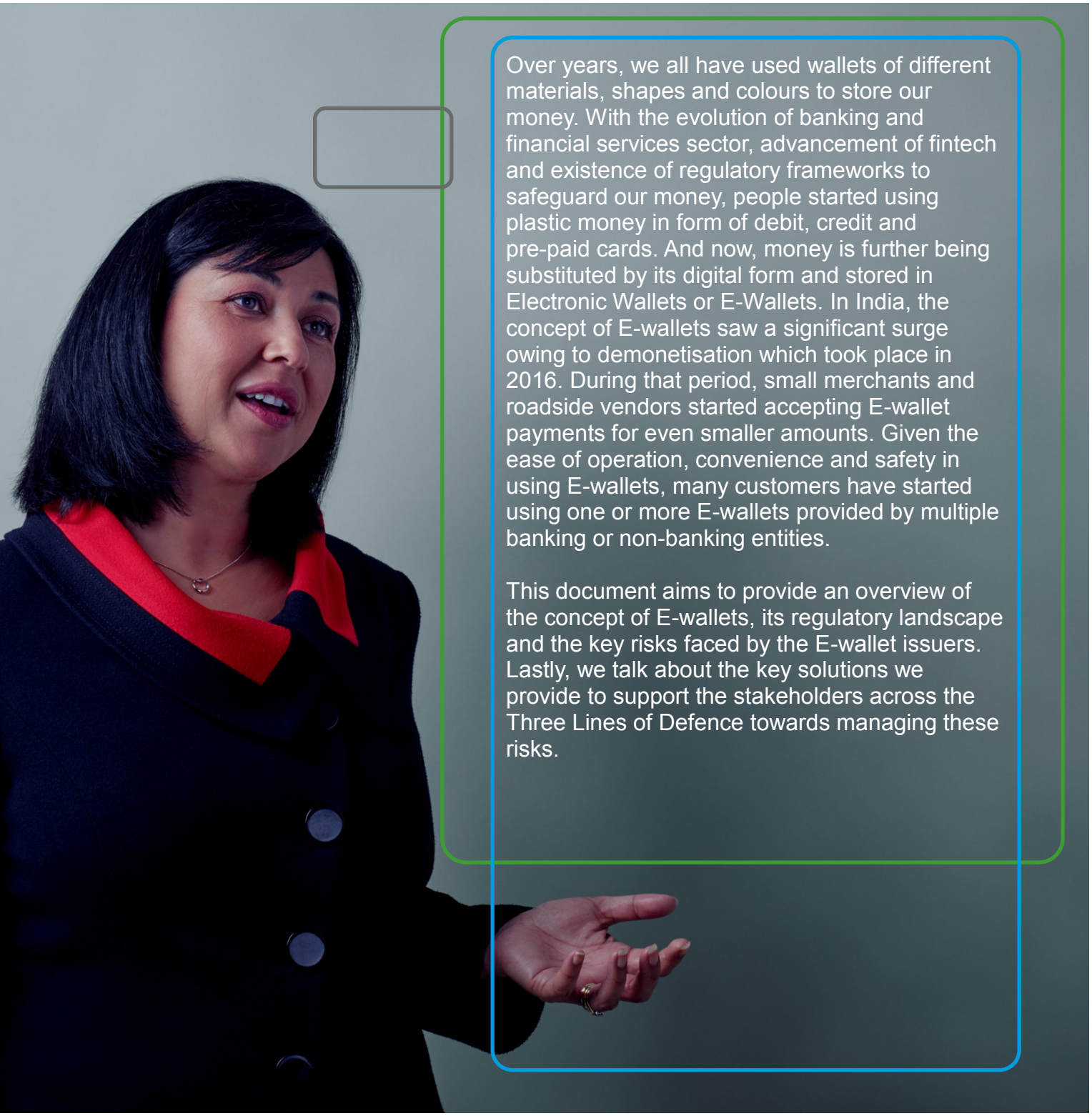
RSM India White Paper - Risk Management in E-Wallet Companies

THE POWER OF BEING UNDERSTOOD

RSM

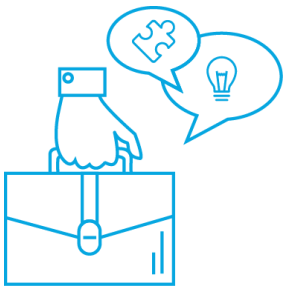
1.0 Introduction



Over years, we all have used wallets of different materials, shapes and colours to store our money. With the evolution of banking and financial services sector, advancement of fintech and existence of regulatory frameworks to safeguard our money, people started using plastic money in form of debit, credit and pre-paid cards. And now, money is further being substituted by its digital form and stored in Electronic Wallets or E-Wallets. In India, the concept of E-wallets saw a significant surge owing to demonetisation which took place in 2016. During that period, small merchants and roadside vendors started accepting E-wallet payments for even smaller amounts. Given the ease of operation, convenience and safety in using E-wallets, many customers have started using one or more E-wallets provided by multiple banking or non-banking entities.

This document aims to provide an overview of the concept of E-wallets, its regulatory landscape and the key risks faced by the E-wallet issuers. Lastly, we talk about the key solutions we provide to support the stakeholders across the Three Lines of Defence towards managing these risks.

2.0 What are E-wallets and how they operate?



■ What are E-Wallets?

- E-wallets or Digital Wallets are virtual wallets where the users store money
- The service is provided by a Pre-paid Payment Instrument (PPI) issuer
- Money stored can be used towards bill payments, funds transfer and availing services from merchants

■ Operating model

- User creates the E-wallet / account with the PPI Issuer
- Users add money in their E-wallets by using debit, credit card, net banking and even doorstep cash collection service in some cases
- Once topped-up, user can transfer funds / buy online and for in-store purchases, even scan the QR code to make payment

■ Some key players in India

- Banks
- Mobile phone operators
- E-commerce companies
- Cab aggregators
- Transport companies
- Other Non-banking companies

3.0 Regulatory Landscape

The Payment and Settlement Systems Act, 2007 (PSS Act, 2007) provides for the regulation and supervision of PPIs in India. Reserve Bank of India (RBI) is the regulatory authority for this purpose.
The below table provides the regulatory landscape of PPIs in India.

KEY REGULATIONS	Compliance with **RBI Circulars / Guidelines** on – KYC / AML / CFT – Cyber Security Framework – Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds - Implementation of Recommendations
CATEGORIES	• Three categories of payment instruments – 1. Closed system payment instrument, 2. Semi-closed system and 3. Open systems • Digital wallets or E-wallets fall under the Semi-closed system payment instrument category
PRE-REQUISITE	• All non-bank entities having a **minimum positive net worth of Rs. 5 crore** at all the times • By the end of **3rd financial** year from the date of receiving final authorisation, the entity shall achieve a minimum positive net-worth of **Rs. 15 crore** to be maintained at all times
RBI CIRCULAR	RBI's **"Master Direction on Issuance and Operation of Prepaid Payment Instruments"** lays down the directions to be followed by the PPI Issuers, System Providers and System Participants

4.0 Key risks faced by the PPIs

Businesses and risks are inseparable, all business processes have inherent risks, and by designing and implementing the mitigating controls, still have to live with residual risks.

The ease with which the E-wallet customers execute the transactions on their smart phones, tablets or computer screens is as a result of significant amount of risk management activities being carried out in the back end by their respective PPIs.

Some of the key risks being faced by the PPIs in running the E-wallet business are captured below.

Organisations conduct periodic audits to identify any gaps in the processes and improve the effectiveness of risk management, control and governance processes with the objective to add value and improve operations.

Nature of Risk	Some Indicative Risks	Audit Objective
Regulatory Risk	– Non-compliance to RBI's regulations / directions – FEMA non-compliances	To provide assurance on Compliance to Regulatory requirements
Fraud Risk	– Unauthorized transactions – Siphoning of funds – Cyber frauds – Accounting Frauds	To enable existence of necessary preventive and detective Fraud Controls
Third Party Risk	– Selection of inappropriate vendors – Non-compliances / control gaps in vendor managed processes – IT failures at Vendors	To ensure continuous monitoring over third party operations and strengthen controls
Revenue Leakages	– Unbilled / under billing of Fees, Commission, Delivery charges, etc. – Unreconciled balances with third parties	To arrest revenue leakage areas and ensure controls over billings and collections are appropriate
Information Technology Risk	– Platform / Application Design & Operations – Network & Infrastructure Security – Data Governance, Integrity and Security – Data Privacy	To provide assurance on adequacy of development process, customisations, security & availability of infrastructure
Strategic Risk	– Flawed Business Planning – Failure of tie-ups / alliances	To enable adequacy of design & business requirements alignment, future technology design, process design and control environment

Each of the above risks are further elaborated below, indicating what can go wrong under the respective risks. The indicative risks reflects the complexities and nuances involved, thereby requiring adequate preventive and detective controls to mitigate the risks.

Following are the illustrative risks / examples under each of the risk types

Regulatory Risk	– KYC non-compliances – CFT non-compliances – Non-compliance to interoperability requirements – Inappropriate Consumer Grievance Redressal – Erroneous regulatory Returns – AML non-compliances – FEMA non-compliances – Non-compliance to RBI Master Circular on Cyber Security Framework – Non-compliance to minimum Net-worth requirements – Other non-compliances to RBI Master Direction on PPIs
Fraud Risk	– Unauthorised transactions in customer accounts – Misappropriation of customer funds – Over / under reporting of customers / users – Accounting Fraud, Abuse / Misuse of sensitive personal information of customers – Use of bribery / corrupt practices to grow business – **Identity Theft** - fraudulent acquisition and use of sensitive personal information – **Friendly Fraud** – transaction denied, though goods or services were actually received – **Pharming** – re-directs website traffic to an illegal site where customers unknowingly enter their personal data. – **Phishing –** sending seemingly official communication from legitimate source to steal sensitive personal information
Third Party Risk	– Selection of inappropriate vendor / improper due diligence – Non-compliances to Regulatory and Statutory obligations by third parties – Dependency on single vendor for critical business processes – Inadequate IT Security measures – Potential Frauds – Improper / unfavorable legal contracts with third parties – Over / under payment to third parties – Inadequate ongoing monitoring of third parties – Absence of / inappropriate BCP / DR plans – Non-compliances to agreed policies, procedures and SLAs by third parties
Revenue Leakages	– Payments made to merchants, not recovered from customers – Unbilled fees / commission / delivery charges – Excessive cashbacks / discounts offered to customers – Unreconciled balances with third parties – Errors in exception pricing (fees and waivers) – Incomplete / unexecuted customer orders – Under-billing to customers – Untracked conditional offers – Unenforced price contracts – Delay in price changes

Information Technology Risk	– Non-compliances to regulatory requirements – Cyber security lapses, IT systems not aligned to business objectives – Software assets are not monitored appropriately – Unauthorized changes to the applications and systems – Absence of IT Policies and Procedures – Inadequate business continuity/disaster recovery plan – Unauthorized / excessive user access to the IT systems – Poor Data-center controls – Weak / unsecured network perimeter of the organisation
Strategic Risk	– Weak / unsecured network perimeter of the organization – Business processes not aligned to business goals and objectives – IT Platforms and systems not future ready – Lack of adequate market research and insights – Inappropriate business alliances – Failure to meet revenue and expense targets – Ineffective products – Inappropriate response to changing business dynamics – Inadequate resource allocation – Lack of innovation and disruptive ideas – Poor marketing and branding philosophies

5.0 Relevant Risk Management Solutions

Organisations, especially in the Banking and Financial Services Sector, deploy a three Lines of Defence (LoD) structure to mitigate the risks across the entity level and at individual process level, where:

1. First line of defence – are functions that own and manage risk
2. Second line of defence – are functions that oversee or specialise in risk management, compliance
3. Third line of defence – are functions that provide independent assurance, above all, i.e. internal audit.

We provide a set of relevant risk management solutions across the three LoD in this space

Business or the 1st LoD	Risk / Compliance or the 2nd LoD	Internal Audit or the 3rd LoD
Business Process Improvement	**Governance & Risk Management**	**Internal Audit**
– Develop and define **business processes, policies and SOPs** – **Revenue risk** management – **Cost** management solutions	– Developing / updating the **Risk Management Framework –** Credit, Market, Operations, Financial Reporting and Compliance – **Internal Financial Controls –** E2E support in scoping, process documentation, RCM, testing and reporting – **Security and Controls Compliance** for Outsourced Operations – **Third Party Risk** Management – **Fraud** Risk Management	– **Risk Assessment** and **Audit Scoping** – **Full scope** Internal Audits – **Data Analytics** – **IT** Audits / IT **General Controls** – Augmentation, Co-sourcing and out-sourcing **delivery models**
Segregation of Duties	**Compliance**	
– Defining the **SOD Framework / Matrix** – Review of **Role** definition in ERP – **User Access** rights review	– Create **Compliance Obligation Register covering RBI, FEMA** – Ongoing **Regulatory Compliance** reviews – **System Audits**, including **Cyber Security Audit**	
Reporting & Certifications		
– **Net-worth** Certifications – **Escrow Account** Certifications – Support in creating **regulatory reports** like – Customer grievance report, statistics, etc.		
IT Services		
– Design IT **Policies and Procedures** – Design and test of **Information Security / Data Privacy / Cyber Security framework** – **Data Analytics** and **Continuous Control monitoring** – Regulatory Compliance **(RBI Info-Sec, FIU, UIDAI, IT Act 2008)** – **ISO 27001** Readiness & Sustenance – **IT Infrastructure, Applications & processes** review – **PCI – DSS** Readiness – Designing and Testing of the **Business Continuity and Disaster Recovery Plan**		

For further information please contact:

RSM Astute Consulting Pvt. Ltd.

13th Floor, Bakhtawar, 229, Nariman Point, Mumbai - 400021.

T: (91-22) 6108 5555 / 6121 4444

E: emails@rsmindia.in

W: www.rsmindia.in

Offices: Mumbai, New Delhi - NCR, Chennai, Kolkata, Bengaluru, Surat, Hyderabad, Ahmedabad, Pune, Gandhidham and Jaipur.


facebook.com/RSMinIndia


twitter.com/RSM_India


linkedin.com/company/rsm-india

In this white paper, we have aimed to provide an overview of the concept of E-wallets, its regulatory landscape and the key risks faced by the E-wallet issuers. We have also discussed the key solutions we provide to support the stakeholders across the Three Lines of Defence towards managing these risks.

It may be noted that nothing contained in this white paper should be regarded as our opinion and facts of each case will need to be analyzed to ascertain applicability or otherwise of the laws and regulations in place. and appropriate professional advice should be sought for applicability of legal provisions based on specific facts. We are not responsible for any liability arising from any statements or errors contained in this white paper.

28 January 2019