🟡	🟡	🟡
Robust incidence response on consequence management mechanism	🟡	🔴	🟡

🔴 Low level of preparedness 🟡 Medium level of preparedness 🟢 High level of preparedness

[9] A Multi—System Operator is a cable operator who receives programming services from a broadcaster and transmits them for simultaneous reception either to multiple subscribers directly or through one or more local cable operators. Some of the well- known MSOs in India include Hathway, IMCL, Siti Cable Network, DEN Networks and media house TV18.
Source - http://www.thehindubusinessline.com/features/smartbuy/tech-news/reliance-jio-applies-for-panindia-cable-mso-licence/article6789255.ece

[10] Over the top service providers are those companies that provide services such as internet based calling, messaging and music streaming. Skype, Viber, WhatsApp and Google Talk are some of the well known over the top service providers.
Source - http://indianexpress.com/article/technology/social/trai-seeks-to-regulate-ott-players-like-skype-viber-whatsapp-and-google-talk/

A more robust fraud mitigation approach would involve deriving synergies from respective stakeholders (banks, telecom companies etc) and integrating them to build a robust, comprehensive fraud risk management framework. In our view, the success of such an integrated approach to fraud risk management in the mobile wallet industry rests on three pillars:

1. Strong Foundation - Coordinated SDLC Governance

Organizations need to take cognizance of all possible fraud scenarios while developing the products or application. For instance, while designing the function document and testing, the risks hypothesis and controls needs to be jointly formulated with common understanding between financial institutions, MSO/ OTT and the IT developers. Further, UAT needs be comprehensive to cover all exceptions and fraud scenarios and tested not only by business users from all entities, but also independent control functions. The roles and responsibilities between organizations and departments needs to be clearly defined, including accountability in case of any fraud incidence.

2. Leveraging data analytics to build a Fraud Indicator Dashboard for robust monitoring

Building upon the learnings from Risk Analytics in the Banking sector and Fraud Management Systems in the Telecom sector, mobile wallet companies can develop a Fraud Indicator Dashboard to help in early detection of red flags. We have observed that such a dashboard can help in the following key areas:

- Provide real time fraud alarms on customer transactions (nature, value, frequency, threshold violations, destination party etc.), and internal violations (intrusions, access violation, configuration change etc.)
- Enable customer profiling through basis and statistical analysis– repeat failure attempts, historic background on default (from telecom or bank), KYC violations, high value transactions, transaction recipients (e.g. black listed merchant), IMEI analysis etc.
- Internal Control Health Assessment and Point of compromise– Pattern analysis on access violations (or attempt to Violations), security breaches/ intrusions, modification to logs, source code/configuration changes, report modification, patterns in reporting etc.
- Provide analysis to strengthen product gaps: Analysis and correlation on customers' usages and balance movements to identify outliers. E.g.
  – Analysis to identify bonus payout to customers against registration of same referral MSISDN.
  – Analysis to identify cash out post getting bonus for wallet refill
- Enable Social Media Crawling and analysis to identify any information around potential fraud/misconduct/ product gaps from public domain.

3. Effective Consequence Management

- **Tone at the top: Disciplinary Actions**

Organizations need to set the right tone at the top and exercise strong disciplinary action against identified suspects. We have observed that in organizations where disciplinary actions have been taken (supported by evidence preservation and case management), the instances of frauds have drastically reduced.

- **Crisis Management**

Brand reputation can take a severe hit if frauds reported in the public domain (by customers, for instance) are ignored. Therefore it is important to have a sound process to manage customer grievances due fraud and transfer accountability to the party responsible for this.

Conclusion

Adoption of mobile commerce is dependent on customers' perceptions about how safe their virtual money is from fraud. Over time, the ability to successfully counter frauds can become a key business differentiator for mobile wallet companies. Fraud, therefore needs to be considered as a critical business risk rather than just a one-off financial loss.

Regular monitoring of controls and reviewing fraud risks can be crucial in maintaining an effective risk mitigation strategy for mobile money service providers, considering the evolving nature of deployments with more product offerings or a growing customer base. It is equally important to note that with deployment changes, the sophistication of frauds perpetrated also can change. Operators therefore need to ensure adequate resources to regularly review both the effectiveness of controls and potential new trends in fraudulent activity.

Acknowledgements

This document required significant research into various sources including public domain sources. Rahul Talwar and Vaibhav Goel, both Managers in the Forensic practice of Deloitte in India contributed to this. We are also thankful to the Risk and Brand teams at Deloitte India for supporting us in this endeavor.

Contacts

For more details on this topic, please contact the following people.

Rohit Mahajan
Senior Director and Head
Forensic - Financial Advisory,
Deloitte in India
Tel: +91 22 6185 5180
Email: **rmahajan@deloitte.com**

Jayant Saran
Senior Director
Forensic - Financial Advisory,
Deloitte in India
Tel: +91 124 679 3607
Email: **jsaran@deloitte.com**

Arjun Rajagopalan
Director and Telecom Sector Leader
Forensic - Financial Advisory,
Deloitte in India
Tel: +91 124 679 3674
Email: rarjun@deloitte.com