



# BANKING FRONTIERS

- ▶ Alternate Channels @ Indian Bank
- ▶ HFCs and Risk Management
- ▶ Fintechs in Switzerland
- ▶ Corporate Communications

[www.bankingfrontiers.com](http://www.bankingfrontiers.com)



ANGAJ BHANDARI



SUNITA HANDA



VIJAY CHUGH



LALIT MOHAN



MUNISH MITTAL

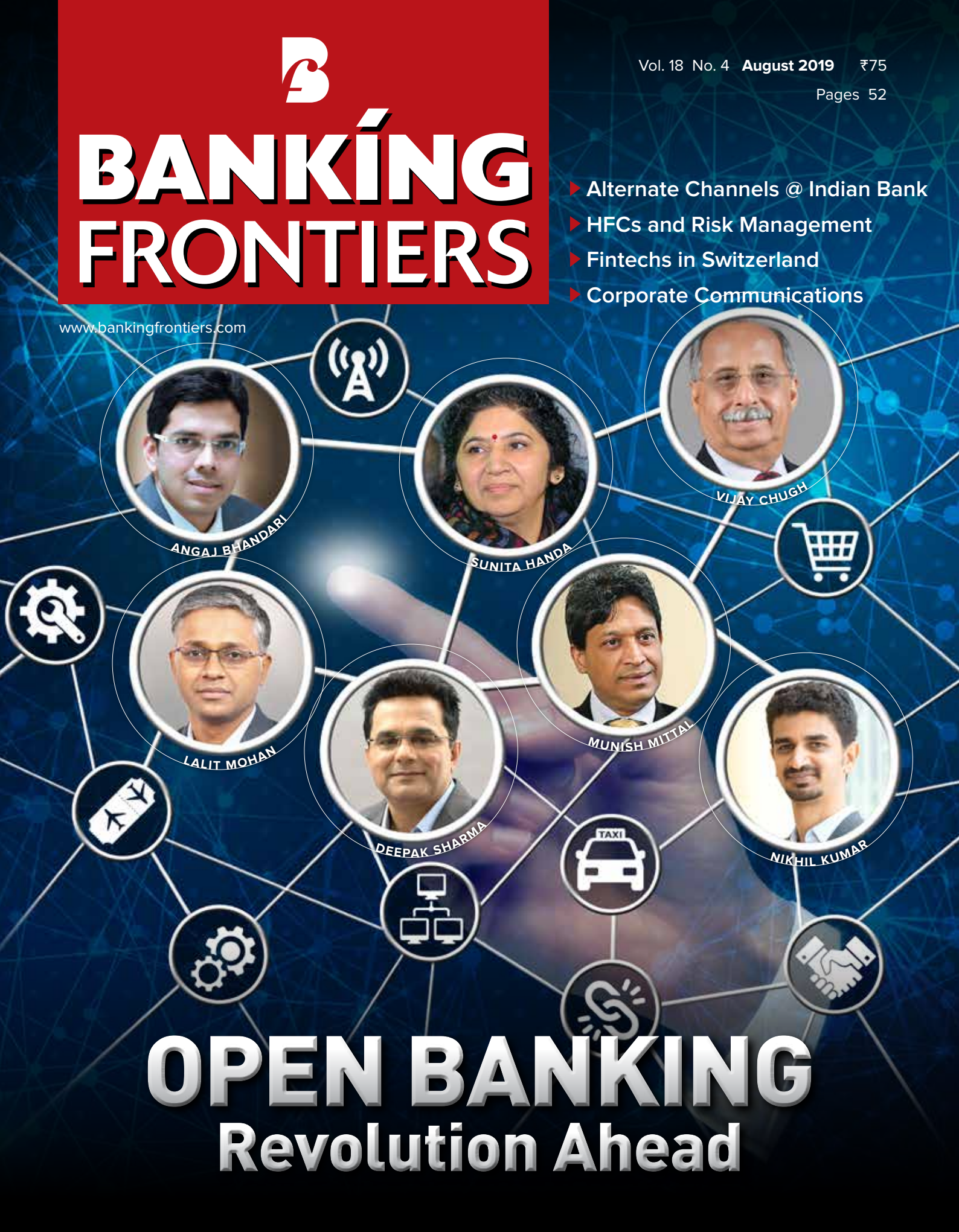


DEEPAK SHARMA



NIKHIL KUMAR

## OPEN BANKING Revolution Ahead





# OPEN BANKING Revolution Ahead

While open banking is creating a buzz in Europe and several countries, bankers in India are curious to know the progress and the prospects. Banking Frontiers spoke to a few banking technocrats and discovered a promising scenario:

**A**pplication programming interfaces, or APIs, are leading a wave that's transforming today's banking scenario. Standardized and easy-to-implement APIs are supplementing several other disruptive technologies that are making inroads into banks. Most banks are adopting such technologies wholeheartedly to gain agility and move ahead of the competition. APIs could actually become the greatest banking innovation in the current generation. If there is any resistance to mass proliferation, it could be the slower evolution of standards and regulation whose support is critical.

APIs are today heralding what is described as open banking, which is enabling third-party developers to build apps and services around more traditional banking and financial services. Open banking leverages open data to create better financial transparency. It is crucial because a bank customer can access his or her data, facilitating better and informed decisions on choice of bank products

and services. It is also a key factor in creating competition among banks, which means better products and services.

## ADVENT OF PSD2

What has indeed become a fillip for open banking is the revised Payment Services Directive 2, or PSD2, a regulation enforced by the European Union, which came into effect in January 2019. It seeks banks to open their services to third parties so that they can initiate payments and aggregate information for customers. What the European Payments Council has done is that it has asked developers to make banking APIs follow certain uniform standards. This is expected to create a banking system where services of banks can be availed of by individuals, corporates, other banks and market players in a more cohesive, transparent and efficient manner.

Indian banks are privy to these developments and are quite eager to adopt the system. Of course, lack of standards and

regulations are points of worry for them. Let us first discuss regulations. It is assumed that Indian regulators have 3 options. They can be pro-active, active or reactive. The question that arises is which is the best fit for India? Is it better to be a pioneer or to learn from the experiments of others and then put in meaningful regulations? Where should the regulator seek the balance between innovation and stability?

### REGULATORS NEED TO BE BALANCED

Deepak Sharma, chief digital officer at Kotak Mahindra Bank, feels that Indian regulators need to be balanced and active by bringing global insights, innovation, risks and the financial inclusion framework as the foundation for open banking. He commented: “India follows the account aggregator standard for sharing customer data with customer consent among regulated entities. The purpose is quite similar to open banking / PSD2 standards. We have well-defined API interfaces and clearly defined roles and responsibilities between the financial information provider, financial information user and the account aggregator in the account aggregator ecosystem. Various banks have already begun working on an account aggregator model.”

Sunita Handa, chief general manager (IT-Channels & Ops) at State Bank of India, believes that while it is true that most of the time innovation will be ahead of regulation, the regulatory authorities in India are not much behind in promoting and participating in digital innovations. “For example,” she said: “UPI and account aggregators showcases the pragmatism of the Indian banking regulators as far as open banking is concerned. Initiatives like setting up a regulatory sandbox provide a structured avenue for the regulator to engage with the ecosystem and to develop innovation-enabling or innovation-responsive regulations that facilitate delivery of relevant, low-cost financial products. RS like tools enable more dynamic, evidence-based regulatory environments which learn from, and evolve with, emerging technologies. So, in my view, the best fit is a mix of pro-active, active and reactive intervention by the regulators.”

### MOTHER OF ALL OPEN BANKING

Unified Payment Interface, or UPI, developed by the National Payments Corporation of India (NPCI) can be considered as the mother of all open banking APIs in the world, maintains Munish Mittal, CIO at HDFC Bank. He believes India does not have any dearth of regulatory institutions and experts. “With people like Nandan Nilekani and organizations like the RBI, Niti Aayog, NPCI, etc, the country (and thus the regulator) has done a fantastic job with UPI. Aadhaar validation means that the country offers an authentication API for the identification of a citizen for facilities such as open telecom, open commerce, etc. The government,



**Sunita Handa** opines that government regulations on open banking ensure that banks share customer information over regulated frameworks

regulators and the department of financial services have been pro-active, and this facilitates financial inclusion for larger strata of society,” he explains.

Mittal also points out to the NBFC account aggregator model, which is coming up. Online validation of credit report using API, etc, and other pilots being done using blockchain, 26AS, etc, are pointers to the proactive stance that the country has taken.

### NEED FOR ORGANIC MODEL

Angaj Bhandari, country manager for India & South Asia at FIME, raises the issue whether regulators should follow an organic or prescriptive model. He believes that each market should take an individual approach, but regulators and interbank networks (like NPCI) can learn lessons from other markets, such as Europe’s PSD2. “Ultimately, though,” he argues, “each market should design a regulatory framework and innovation initiatives that suit their own financial sector and unique consumer sentiment.”

Vijay Chugh, former CGM & head of Department of Payment & Settlement Systems at Reserve Bank of India, feels PSD2 will bring in more competition and hence lower pricing, which will be beneficial to the customers in Europe, where risks are high, and costs too are high. What PSD2 does is limit the risks and hence lower the costs, as it reduces the cost of branches, reconciliation, etc, by creating an open banking model, he explains.

“In contrast, India is taking baby steps. Our UPI is an open banking platform. So, there is no need to go to each bank for a tie-up. PSD2 is a handshake platform. It empowers companies like Google and others to provide APIs and connect customers with their banks,” says he.

Nikhil Kumar, co-founder & chief evangelist at Setu, which builds low-cost, modular API infrastructure, concurs and says that regulators have been pro-active for a lot of policies including platforms like UPI. However, he believes there is no one size fits all as the world is changing at a rapid pace, and hence recommends an active-active approach. Regulators, says he, should do the minimum and allow enough room for banks to innovate. This could be a combination of setting standards and allowing banks to innovate on their API offerings.

### CUSTOMER CRITERIA

“How does open banking consider the needs of customers? The key issue is trust between fintechs and the customers and, indirectly, it is the banks that are exposing their data through these fintechs. Crucially, it is the responsibility of banks to welcome these new participants into the transactional e-banking channel without compromising the integrity of payment data and user experience. This is the biggest challenge facing banks today in the age of open banking,” comments Angaj Bhandari of FIME.

These challenges aren't limited to the compliance of bank interfaces (APIs) or the securing of third-party channels, but to the authentication journey of the payment service user too. In Europe, this has been the source of a lively debate between TPPs (fintechs) and ASPSPs (banks). Deciding how strong user authentication is (Secure Customer Authentication (SCA), 2-Factor Authentication etc.), through which authentication channel it will need to go through (redirected from banks or decoupled and via Fintechs), and how it impacts the user experience are all central points of contention.

Bhandari adds that this is fundamental for banks, "Demonstrating that their API and authentication methodology do not create any unnecessary points of friction is important in ensuring end-users aren't dissuaded from using the services of fintechs."



**Deepak Sharma affirms that API security revolves around the strategies for rollout and implementation**

In the UK, the Open Banking Working Group (OBWG) has released the standard for open banking. As for India, the RBI has permitted only NBFCs to perform the role of account aggregators. The NBFCs would provide account aggregation services in response to a specific application by the customer for such a service and would be backed by appropriate agreements and authorizations," she explains further.

An account aggregator will be required to have a board-approved policy for pricing services. The pricing will be in strict conformity with the internal guidelines adopted by the account aggregator, which need to be transparent and available in the public domain. Further guidelines are expected once the above system goes live and provides new experiences for all stake holders.

### SEAMLESS JOURNEY

Vijay Chugh emphasizes that the ultimate goal of open banking is to provide one seamless end-to-end journey for the desired outcome of the customer. A seamless experience is safer for less educated customers, which is a major criterion in any developing country, including India, he adds.

Nikhil Kumar avers API banking has the ability to improve customer experience multi-fold and he suggests that it is the strategy that banks will adopt in future to add value to existing customers and acquire new customers. "There is no reason why a small business owner cannot access his bank account from his accounting software. We have the tools for it and that will be the future - when banking will go where the customer goes," says he.

### NEED FOR BEST PRACTICES

Have standards and best practices evolved in APIs?

Lalit Mohan, senior domain expert, at Institute for Development and Research in Banking Technology (IDRBT), points out that there are recommendations and guidelines that can be drawn from PSD2, BIAN, W3C, regulators and government bodies in India, New Zealand, Hong Kong, etc. He strongly believes banking industry in India has an advantage of less legacy systems and processes to contend with compared to some of the old global banks. "However, the work on standardization (naming, signature, versioning, etc) and best practices on APIs are in the early stages. I expect this to quickly mature in the next few months to strengthen API banking," says he.

Sunita Handa of SBI is of the view that government regulations on open banking ensure that banks share customer information over regulated frameworks. This will help banks and third-party service providers gain additional insights about customers, and, in turn, innovate their banking products. "Following the implementation of the PSD2 regulation, banks in Europe will need to provide customer transaction data to account information service providers (AISPs).

### CONCRETE PRACTICES

Deepak Sharma of Kotak Mahindra Bank stresses on 4 concrete practices: (i) have an internal centralized repository for APIs to ease discoverability of existing APIs. (ii) use standards such as WADL/ Open API specs to build and publish APIs, which will help in long-term manageability and auto generation of codes. (iii) have a micro services framework to build and deploy APIs faster. (iv) publish external APIs through a developer portal / API manager, which will help scaling of integration with partners, in addition to enhanced security.

Munish Mittal of HDFC Bank outlines the standards and practices followed by his bank in this regard: "We have a formally designed process of standards for opening our APIs for partners such as Zerodha, Swiggy, etc. This is under our IT policy - how APIs should be conceptualized, developed, onboarding, legal agreement, how to inspect payload, encryption, O-AUTH2, etc. It also clarifies what should be approved by IT head, business head and risk head. It also includes who will approve what type of API each partner should use for pulling data, payment, etc."

The bank has done this standardization last year and the base foundation is now complete. There is a review frequency defined in that for test of design and operating effectiveness and the bank keeps improving on this.

If a bank is operating in different areas, will it have to follow different standards? Angaj Bhandari of FIME argues this is more of a strategic decision for banks to take. "International banks must give enough flexibility to local branches to decide which API standard to implement and which API standard to give fintechs access to, simply because many fintechs have already started to perform their integration testing against existing APIs."

### QUESTION OF API SECURITY

APIs are now graduating from trial stages to mainstream usage, but

there remains a vital question about security, how security systems can be strengthened and the need for certification.

Nikhil Kumar of Setu points out that in the early days, APIs in banks were mostly developed and used internally. Externalizing these services requires investment in technology, people and partners. The industry is very nascent but there are a lot of playbooks on how to make this happen.

Tackling the tech aspect, Deepak Sharma explains that APIs are controlled by authentication (SSO, JWT, SAML, OpenID connect) and by authorization (O-Auth). Deployment of an API manager ensures security validation for the public API uses, with additional security measures - such as Rate Limit (number of requests/second), Quota Limit (daily usage access to APIs), Access Control (whitelisting IP or Domain) API Key Verification, Request Validation (header validation, content type), Certificate Authentication and Mutual SSL Handshake - all enhancing security.

Web services security, SOAP and REST APIs security have been topics of continuous research. These are as critical as mobile and web applications except that the interface is different. Lalit Mohan of IDRBT says while there are existing guidelines and best practices, banks are expected to continuously monitor on authentication, authorization, DDOS protection, data encryption and other protection mechanisms. He adds that IDRBT too is contributing by preparing an API security



**Munish Mittal maintains that UPI can be considered as the mother of all open banking APIs in the world**

and governance document in collaboration with the financial and technology sectors to recommend good practices.

HDFC Bank looks at various parameters for strengthening API security. The first is incoming data schema validation, which includes things like what kind of data format is being used, JSON data types, xml, etc. The second is authentication and authorization using device identification, time window, geo-location, digital certificates, user id+pwd, etc. The bank's strategy is to have a layered approach. For open banking, O-Auth is very important as it is 2-way SSL. The third is threat detection and checking if any malware is being injected. For this, there is need to decode any attachment and apply server grade virus scanning before saving it. The fourth is SSL everywhere to secure the channel and establish mutual trust and integrity. The bank ensures that all these are never done away with. Finally, it looks at rate limiters to limit the number of transactions.

API security is similar to financial services providers using various methods to authorize and authenticate payments. A trusted environment with policies for authentication and authorization is a must. Nikhil Kumar says, as emphasis on strengthening API security is increasing, there is need for designing standards to ensure security practices are not monolithic by design. As mobile scales, much more needs to be done to ensure new users who are using digital are safe and have enough protection, he adds.

## Future Course of Innovation thanks to API Banking

Use of new technologies has dramatically altered the course of innovation several times in the past. So, the critical question arises whether open banking will change the course of innovation for banks. If so, in what direction?

According to Deepak Sharma of Kotak Mahindra Bank, it will. He elaborates as new business models are driven towards the ecosystem-based model, open banking / API banking will become a critical foundation to create one's own ecosystem or embed in another ecosystem. "I expect more innovative solutions to be launched by banks with fintechs/startups. I believe that the future of banking would be around embedding banking services directly in the preferred app of the customer," he asserts.

He highlights 4 impacts derived from API Banking:

1. Building customer centric solutions in collaboration with fintech partners
2. Enabling faster launch of innovative solutions

3. Generating additional revenue streams with new business models
4. Distributing of banking products and services in 3rd party ecosystems.

Sunita Handa of SBI views open banking basically as creating a data architecture where a network of institutions can share the data through APIs. The data architecture is used to create guidelines on how customer data can be created, structurally stored and securely accessed. If this happens, she is sure, it would open the doors to a lot of innovation benefitting the single most important entity, that is, the customer. She goes on: "If the aspects relating to customer consent for data share and the authentication piece are well addressed, the innovation will be worth all the effort at all levels. Collaborations between banks and fintech will go to the next level to serve the customer in best possible ways."

"Absolutely," asserts Lalit Mohan of IDRBT.

"Banks are expected to take technology innovations to the next stage. They are expected to work with fintechs to co-innovate on various use cases for making API possible. UPI has already been a disruptor and driving innovation in banking industry. These changes are expected to make existing core banking software more as a system of records rather customer engagement."

Vijay Chugh sees open banking as a catalyst for new data revolution. It will enable bank switching and bank will not be able to demand loyalty as they have done so far, he believes. "Open banking also makes banking more agile and collaborative. Banks will also have to design business models to meet agile customer," he concludes.

Angaj Bhandari is of the view that the rising acceptance of new payment channels, particularly the mobile money transfers (P2P and Account-to-Account transfer) and authentication methods such as tokenization and biometrics are making these new payment channels more secure.

## COMMONLY USED METHODS

Sunita Handa lists some of the commonly used methods:

- 1. Use of tokens:** Establish trusted identities & then control access to services & resources by using tokens assigned to those identities.
- 2. Use encryption and signatures:** Encrypt data such that it requires signatures to ensure that the right users are decrypting and modifying the data involved, and no one else.
- 3. Identify vulnerabilities:** Keeping up with the operating system, network, drivers, and API components is essential. Know how everything works together and identify weak spots that could be used to break into your APIs. Use sniffers to detect security issues and track data leaks.
- 4. Use quotas and throttling:** Place quotas on how often your API can be called and track its use over history. More calls on an API may indicate that it is being abused. It could also be a programming mistake such as calling the API in an endless loop. Make rules for throttling to protect APIs from spikes and Denial-of-Service attacks.
- 5. Use an API gateway:** API gateways act as a major point of enforcement for API traffic. A good gateway will allow you to authenticate traffic as well as control and analyze how your APIs are used.

## SECURITY CERTIFICATIONS

Surely, banks cannot be secure by focusing only on their own systems. What security standards or certifications do they seek in the APIs of the companies they are connecting with?

Deepak Sharma says in Kotak Mahindra Bank all the communications are encrypted and O-Auth2.0 is used for securing access. Access is limited by whitelisting the IP address from where

### How is FIME helping banks?

FIME provides a range of services – from initial consultancy to test tool support. It has already helped a major French bank to comply with STET's open banking API standard and supported numerous banks in defining their strategy. FIME's experts are also supporting banks and fintechs to design, develop and deploy API test plans and ensure alignment with the regulatory technical specifications from PSD2. It's strategy is to bring to the digital hub, as it has in supporting STET, a mutualized standard testing infrastructure and services that can be exposed to members of interbank networks. The aim is to incorporate a number of API and security standards, as well as regulatory specification standards, to deliver a totally customizable, agnostic solution for players to 'pick and mix' elements in-line with their needs. FIME can cover any type of test requirement and deliver tailored test plans. The company is in touch with some 15 national interbank networks in Europe and with more than 40 payment authorities worldwide.



**Vijay Chugh emphasizes that the ultimate goal of open banking is to provide a seamless end-to-end journey for the desired outcome**

the request originates. Handling of access / security token and input validation are the key security standards the bank has deployed.

Lalit Mohan reveals that IDREBT is reviewing the existing ISO 27001, OWASP, W3C, PSD2, PA-DSS and other standards/guidelines to validate its applicability to APIs.

Angaj Bhandari of FIME offers an interesting perspective and discusses the company's recent launch of an Open Banking API test platform, TrustAPI, that provides a suite of API conformance tests to support Open API developers (Open API platform vendors, banks, interbank networks, third party providers and technical service providers). Harnessing the power of various standardization efforts globally, the tool supports testing in-line with the STET – a major European automated clearing house – open-access API standard, with work underway to incorporate other standards into the test library such as the Berlin Group's NextGenPSD2 and Open Banking UK

(OBUK) API standards. This ensures players can quickly test they have implemented APIs according to the selected or locally enforced API standards. Not only does this ensure interoperability with other actors, it also serves as evidence to the ecosystem of compliance, including regulators.

Munish Mittal points out that there are API-related certifications for UPI, RuPay, Mastercard, Visa, Diners, etc.

## EVOLUTION & TESTING

What are the challenges in testing the APIs? Deepak Sharma reminds us that API security revolves around the strategies for rollout and implementation - to identify and mitigate the unique vulnerabilities and security risks of APIs. The key challenges to address in payment system testing, he says, are to do with performance and security. "We perform load testing, functional testing, penetration testing and application security testing to identify and address the vulnerability before deployment," says he.

He also points out that API Manager is a critical tool both in terms of scaling the integrations and enabling standard security across APIs published on it. API security standards are defined for implementation of new APIs on the API Manager.

Lalit Mohan feels security and performance have always been a focus area for payment systems and this continues to be a focus for APIs as well. "Usability to enrich user experience of payment systems is gaining momentum and importance of API standardization is going to be pertinent to bring consistency and reduce development time of banks and fintechs," he adds.

He says Swagger is becoming a prominent tool for API testing. "Performance testing is going to be key as the human driven lag for CRUD operations is going to be machine driven. Existing performance and security tools can continue to be

leveraged to ensure ISO 27001, PA-DSS and other guidelines applicable in banking. Microservices, continuous integration testing and DevOps will gain momentum with increasing adoption of APIs in the IT heavy banking industry,” he predicts.

Angaj Bhandari of FIME dives deeper. He divides the entire testing landscape into 5 major components:

- 1. Functional testing:** Ensuring Open Banking API functionality and validating compliance with technical open banking standards, such as the Berlin Group’s NextGenPSD2, OBUK and STET’s API standards.
- 2. Security testing:** Carrying out a risk analysis to determine the main threats and vulnerabilities to the system and which payment service providers are vulnerable.
- 3. Sandbox:** Simulating the connection to a real bank via an open banking API during the integration phase.
- 4. Performance testing:** Exhaustive regression testing to ensure all portions of the software are operating correctly as new third-party apps are integrated into banking apps.
- 5. Functional & Security testing:** Reviewing multi form factor ‘Strong Customer Authentication’ solutions.

## WILL CHANNELS CHANGE?

Finally, what could be the impact of Open APIs on existing bank channels? Channels are a major driver of digital transformation. Sunita Handa sees API-based banking co-existing with legacy channels for a fairly long time. She points out that a consumer migrates to a new channel only when he/she sees a clear value addition there. Although



**Angaj Bhandari avers that banks should welcome fintechs into the e-banking channel without compromising data & user experience integrity**

consumers’ demand for transparency and change is the main driver pushing this change in the consumer interface side, the impact on existing channels is perceived to be slow and steady.

Munish Mittal of HDFC Bank says there will be newer channels in addition to the existing channels like branches, website, mobile apps, relationship manager, etc. “For example, a bank can now reach customers using WhatsApp and Facebook messengers using APIs. In Google’s search engine, if a customer is searching for personal loan, an HDFC loan offer can pop-up. This is an extension of the existing channel. In fact, the bank is wherever the customer is on Netflix, MakeMyTrip, BookMyShow, etc, as long as we can enable the customer to make a payment using any device and anywhere in cyberspace,” he elaborates.

He also adds that corporate customers use ERP systems with which they are comfortable. “Those systems can become bank channels. We were probably the first to do host-to-host connectivity,” he commented.

Deepak Sharma says open banking starts with creating an Open API environment that allows systems to connect to the bank’s internal portfolio of resources. At the basic level, says he, private and proprietary APIs will be tightly controlled for access to the core platforms processing general ledgers, transaction systems and so forth. There are also internal business APIs accessible by product managers within the institution that they can use to compose new offerings by connecting microservice functionality.

He believes that a published set of partner APIs may be used by strategic partners that the institution wants to use for productivity,

## Coordination among Banks

Ideally, who should coordinate the API roadmap among Indian banks – RBI or IBA or some other body? Deepak Sharma says for APIs which are governed by regulations (for example, account aggregation and sharing of customer data), is better to be governed by RBI. For remaining APIs, the roadmap can be decided by the bank covered based on the market segment and risks. This would encourage healthy competition and faster rollout of innovative API-based services. Sunita Handa points out that RBI is looking to its experience and regulatory outlook on banking matters, while Lalit Mohan says IDRBT has started work in collaboration with banks on API standardization, security and governance. It is expected to provide guidelines and best practices to banks, fintechs and other stakeholders.

He also shares another perspective: “While APIs sound like a technology innovation, business teams are expected to be equally involved and see this as a new opportunity for greater outreach and value creation.”

While APIs will likely provide the most secure and effective solution for access to accounts, standardizing and harmonizing the access to accounts will provide open and equal access for all TPPs. Angaj Bhandari lists 3 must-have deliverables for an Open API standard body:

- ◆ Developing technical standards and specifications for Open API
- ◆ Governing adherence to relevant API, Strong Customer Authentication and Secure Channel standards.
- ◆ Providing security guidelines for API, Strong

Customer Authentication and Secure Channel implementations.

Munish Mittal sees it is a collaborative responsibility of RBI, IBA, NPCI, IDRBT, policy bodies like Niti Aayog and banks themselves. He says regulators are playing a proactive role and banks should be able to see value proposition of the regulators and put up the merits and de-merits for debate for the larger interest of the consumer and country and consensus should be arrived at. “Also there is a role for PFRDA, NSDL, AMFI, SWIFT, Ripple, etc. All major concerned parties have to collaborate. Even NIBM can play a role. So could IIMs and IITs. They are playing a consultative role by being on RBI committees. Regulators should be active.

It is a big change for the regulator to be proactive,” says he.

HR functions, and so on. And finally, there may be a set of public APIs that are open to 3rd-party providers (TPPs) to access a more limited set of functionalities and data. “As TPPs begin gaining access to the institution’s platforms through the APIs, and as the institution itself begins to share customer data outside its own walls, robust governance, security and privacy policies and practices must be put in place to control and audit the new



**Nikhil Kumar suggests no one size fits all as the world is rapidly changing, recommends an active-active approach**

connected environment. The 4 key areas of data and security access that must be addressed are (i) data quality (ii) authentication (iii) customer consent (iv) data governance and (v) analytics.”

Lalit Mohan predicts that the existing digital channels would become more agile and will be tested for scalability and extensibility. He expects banks to do due diligence for relevant APIs and integrate with fintechs and have first mover advantage. Banks will innovate and compete with fintechs to ensure customer experience is sustained and customer stickiness is maintained.

Nikhil Kumar, however, emphasizes that nothing is bigger than what UPI has done for payments in India. It has managed to enable 100 million plus customers to get on to mobile banking in no time. With the account aggregator initiative kicking, India is also looking to lead the data race and not just payments!

**KEY TAKEAWAYS**

Undoubtedly, the banks of the future will be guided by digital transformation and new technology. As customers adopt digital



**Lalit Mohan reveals that IDRBT is reviewing existing standards & guidelines to validate their applicability to APIs**

activities already taking off across Europe, the Middle East and Asia, it seems even those that fall outside of regulatory mandates are looking to open banking as an inevitable, exciting and more valuable future.

Multiple standardization and interoperability efforts by RBI have propelled the modernization and expansion of India’s banking sector. And, in this regard, India’s systems are in a strong position to continue its transformation. It’s clear that continued standardization combined with the adoption of open APIs is the next step for the nation, with defining a more seamless and secure API infrastructure an urgent need to realize this vision.

It remains unclear exactly which path this will take: fully proactive, active or reactive, but as Angaj Bhandari at FIME noted, a combination is perhaps most likely and best suited. Learning from Europe’s open banking trailblazers will take the market far, but only when considered in parallel with the unique attributes of India will open banking APIs realize their full potential.

manoj@bankingfrontiers.com

products and services across various aspects of their daily life, they increasingly expect the same seamless experience from their banking too. Until recently, customer financial data was centrally held within financial institutions, but this power is shifting. In the age of open banking, this focus has shifted to the consumer, and how more valuable services can be delivered.

With an array of open banking

**FIME’s Open API testing platform TrustAPI**

**W**ith TrustAPI, banks and third-party providers (TPPs) can now quickly verify APIs against PSD2-compliant standards, fast-tracking the launch of open banking services. The platform:

- ◆ Simplifies functional API regression testing
- ◆ Enables the creation of customized API test plans and case scenarios
- ◆ Delivers quick and easy-to-assess reports and test coverage (visuals & reports)
- ◆ Provides a user-friendly interface that requires no advanced knowledge of test scripting

languages

- ◆ Constantly adding new Open API standards, including Open Banking UK, NextGenPSD2 Access to Account, STET, etc.)

TrustAPI has been built to comply with multiple API standards. Its USP is that it is the first tool of its kind to automate API testing. Most existing API testing platforms are manual or use a script. FIME’s approach is to write tailored, customizable test plans that are defined to test against the functionality and features the banks

and fintechs want to implement.

“We’re the first to totally automate the testing of APIs. TrustAPI enables the creation of multiple, customizable test plans - it is unique. The tool has been designed to test against today’s existing API protocols, with the flexibility to add other API standards. Banks get full control – with a modifiable test plan and quick and easy-to-assess test coverage, they can edit and update their test plans as requirements change,” explains Angaj Bhandari in simple terms.