Moving Beyond SMS based OTPs

Enhancing the security of digital transactions and enabling seamless customer communication

Table of Contents

EXECUTIVE SUMMARY

Over the last two decades, the payments landscape in India has evolved from 'Cash is King' to 'UPI Chalega'. This monumental change is a result of an amalgamation of growth in use of smartphones, internet use and financial services. India is one of the few shining examples of an economy which has leapfrogged from use of cash to a high adoption of digital payments. While this has had several positive impacts on the economy and society, consequently, however, the associated risk of frauds attached to digital payments has also risen.

It is pertinent to note that the banking and payments regulator – the Reserve Bank of India ('RBI') has prescribed several measures to safeguard the customer against frauds or thefts while undertaking a digital payments transaction. One of the key measures towards this is the implementation of Additional Factor Authentication (AFA) or 2 Factor Authentication (2FA), by whatever name called. Under this mechanism, at least 2FA is required from customer's end, to authenticate a transaction. Interestingly, what constitutes as standard 2FA has not been regulatorily prescribed thus far. Yet, banks and PSPs primarily resort to SMS based OTPs as one of the factors of authentication.

Furthermore, an alert regarding an executed transaction is also required to be sent to the customer from a regulatory standpoint. Here again, SMS is a commonly used mode of communication on account of regulatory mandate[1] in certain cases than the discretion of the banks and PSPs.

However, even though SMSes are widely used to authenticate transactions and communicate with the customer, they cannot be stated to be the safest channel with certainty. in fact, there have been rising instances of transaction frauds on account of SMS phishing/SMS cloning, etc.

Also, over the years, in line with the advancement in technology, there has been an emergence of newer channels and authentication factors, which provide enhanced security against such instances of fraud/thefts. Moreover, the added cost of sending SMSes is higher when compared to the cost of using newer channels for transaction execution and completion notifications.

As a result, the industry is seeking out credible alternatives to SMSes (like device binding, In-app notifications, App codes, OTPs through web-based messaging apps, etc.) in a digital transaction journey, as enumerated in the Paper below. This Paper delves deeper into the existing landscape, drawbacks and why the time now is ripe to evaluate indicative alternatives to SMSes for enabling AFA and communication with the customer.

[1] https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=2336 ; https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=11446&fn=9&Mode=0 https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=6309&Mode=0

DIGITAL PAYMENTS & TRANSACTION ALERTS – INDIA LANDSCAPE

> "100X increase in digital transaction in last 9 years."
> *- PIB*

Over the past decade, India has witnessed unprecedented growth in digital payments coupled with the Government's vision to expand digital transactions in the country has made the entire digital payments rail efficient, transparent, qualitative, and secure. As a result, India is sprinting towards a world-leading digital payments ecosystem. During the last nine years, the number of digital transactions in India has increased from a mere 127 crore in 2013-14 to 13,686 crore transactions in FY 2023-24 (as on February 08, 2024), which is over an 100 times increase.[2] This growth can be largely attributed to:

- Government policies and initiatives such as the Digital India programme, JAM[3] Trinity, etc., which have provided an impetus to financial inclusion in the country
- Supportive regulatory regime facilitated by the Financial Sector Regulators (FSRs)[4] and other ancillary regulatory bodies[5]
- Emergence of financial technology (FinTech) companies that have brought in new technologies to ease and enhance end user experience, and
- Increased FinTech-Bank/NBFC partnerships to digitize the entire economy till the last mile (including rural and semi-urban demographics).

Such top-drawer infrastructure built by payment service providers (PSPs) to support smooth transaction flows have resulted in the augment of easy and convenient modes of digital payments such as Bharat Interface for Money-Unified Payments Interface (BHIM-UPI), Immediate Payment Service (IMPS), Prepaid Payment Instruments (PPIs), National Electronic Funds Transfer (NEFT), Real-Time Gross Settlement (RTGS), Internet Banking, and more. Such modes of digital payments have not only registered substantial growth but also transformed the entire digital payment ecosystem.

> Digital payments in India continue to grew at a Y-o-Y transactional volume growth of 56% in FY 22–23 and is expected to grow 4X by FY 26–27.
> *- PwC Payments Handbook (2022-2027)*

[2] https://static.pib.gov.in/WriteReadData/specificdocs/documents/2023/may/doc2023521200801.pdf
[3] Jan Dhan-Aadhar-Mobile (JAM)
[4] Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Insurance Regulatory & Development Authority of India (IRDAI), Pension Fund Regulatory and Development Authority (PFRDA)
[5] Ministry of Electronics and Information Technology (MeitY), Unique Identification Authority of India (UIDAI), National Payments Corporation of India (NPCI), etc.

The ease of making digital payments, especially through UPI[6] has resulted in it emerging as one of the most preferred digital payment modes in the country. According to PwC Payments Handbook, over the next five years, UPI is expected to constitute almost 90% of total transactional volume in retail digital payments, as its adoption rises in rural areas and tier 3 and 4 cities.[7]

> UPI recorded 774.4 crore digital payment transactions with the value of INR 12.04 lakh crore in July 2023.
> ***- NPCI***

Digital transactions today are steered by innovation and speed. Therefore, customers as well as PSPs have adapted to the ever changing innovations in the digital payments landscape. However, certain critical processes such as authentication and intimation methods, which form part of a digital transaction lifecycle still follow traditional methods. Thus there is an immense scope for innovtion and change in these processes, which can certainly prove to be fruitful in making the digital finanical ecosystem more efficient.

The RBI's 'Payments Vision 2025' recognizes the emerging concerns around use of SMS based OTPs for authentication and intends to weave in alternative authentication mechanism(s) for digital payment transactions. Consequently, the RBI in its 'Statement on Development and Regulatory Policies'[8] dated February 09, 2024, has proposed to adopt a principle-based "Framework for authentication of digital payment transactions" to facilitate the use of alternative (to SMS based OTP) mechanisms for digital security.

Thus, this Paper seeks to provide an overview of the inherent disadvantage in use of SMS based OTP for authentication of digital transactions and transaction intimation to customers. Throughout the course of this Paper, we endeavor to touch upon nuances of how India's top-notch digital payments ecosystem compares to that in the other economies across the globe. And drawing from the current practices of India as well as case studies from across the globe, the Paper delves into recommendations for alternatives that can be considered to further make the existing digital transaction lifecycle efficient, speedy and seamless for both customers as well as PSPs.

[6] https://www.npci.org.in/statistics/monthly-metrics
[7] https://www.pwc.in/assets/pdfs/the-indian-payments-handbook-2022-2027.pdf
[8] https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=57276

TRANSACTION AND AUTHENTICATION FLOWS – CURRENT SCENARIO

It is pertinent to note that a perceptible increase in financial transactions through digital means is indicative of a customer's ease and trust in technology as a facilitator. Any digital transaction requires the Regulated Entities (REs) providing such transaction related services to:

- **Authenticate the customer:** At present, customers are authenticated using one-time passwords (OTP) received via SMS on the registered mobile number of the customer. This is known as 2FA (Two factor of authentication) or AFA (Additional Factor of Authentication).
- **Post-transaction alerts sent to the customer:** Upon transaction completion (whether successful or failed), issuers intimate the customer of the transaction success/ failure via SMS/ email/ both.

However, increased digitization across financial services such as payments, lending, investments, etc., has led to an unprecedented increase in financial and identity frauds, as well as enhanced cyber security threats. Hence, to mitigate the risks involved in digital transactions, such as frauds, chargebacks, failed transactions, etc., banks and PSPs like card issuers, merchants, and payment processors across the globe typically use a combination of AFA/2FA to authenticate the transactions made by the customer.

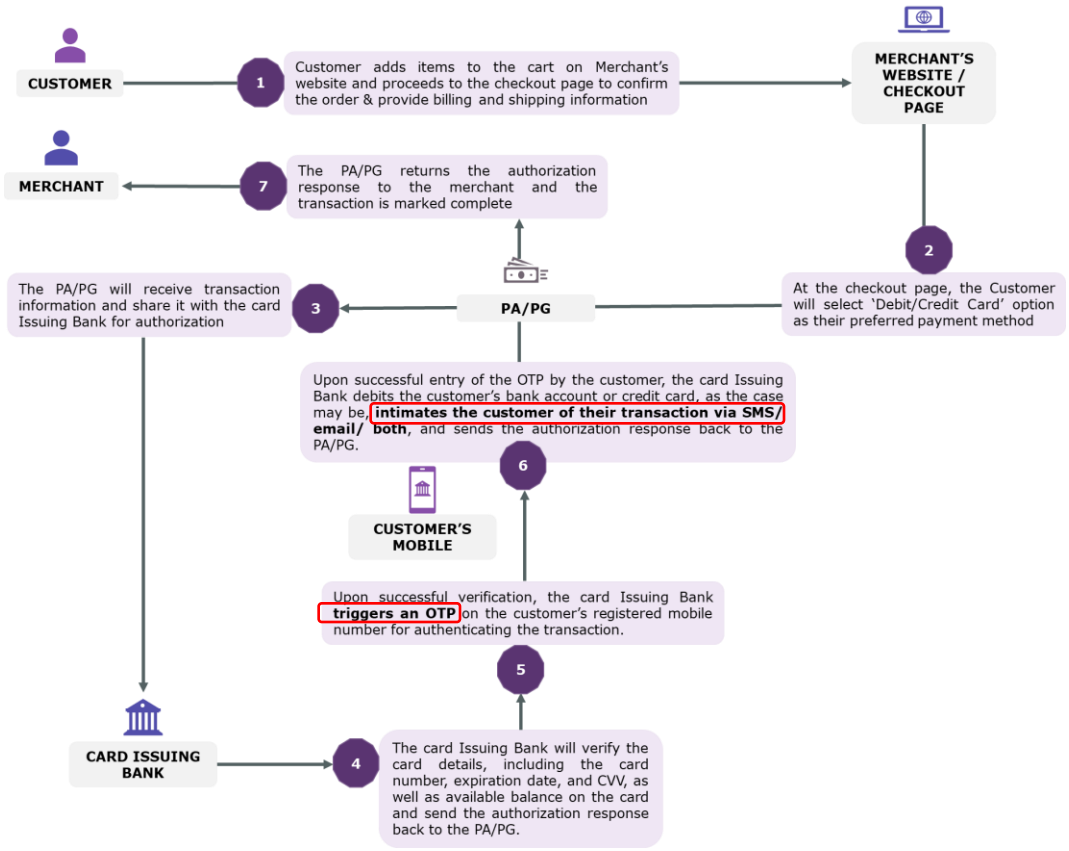
To this front, while security measures have matured, frauds and cyber security attacks have also become more sophisticated. As a result, SMS based OTP mechanisms have proved to have riskier and unsecure. For instance, new-age fraudsters have the capability to hack into customers' phone to read OTPs and commit finanical fraud. Therefore, relying solely on these traditional methods of authentication and transaction intimation may not be the most secure way of making digital transactions efficient and seamless.

Entities are continuously looking to adopt alternative mechanisms for authenticating customers and intimating them of a transaction. However, these methods are today used in addition to the existing ones, especially in India.

India Landscape

The RBI has repeatedly emphasized the importance of ensuring customer protection against potential frauds whilst adopting digital transactions in all its communication viz. circulars, regulations and guidelines. With the emergence of embedded finance, super apps, etc., an increasing number of companies are focused on making the customer's digital transaction journey simple, seamless, and speedy. The need for alternative means of authenticating and intimating the customers of their transactions is a critical component of any customer's digital payment journey.

For better understanding, by way of example, the depiction below explains a typical e-commerce digital transaction flow in India.



Things to note:

- *For the purposes of reference, we have used a typical example of a customer making a payment on a merchant website using the card payment method.*
- *Payment methods like internet banking, debit and credit card transactions, etc., require 2FA. However, it is pertinent to note that different banks and PSPs may use different mechanisms for authentication since the RBI has not prescribed a particular method to undertake 2FA.*
- *In case the customer opts for UPI payment, there is no OTP-based authentication involved. The customer simply goes on their UPI app and enters the PIN to complete the transaction. However, the customer and the merchant/receiver are intimated of the trasaction using SMS/email/both by the Issuing Bank and the Acquirer Bank respectively.*

In India, SMS based OTPs are typically used for authentication of payments, which is followed by transaction alert through SMSes and / or E-mail (mandatory for debit/credit card transactions and wherever possible for other payment instruments) to intimate the customer.

It is pertinent to note that one of the primary objectives of digital transactions is to provide an efficient, convenient payments experience to the customer and at the same time, to safeguard the customer from potential frauds/thefts during the digital payment process.

However, as we move towards a well-connected and tech-driven ecosystem, it is of the utmost importance reflect on the challenges and issues arising from the traditional methods of transaction intimation and authentication mechanisms.

In the next chapter, we look at the feasibility of the current communication trails in banking transactions and how India compares to the global practices.

TRANSACTION INTIMATION TO COMMUNICATE BANKING ALERTS – CURRENT METHODS AND THEIR FEASIBILITY

India has the highest FinTech adoption rate of 87% as compared to the global average of 64%.[9] The partnership between FinTechs and traditional financial institutions has enabled digitzation of the entire financial ecosystem, which has alleviated the entire banking ecosystem. Right from the manner in which banking business is undertaken to day-to-day operational functions such as payments, money transfer, handling of grievances, etc.

While different jurisdictions have different methods of communicating post-transaction alerts in a digital transaction lifecycle, traditionally, customers are intimated of their banking activities using SMS and email (wherever possible) on the registered mobile number and email ID respectively. Whether it is regarding completion of a transaction, failure of a transaction, account balance alerts, receiving OTPs, etc., SMSes have remained a preferred mode of communication and intimation on account..

However, the technological advancements and increased adoption of smartphones and internet penetration across regions have paved way for alternative means of intimating the customers of their transactions.

The intent behind considering alternative methods of authentication and transaction alert stems the issues plaguing the banking ecosystem in terms of SMS-based alerts. As most users have switched to app-based messaging, the bulk of SMS received are mostly promotional in nature. Hence, SMS as a mode of communication may have become less preferred and is marred with several challenges.

1.1.1 Security risk

Important messages containing information on financial transactions are often lost and difficult to locate in a barrage of unsolicited promotional and spam messages. Additionally, in cases where the customer has dual SIM but only has one number registered as his official mobile number, it poses as a challenge to differentiate between the promotional spam SMSes and time sensitive SMSes received for the purpose of undertaking a financial transaction.

Thus, the primary purpose of SMS alerts (intimating the customers) gets eroded. On previous occasions, Telecom Regulatory Authority of India (TRAI)[10] and RBI[11] have acknowledged the increasing threats arising from SMS based frauds. Additionally, in general, the increasing SMS

[9] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1759602
[10] https://www.trai.gov.in/sites/default/files/RegulationUcc19072018_0.pdf
[11] https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf

failure rate (22% as per industry standards) has been a growing reason to evaluate alternate modes of intimating the customer of their financial transactions/ updates.

It becomes difficult for customers to differentiate the authenticity of the sender thus putting the credibility of the communication at stake and elevating the prospect of frauds and failure rates. Additionally, with increased sophistication of financial frauds, ascertaining the genuineness of such fraud based SMSes is nearly impossible. Plus, telecom companies or their aggregators have no set mechanism to be able to authenticate the legitimacy of these messages. Technology enabled financial transactions thrive on customer trust, and any challenge to the credibility of communications may dissuade the customer from engaging in digital financial transactions.

Regulatory and policy recognition

TRAI, by way of guidelines[12], has endeavoured to prevent SMS-based frauds by imposing restrictions on **commercial SMSes**. However, in absence of these guidelines being applicable to personal SMSes, fraudsters continue to use SMS as means to cheat customers conducting their banking activities online. By way of disguising the SMSes to seem like they have been sent by the customer's bank/ RE (Issuer), fraudsters have maliciously misled many customers to experience financial losses.

In fact, in July this year, in a written reply to the Parliament, the Union Telecom Minister Ashwini Vaishnaw mentioned that a fine of INR 34.99 crore on service providers for failing to curb pesky calls and SMS on their network.[13] Consequently, in September 2023, TRAI levied penalties amounting to INR 3.8 crore[14] on services providers for their failure to curb the menace of unsolicited commercial communications (UCC). Recently, in February, the TRAI levied a staggering penalty of INR 110 crores[15] on service providers, for their failure to curb pesky calls.

Further, RBI's BE(A)WARE – A booklet on modus operandi of financial fraudsters, acknowledges the surge in financial frauds through various modes including SMS-based frauds, OTP-based frauds, cloning, SIM Swapping frauds, etc.[16] In an ongoing effort to curb menace of spams through UCC, on June 02, 2023, TRAI issued Direction regarding implementation of Digital Consent Acquisition (DCA) under TCCCPR, 2018. This program mandated the Indian cellular providers to obtain explicit consent from users before sending them promotional materials.[17]

[12] https://www.trai.gov.in/sites/default/files/RegulationUcc19072018_0.pdf
[13] https://economictimes.indiatimes.com/industry/telecom/telecom-news/trai-imposes-penalty-of-rs-35-crore-on-telcos-for-violating-pesky-call-sms-norms/articleshow/102019145.cms
[14] https://telecom.economictimes.indiatimes.com/news/industry/trai-levies-rs-2-81-crore-on-airtel-for-failure-to-curb-ucc/104031426
[15] https://timesofindia.indiatimes.com/city/delhi/trai-fines-telcos-110cr-for-failure-to-tackle-pesky-calls/articleshow/107442262.cms
[16] https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf
[17] https://www.trai.gov.in/sites/default/files/PR_No.50of2023.pdf

1.1.2 Cost as a challenge

In banking and payments, SMS is a mandatory mode of communication, the cost for which comes as a significant cost to be borne by RBI regulated entities. Separately, the onus and cost of sending post transaction alerts are borne by the RBI regulated entities and the card issuing bank as the case may be. In compliance with the guidelines in effect, an SMS alert is pushed out for all transactions irrespective of the value. The cost of SMS charges is significantly high and dampens the growth prospects of the Issuers. In fact, it is noted that, the cost for time sensitive SMSes such as OTP/ balance enquiry, etc., have a steeper cost attached to it than general promotional messages. For instance, general SMS costs approximately INR 0.12 per message.

While the cost of SMS is a pressing challenge, incurring this cost does not ensure delivery of the SMS either. On an average, on a daily basis, the failure of delivery rate stands at 22%.

Therefore, the industry can easily offset the failure of delivery rates as well as high SMS costs incurred by them, by resorting to alternative methods of communication other than SMS. This has been detailed in the ensuing paragraphs. Moreover, the issuers can divert these resources to engage in furthering the cause of consumer education enabling them to transact more confidently.

1.1.3 SIM-based frauds

With cell phones having become an essential component in this virtual world, transactions of any kind are now feasible on the fly. However, the widespread use of mobile technology has attracted cybercriminals, who are now more inclined to turn to innovative and complex methods of perpetrating fraud and other online crimes. Mobile SIM switching and SIM cloning are two examples of cyber frauds that scammers use to deceive mobile users. In these scams, the fraudsters take control of the victim's phone number and corrupt the device.

SIM Swapping

SIM swapping, often referred to as SIM splitting, SIM jacking, or SIM hijacking, is the process of switching from your current SIM card to one that is controlled by a cybercriminal. Here, the criminal registers a new SIM card with the user's current mobile details and through this deception, the cybercriminal obtains access to your private and sensitive financial information.

Controlling the user's mobile SIM or phone number provides the scammer/fraudster access to their OTPs, PINs, and authentication text messages (SMS), giving them access to sensitive and important financial and personal information that they can use to perpetrate fraud.

In one of the recent news articles, the police official described the sim swapping process by stating that the fraudsters usually have an associate working with the telecom company. So, they easily duplicate the SIM with the personal details they have procured after the malware or

phishing attack. Once they have the duplicate SIM, they can easily receive any banking authorization messages or OTPs.[18]

SIM Cloning

SIM cloning, on the other hand, is like switching SIM cards. It is the process of making a copy of the original SIM in which the actual SIM card is copied using a software. In order to identify and authenticate users on mobile phones, the victims' International Mobile Subscriber Identity (IMSI) and encryption key are obtained for the fraudster to take over and use the mobile number to track, monitor, make calls, listen to calls, and send texts by cloning the SIM card.

Through SIM cloning, a fraudster can run a victim's phone covertly by tracking their whereabouts, monitoring their phone, listening to their calls, accessing their financial and personal accounts, and more. It gives the scammer the ability to phone or text from the victim's number while posing as the user.

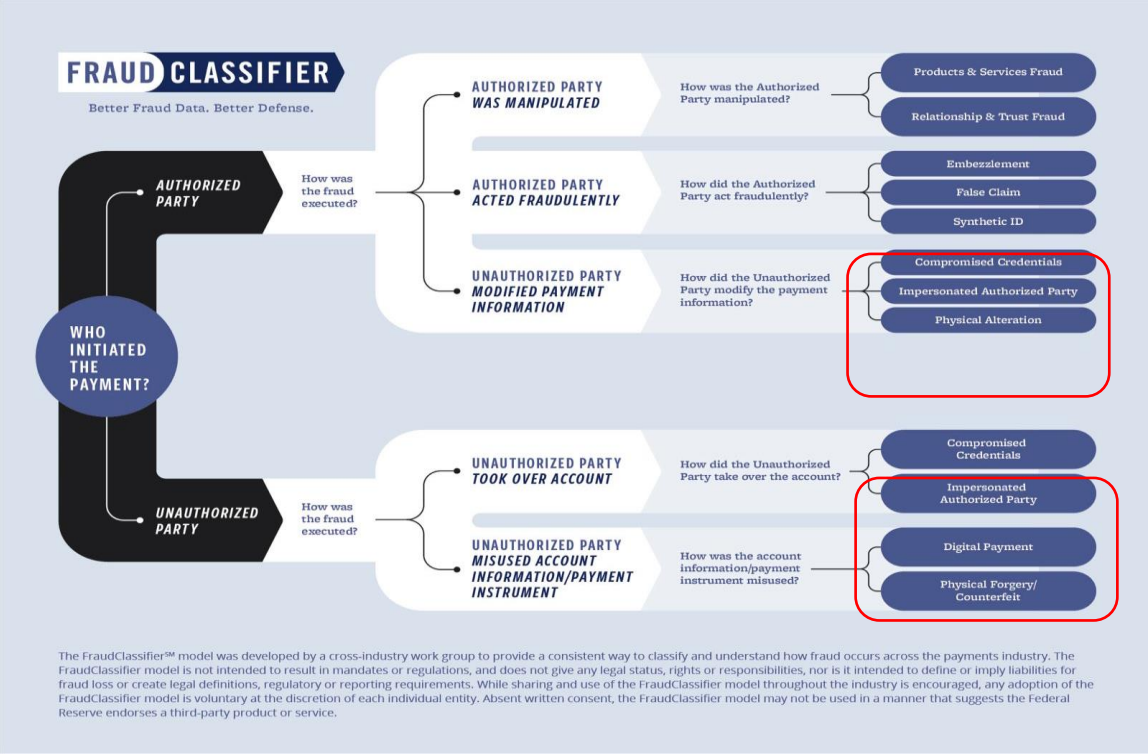
Through SIM cloning, the fraudster will be able to see incoming messages and modify the victims' account passwords by virtue of SMS OTPs being used as the standard two-factor authentication method. The victim's passwords, PIN, OTP, and other credentials can be readily hacked by the fraudster, who can then use them to commit financial scams, extortion, and other crimes.

[18] https://indianexpress.com/article/explained/explained-sci-tech/sim-sawp-scam-9003615/

CUSTOMER AUTHENTICATION THROUGH VARIOUS FACTORS OF AUTHENTICATION IN BANKING – CURRENT METHODS AND THEIR FEASIBILITY

The pandemic particularly accelerated the adoption of contactless and online payments. With such increased adoption, the question around security and safety of digital transactions is bound to arise. In order to ensure that the digital payments ecosystem is fraud averse to the highest potential with minimal to negligible monetary and data leaks, online transactions are authenticated using OTPs delivered to the registered mobile number or email of the customer. This 2FA/ AFA mechanism helps in keeping unauthorized users from accessing sensitive information and from minimizing frauds.

To better understand frauds, here's a quick snapshot of fraud occurrence when the payment is initiated by the authorized party vis-à-vis an unauthorized party:



Source: The Federal Reserve – FedPayments Instrument

Things to note:

- *The above diagram[19] is an example of a typical fraud classifier used globally*

[19] https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/

- *A similar framework can be adopted for the Indian landscape as well, since the primary factors remain the same, broadly.*

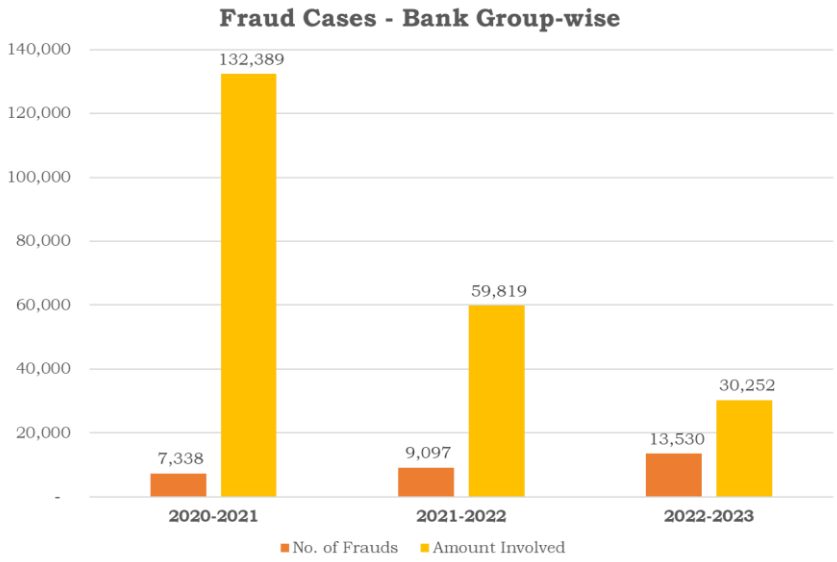
1.2 Current Methods

Since the OTP is shared on the customer's registered mobile number or email ID or both, it acts as a good deterrent to financial fraud since the customer has full control over his phone and personal details. However, over the years, digitization has resulted in fraudsters becoming increasingly sophisticated. From hacking OTPs to sharing fraudulent links via messages and email to hack into customers' phone and ultimately bank accounts, committing financial fraud has also become advanced.

The recent FedEx fraud is a jarring example of how customers fall prey to financial frauds due to these fraudsters having access to a customer's sensitive personal information.[20]

1.3 Feasibility

RBI Annual Report 2022-23[21] states that majority of the frauds have occurred predominantly in the category of digital payments (card/internet) in terms of volume. The Annual Report has further classified that small value card/internet frauds contributed maximum to the number of frauds reported by the private sector banks, and the frauds in public sector banks were mainly in loan portfolio.



Data Source: RBI Annual Report 2022-

In the current context, majority of the frauds occurring at the time of authenticating a customer when they make an online payment, happen on account of usage of SMS based OTPs. In today's technologically advanced environment, SMS OTPs have proved to be more and more inconvenient

[20] https://www.indiatimes.com/news/india/woman-details-losing-money-from-all-accounts-fedex-mdma-scam-607547.html
[21] https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/0ANNUALREPORT20222322A548270D6140D998AA20E8207075E4.PDF

by the day. This is largely due to delayed or non-delivery of SMS OTP (as detailed in the previous section) or incorrect entry of OTP by the customer. This results in a hop in the customer's digital payment experience while also leading to reduction in Gross Mercantile Value for merchants. Additionally, SMSes, are insecure, non-encrypted, non-cryptographic protocol and its contents can easily be accessed/ hacked when compared to the technology-based alternatives, as outlined in this paper. Moreover, SMSes are subject to frequent hijacking attempts through SIM phishing attacks, SIM cloning, etc.

RBI's BE(A)WARE booklet[22] talks about OTP-based frauds. In these cases, fraudsters impersonating as NBFCs or Banks, send SMS / messages offering loans or enhancement of credit limit on NBFC/bank customers' loan accounts, and ask the customers to contact them on a mobile number. When the customers call such numbers, fraudsters ask them to fill forms to collect their financial credentials. Fraudsters then induce / convince the customers to share the OTP or PIN details and carry out unauthorised transfers from the customers' accounts.

Problems with SMS-based OTP

With the rise in use and ease of online payments, the number of financial frauds has also risen. Fraudsters have found sophisticated methods to swindle people. One such way through which hackers commit financial fraud is OTP hacking and mirroring. Fraudsters have devised increasing number of ways to dupe unsuspecting individuals by leading them to disclose sensitive personal information (such as OTPs, card details, etc.) to steal their hard-earned money.

According to the Karnataka Criminal Investigation Department, OTP-based financial frauds have snowballed, especially in the last few years, in which criminals dupe the bank customers into revealing the OTP or access these OTPs by gaining access into the customer's smartphone. Even as customers become more aware and cautious, another way that the fraudsters have found to bypass the OTP deterrent is that they request the customer's bank to change the registered phone number linked to the customers' bank account. In these cases, a fraudster walks into a bank, impersonates the customer it is trying to defraud, requests a change in their registered mobile number and uses the new connection to receive OTPs for transactions.[23]

OTP scams have become so innovative that criminals have begun duping a bank customer by contacting the customer's mobile operator with fake identity proof, leading the operator to deactivate the original SIM card and providing a duplicate SIM card to the fraudster, thus generating OTP on the new number and defrauding the customer.

[22] https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf
[23] https://cyberpolicebangalore.nic.in/general-awareness/otp-fraud.html

Around 9,34,109 incidents accumulating to INR 1,434.75 crore is the estimate of the loss incurred by the customers due to Phishing, Vishing and Credential/OTP compromise between April 2020 and March 2022.[24]

In August 2023, NDTV also released a documentary on India's OTP scams called, "Inside India's OTP Mafia - Nuh To New York" where it portrays how around 20,000 Indians (only includes the number of cases reported) fall victim to cyber criminals, every day.[25]

Hence, to protect the sanctity of the flourishing growth of India's digital payments ecosystem, it is imperative that all stakeholders, including industry players, regulators, policy makers and the government take appropriate steps to address the growing concern around customer's financial safety. To this front, the industry has collectively endeavoured to make certain suggestions that may be considered to in place of SMS based OTP transaction authentication.

[24] https://timesofindia.indiatimes.com/business/india-business/over-9-lakh-incidents-of-phishing-otp-compromise-reported-in-last-two-years-42-indians-have-experienced-financial-fraud/articleshow/93361388.cms
[25] https://www.ndtv.com/video/shows/ndtv-special-ndtv-24x7/inside-india-s-otp-mafia-watch-ndtv-s-investigation-you-could-be-their-next-victim-719975#pfrom=home-ndtv_topscroll

SUGGESTED ALTERNATIVES

1.4 For transaction intimation to communicate alerts

As stated above, such widespread cases of frauds and thefts on account of legacy systems and underutilization of modern technological tools pose as a barrier to India's growing digital financial ecosystem. With increased access to the internet and smartphones, the time is ripe to consider alternate modes of transaction intimation (and authentication which is detailed below) to scale the ecosystem further.

And primarily, to remedy the increasing number of frauds using SMS channels, as detailed above, the following alternatives along with their rationale are suggested:

1.4.1 In-app notifications (for smartphones)

In most cases, online payments are either Card Not Present (CNP) transactions or Card Present (CP) transactions. CNP transactions, generally include UPI payments, scan and pay, money transfers using the app, netbanking, etc. Such payments are facilitated through the mobile application of a payment service provider, i.e., the customer's bank or a Third-Party Application Provider (TPAP).

i. *CNP Transactions*

In cases where the payment is made using the app, the customer anyway has the mobile application of their preference and choice downloaded on their smartphone and have that app open on their phones at the time of making the transaction. Hence, in CNP transactions, having the customer notified of their transactions via the app itself ('In-app notifications') can make the customer journey seamless by creating a single channel of communication for the customers to remain updated about their transaction history. Transaction and account-based notifications may be prompted on mobile application of the banking app or TPAP of the customer under such in-app notifications.

As per industry insights, it is noted that in comparison to the cost of one in-app notification which is estimated to be INR 0.001, the cost for sending one SMS is estimated to approximately be INR 0.12. Additionally, time sensitive SMSes (OTPs) are charged at a higher rate than short messages or general messages.

As mentioned above, India's digital transactions stood at 13,686 crores as on February 2024. Keeping in view the cost for SMS vis-à-vis in-app notifications as iterated in this section, the approximate cost of sending in-app notifications would have been INR 13.686 crore in comparison to the cost of sending SMS-based notifications which would have been approximately INR 1642.32 crore.

SMS-based notifications experience multiple hops both in terms of transaction intimation and reception of OTPs. Therefore, customers have a hassled experience when it comes to SMS-based notifications which are not only limited to non-reception of the SMS altogether but also of receiving phishing and fake messages. Therefore, as per industry estimates, compared to the failure rate of SMS-based notifications, that of in-app notifications is relatively lower. And since in-app notifications have no third party involved in the delivery of the notification, there is a possibility in reduction of frauds. Additionally, customers generally have additional factor of authentication (AFA) to open these apps. Hence, absence of any intermediary allows the data to be secured within the banking ecosystem or that of the RBI regulated entity providing the digital payments services, as the case may be, and therefore, will be required to adhere to all data security guidelines or directives issued by the RBI.

ii. *CP Transactions*

CP transactions (such as Point-of-Sale (POS) and ATM transactions) where the customer uses their card to transact instead of transacting through the banking/ finance application, in such cases, SMSes may be continued to be used as a mode of intimation and authentication for all customers (a smartphone or feature phone user).

However, it is pertinent to note that RBI has now enabled QR-based ATM withdrawals and QR-based POS transactions. In these cases, since the customer will anyway be required to open the app/ use their smartphone to access the QR code, in-app notifications, instead of SMSes, may be considered as a mode of intimation and authentication.

To conclude

Changing preferences based on India's demography

India's internet and smartphone penetration has undoubtedly proliferated. However, India still has a large population that uses feature phones.

RBI on March 10 introduced UPI123Pay, a new system for digital payments using UPI on feature phones without internet. For feature phones users, UPI123Pay aims to solve the problem of requiring internet, cameras, and more by offering payments via interactive voice response (IVR) numbers, feature phone apps, missed calls, and sound-based payments. RBI also announced the roll-out of a 24x7 helpline for digital payments, which it calls DigiSaathi. The entire infrastructure is supposed to help bring digital payments to the large section of Indian mobile phone users who still carry feature phones.

While steps are being taken to include the feature phone users to the Digital India ecosystem, SMS as a mode of transaction intimation can be continued to be used for such vast feature phone user base. In the meantime, the below suggested alternatives can be considered for smartphone

users since the count for transaction for tech savvy and smartphone users is more as compared to feature phones. Mobile-based transactions jump to 52.15 billion in H1 of 2023 compared to 33.55 billion during the same period in 2022.[26]

Between January 2022 and June 2023, payments acceptance infrastructure channels saw a surge. PoS terminals grew by 44% to 8.09 million while BQRs grew by 21% to 5.69 million. UPI QRs grew by 79% (already on a large base) to 272 million. This growth in UPI QRs is also reflected in the growth in UPI transactions as well as how it has had an impact on other forms of payment.[27] These numbers showcase the increasing use of smartphone/app interface to make payments.

Therefore, for both CNP and CP transactions where the user is a smartphone user, in-app notifications may be considered to be implemented in a phased manner. The RBI may consider a hybrid model by enabling in-app notifications for small-value transactions with a set threshold and continue with SMS based alerts or transactions beyond that threshold. For example, for transactions up to INR 5000, in-app notifications are sent to the consumer for their transactions, and for transactions of a higher value, beyond INR 5000, SMS alerts could be continued to be pushed by the Issuers.

1.4.2 Web-based mass messaging apps/platforms

India is one of the largest markets for cross-platform messaging applications, with over 89%[28] of internet users active on one or more messaging applications.

Web based messaging platforms offer enhanced communication capabilities in areas of consumer engagement starting from customer acquisition to service delivery to support through business branding, rich media integration, and enhanced interactivity. As a result, a host of companies including brands, banks, shopping apps, and more have started using these messaging applications as a mode of communication for order updates, delivery timelines, promotional messages, booking information such as flight tickets, train tickets, etc.

Some key features of these web-based messaging apps are as under:

i. Interactive & Actionable – these apps allow for a two-way communication channel and hence can offer a more engaged customer experience through the use of images, videos, audio, files, GIFs, documents, and more. Further, these apps can:
   - Give an option to consumers to decline a transaction real time without calls/ IVR;
   - Act as digital passbook;

[26] https://in.worldline.com/reports-and-insights#2023
[27] https://in.worldline.com/reports-and-insights#2023
[28] https://engage.sinch.com/blog/messaging-apps-in-india/

- Give customers and option to update the financial service provider in case of a fraudulent transaction;

ii. Multilingual capabilities – these apps have multilingual capabilities which allows a customer to opt for receiving messages or voice notes in their mother tongue or any other language of their choice, thus deepening financial inclusion

iii. Secure & Private – these apps allow businesses to get verified badges (showcased through ticks of various colours) to ensure that the messaging is from an authentic source. Moreover, most of these platforms are end-to end encrypted, i.e., from the customer's device and messaging service provider to the business itself, all in-transit and sent/received messaging are encrypted and locked down to prevent unauthorized access.

iv. Cost Effective - The character limit and non-interactive nature of the SMS makes it a costlier form of communication. In comparison, these web-based platforms are a cost-effective channel to communicate with the customer, and at the same time allows a business to build a relationship which fosters trust.

v. Convenience – On account of high adoption rates, these messaging applications are also the most quickly reachable mode of communication. These days, most customers use one or more of these apps on a regular basis for social and or business-related conversations. This is in contrast to the utility of SMSs in the present day and age, which is limited to Unsolicited promotional and spam messages coupled with transaction authentication and alerts. Hence, it makes it more convenient and user friendly from the customer's perspective to use these apps for authentication purposes and transaction alerts.

It is critical to note that the apps are subject to hacking attempts as well. However, the cyber security measures typically put in place (within their app code) by the app providers is extremely rigorous and elaborate, making them a far more safer option as compared to say an SMS.Given the multiple advantages, web-based messaging apps can be used as a channel to send transaction alerts to customers.

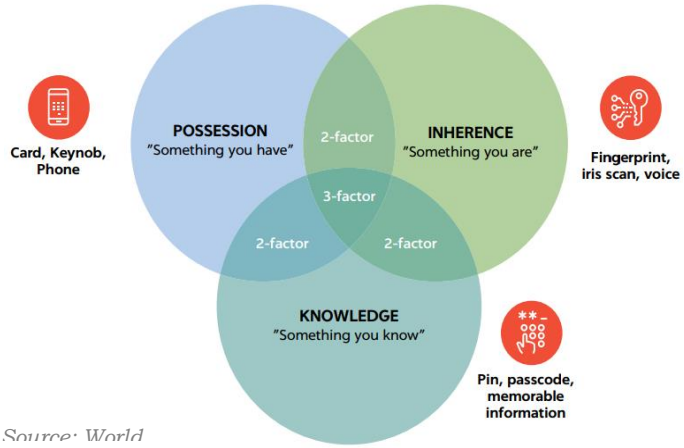
1.4.3 Email intimation

In case of emails, a customer's email is considered to be one of the most secure channels of communicating with them. As stated above, regulatory requirements also prescribe email as a mode of communication and intimation, wherein it is mandatory for banks and PSPs to intimate the customer about the transaction in case of debit/credit cards[29]. It is pertinent to note that presently, Email based transaction alerts are optional for payments processed through other channels like net banking or PPIs[30].

[29] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=6309&Mode=0
[30] https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=11040 ; https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=11446

Given the relative safety and security of emails over SMSs, it is thus recommended that emails can also be considered as a replacement of SMS as a method. In this regard, the RBI would have to direct all Banks and PSPs to mandatorily register email ids of all customers.

While the aforementioned recommendations largely cover customers transacting digitally using a smartphone, it may be noted that the suggestion is not to do away with SMSes as a channel of communication in entirety. For example, India still has a considerable population that uses feature phones and may SMS based intimation will practically work for such segment of customers.



Source: World

1.5 For customer authentication through various factors of authentication in banking

A customer is generally authenticated using any of the three types of factors of authentication illustrated on the right. Typically, an authentication mechanism is considered as strong and secure as long as it meets two of the three factors illustrated here.

From the above, it is evident that the time is ripe to consider alternative methods of authentication. Globally, the regulators are actively seeking alternatives to SMS OTP as an authentication factor. In Europe, the implementation of the revised Payment Services Directive (PSD2) has led to the requirement of a Strong Customer Authentication (SCA) regime. The SCA is aimed at reducing fraud and making online and contactless offline payments more secure. The SCA regime envisages biometrics, retina/iris, etc. as the new-age authentication factors.

Under the SCA regime, a SMS based OTP does not qualify as the knowledge 'factor' when used as the sole authentication factor, instead, it is stated that only a combination of SMS based OTP with a PIN/passcode (which the user knows) will be considered as a (knowledge) factor. Hence, it is clear that there is an intention to move away from SMS based OTPs and towards alternative mechanisms of authentication.[31]

[31] https://www.eba.europa.eu/sites/default/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

Even RBI's Payments Vision Document 2025 mentions exploring alternate risk-based authentication mechanisms for digital transactions that leverage behavioural biometrics, digital tokens, location / historical payments, in-app notifications, etc. Basically, these suggested alternatives have the potential to reduce the social engineering risk of frauds since there are no OTPs to steal.

These alternatives are suggested keeping in mind the core idea of safeguarding the customer while ensuring ease of use.

Case study in reference: Leading App for Securities Trading

- The App Code is cryptographically secure, ensuring only the recipient can view the message.
- The App Code is only valid for 30 seconds, and a new code is generated once the previous code expires.
- Time-based OTPs (TOTPs) are behind an additional layer of authentication, like biometrics and can be stored and generated on a hardware device.
- They do not require external network connectivity like an SMS gateway to

1.5.1 App Code

RBI may consider opting for an app code to verify and authenticate the customer during an online transaction. This method is expected to preserving safety and security of a digital transaction.

It is pertinent to note that the customer's payments/ bank/ investment apps anyway use 2FA to log in to their accounts. This generally includes an m-PIN or the customers' biometric (fingerprint/face ID, etc.). Hence, to read the OTP received on the app, the customer would be required to open the app using the relevant 2FA mechanisms. Additionally, since this OTP would be triggered by the Bank/RE, no third-party such as a telecom service provider would be involved in triggering the OTP. In addition to the above, these app codes can be time-based that expire in 20-30 seconds. Upon the required time frame elapsing, a new code would automatically be generated, and the customer may be required to input the revised OTP received on the app.

1.5.2 Device based Biometric authentication

Biometric as a mode of authentication has continued to grow. It is a method where the customer is their own password. An advantageous development at the back of technological advancement is that today, payments can be authenticated using a customer's face, iris, fingerprints, voice, etc. A host of apps use biometric as a 2FA for logging the customer on to their app.

With wearables paving way for becoming a mode of making payments, it is pertinent to note that the authentication mechanism on these wearables include fingerprint scans, facial recognition, iris recognition, heartbeat analysis, and vein mapping.

Hence, to avert the risks of identity theft and financial frauds, biometric authentication can become a reliable and secure option for digital payments, specifically for smartphone users.

In addition to the above, certain other alternatives include:

Case study in reference: Leading Identity Verification and Authentication Solution Provider

The Provider's Authentication system works by providing the customer with a frictionless/password less login experience. The Provider's system works as under:

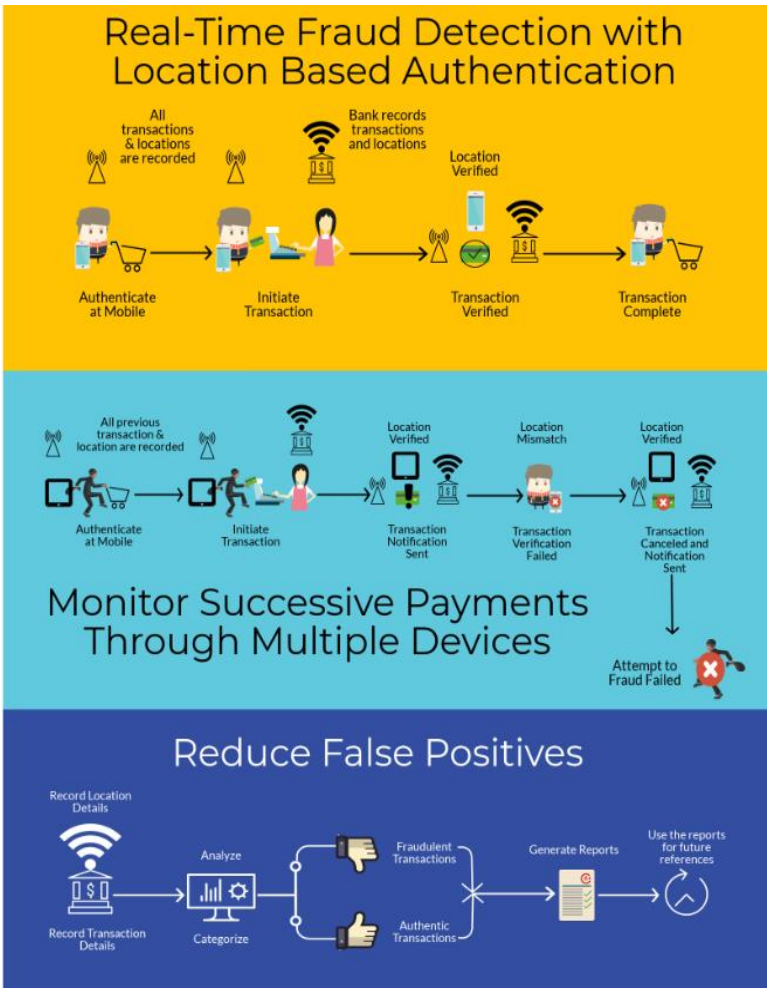
- The customer logs into their account via app, mobile web, or other channels (e.g., Desktop) using cryptographic keys on the mobile device (e.g., the PIN used to unlock your mobile, laptop, etc.)
- Verification of the customer is done by confirming Provider's cryptographic key on consumer's device
- The Provider uses authentication modes based on the widely accepted FIDO2[1]
- Not only is this authentication method Password less but it also enables the customer to configure use of device biometrics (Face, Finger), without use of OTPs or Passwords
- Protects against account open fraud vectors including: First Party (false fraud claim), Third Party Fraud (Identity Theft) and Bot Attacks

a. Mobile Auth – A mode of authentication that passively authenticates the device phone number via mobile network signals for any use case without friction, allowing businesses to seamlessly authenticate active SIM cards. In this mode of authentication, verification comes directly from mobile network operators. Therefore, the customer is only required to only enter username/mobile number. No password or OTP input is required since the verification is obtained directly through the network operator thus reducing friction of passwords and OTPs.

b. Geolocation Authentication -

This authentication mode allows users in a particular geographic area to seamlessly access products and services without requiring them to input any OTP or password or other credentials. Geolocation authentication authorizes a user's access based on the location assigned to their IP address. This is done using information such as the Latitude, Longitude, and Altitude derived from the geolocation. Example of location-based authentication includes corporate mail, military area, banking etc.

The aforementioned models not only act as a stricter safeguarding measure for the customers but also allows unlimited use while maintaining a cost-efficient per user pricing model as compared to transactional OTP pricing models.



Source: Clari5[1]

1.5.3 Web based mass messaging apps/platforms

As stated above, these apps have emerged as the most preferred channel of communication between the masses on account of affordable internet and widespread smartphone adoption. In recent years, the platforms have facilitated interactive and two-way B2C and C2B communications. Given the popularity, the convenience, the cost effectiveness, security and the multilingual ability provided by these platforms, these platforms can be used as a channel of authenticating transactions through OTPs.

While Banks and PSPs can use the RCS/ messaging platforms as an alternative method of authentication by sending OTP on these platforms, SMS can be deployed as a fallback if a consumer doesn't use the messaging platform or if a message isn't picked up after a certain amount of time. In such cases, the OTP can be automatically dispatched via SMS instead, ensuring that the OTP is delivered to the customer to authenticate the transaction. The

messaging platform can also be used to obtain consent from the consumers over the choice of channel to receive OTP and transaction alters.

Case study in reference: Leading Platform for Business Messaging

- The enterprises in retail and ecommerce/ travel and hospitality space are using these messaging platforms for customer acquisition, helping consumers login through OTP on the messaging platform, sending immediate post transaction alerts and tracking the delivery of the order all on the same channel to offer an enhanced and seamless customer experience;
- These platforms follow end-to-end encryption and offers a verified badge for business for brand identification;
- Brands on these platforms use 2-way communication with the customers for various purposes, for e.g.: rescheduling appointment, live location for pick up, consent for returns, handling Disputes and grievance redressal;
- Businesses are also engaging with customers through voice notes and messages in language of customer choice for sending updates;
- Businesses are using these messaging platform for enabling login and sending updates even when the customer is traveling outside India, as the messaging platform doesn't need a cellular network and can work over Wi-Fi.

CONCLUSION

Keeping in mind the technological advancements and increased adoption of smartphones and internet penetration over the years, digital transactions have grown multifold. Such an increased preference for digital modes led to an increased regulatory oversight in terms of customer protection and safety measures.

With reference to Para 5 of the RBI circular on Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions dated July 6, 2017[32], banks are required to register their customers for SMS alerts for electronic banking transactions.

However, while the development in India's digital payments ecosystem has been robust, financial frauds and cyber security crimes have also risen and become more sophisticated over the years. In such a case, relying on SMS OTPs as a single mode of authenticating digital payment transactions may lead to increased scams and financial losses for the users.

New business models in the financial services space are emerging at breakneck speed. In such a scenario, relying solely on SMS based OTP as a mode to authenticate the customer/ transaction may prove to be relatively conservative. Additionally, if SMS based OTPs are relied on as a sole source of verification and authentication, in the coming years, when the number of text messages that will be required to be sent will nearly double, the additional cost of these messages will have to be passed on to customers to reach operational efficiency. Furthermore, in this online era, where everything is available on an app, customers blindly grant full permission to apps (without perusing through the terms and conditions) to scrape their phones for SMS messages, call logs, pictures, and other such permissions. This poses a security as well as privacy threat. Even though FinTechs and financial institutions have undertaken preventative as well as mitigative measures to curb the security flaws and make their digital platforms more secure, in general, technological advancements have made room to explore alternatives to SMS OTPs.

Ideally, authentication factors and channel for intimating transaction alerts should be in line with technological innovations, industry practice and customer choice. Therefore, to protect the customer's financial safety and also safeguard them from bearing SMS charges, especially when new, innovative and secure alternatives have become available, this paper endeavoured to draw attention to how it can help further RBI's vision of finding alternative authentication mechanisms for digital payments.

Affirmatively so, as stated above, even the RBI has expressed its intention to adopt a principle-based "Framework for authentication of digital payment transactions".

[32] https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=2336