Security challenges in the evolving fintech landscape

Growth and impact of fintech

Fintech is a portmanteau word combining financial and technology. It represents the next phase of the evolution of financial services, wherein technology and technology-focussed start-ups and new market entrants innovate products and services currently provided by the traditional financial services industry.[1] Fintech has two primary components: technology-driven innovation in the traditional banking sector and the emergence of new delivery models to provide financial services.

Fintech has disrupted all aspects of the industry—banking and capital markets, asset and wealth management, insurance, and funds transfer and payments. The lending and payments sector is anticipated to experience a high level of disruption with the emergence of online platforms that facilitate lending and borrowing between individuals and businesses, peer-to-peer personal loans, and innovative models for lending to small and medium enterprises.

1. http://www.pwc.com/gx/en/industries/financial-services/fintech-survey/report.html

Connected buyers and sellers

Payments

Non-traditional payment scheme
Mobile money
P2P FX
Cryptocurrency

Cashless world
Integrated billing
Mobile payments

Insurance

Disaggregating forces
Digital distribution
Autonomous vehicle
Strong economy

Connected world
Wearable computers
Internet of things
Advanced sensors

Deposits and lending

Alternative lending platforms
P2P lending

Shifting customer preferences
Third-party API
Mobile 3.0
Virtual technologies

Capital raising

Alternative capital-raising platforms
Alternative due diligence
Crowdfunding
Virtual exchanges and smart contacts

Investment management and market provisioning

Next-gen process externalisation
Capability sharing
Open source IT
Blockchain
Big data
Advanced algorithms
Machine learning
Cloud computing

Empowered investors
Retail algorithmic trading
Social trading
Automated advice and management

Areas disrupted by fintech
Source: PwC analysis

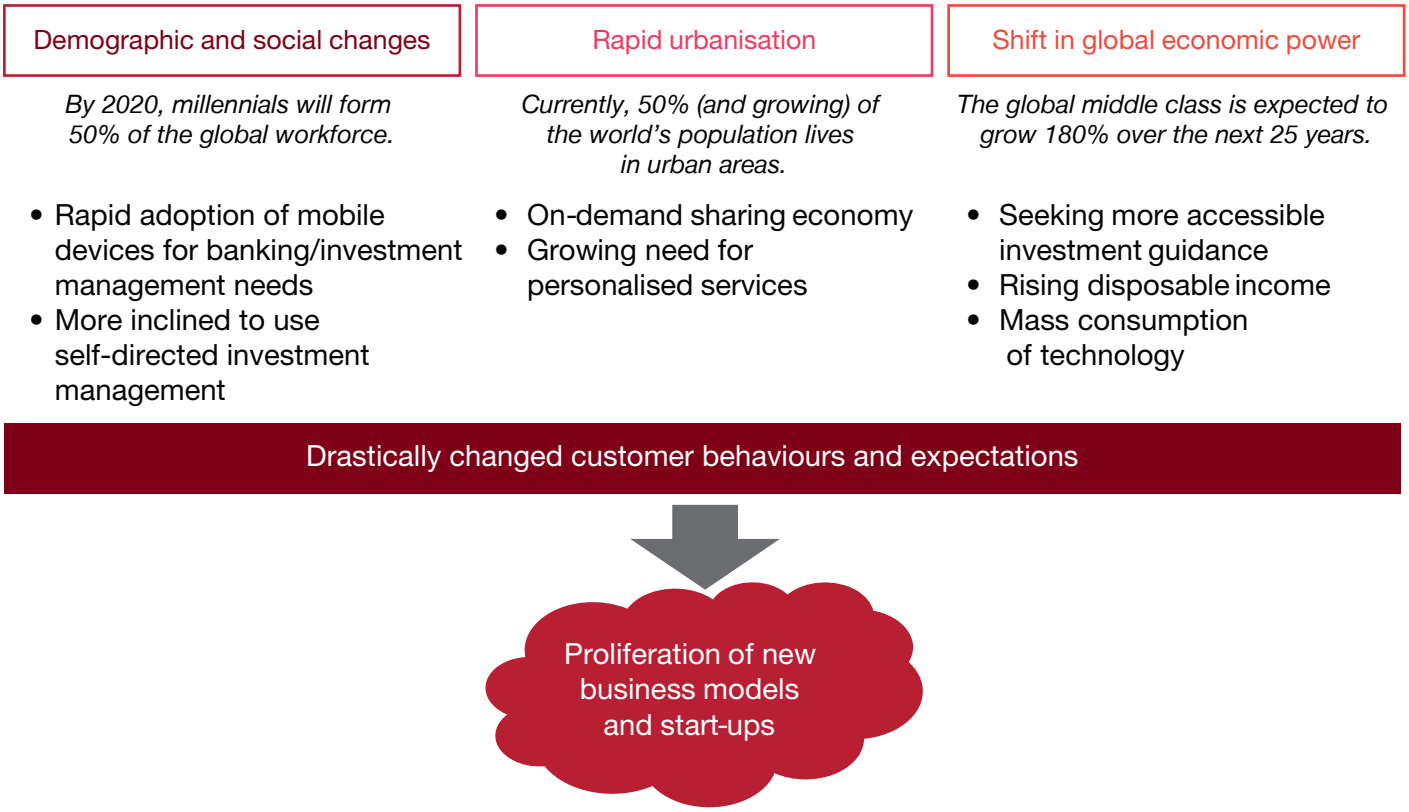
pwc

www.pwc.in

Fintech has not only led to the growth of start-ups but has also begun disrupting the way traditional banks offer services to customers, as banks look to integrate multiple digital channels into an omnichannel customer experience. The increasing adoption of big data, development of better methods to identify and quantify risk, algorithm-based investments, and platforms for users to analyse and optimise their portfolios have revolutionised the asset and wealth management industry.

Blockchain technology has also disrupted fintech through the development of cryptocurrencies such as bitcoin, which are revolutionising payments and money transfers through the elimination of middlemen and development of 'smart' contracts.

Global trends, such as the decreasing age of the average workplace and increasing urbanisation, digitisation and disposable incomes, have contributed to the evolution of the fintech industry.



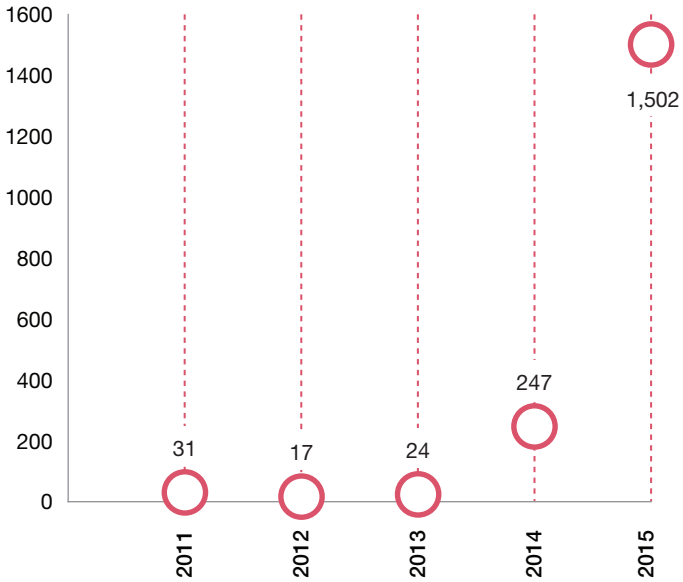
Global megatrends impacting financial services
Source: PwC analysis

Although the industry is still at a nascent stage in India, many start-ups have already emerged—e-wallets such as Paytm and MobiKwik; Citrus, PayUmoney and FreeCharge in payments; and Policybazaar, Coverfox and others in insurance.

India is poised to ride the fintech wave, with over half its population between the age of 10 and 40[2] and an Internet subscription base (wired and wireless) of 24%, which increased at the rate of 20% between 2014–15.[3] The average household income is also on the rise, creating a demand for banking services that is further supported by the increasing penetration of smartphones.

Over the last couple of years, fintech investment has grown rapidly—almost six times in India.

2. Census 2011
3. Telecom Regulations Authority of India, The Indian Telecom Services Performance Indicators



Investments in VC-backed Indian fintech companies (million USD)
Source: https://www.bnymellon.com/_global-assets/pdf/our-thinking/innovation-in-payments-the-future-is-fintech.pdf

While fintech has grown rapidly and offers several advantages such as substantial reduction in costs, improved customer retention and differentiation of financial institutions from the competition, it presents its fair share of threats and uncertainties. Security and privacy are top threats to the rise of fintech. The subsequent sections of the paper discuss the emerging security and privacy risks in the fintech space.

Security and privacy challenges faced by fintech companies

The financial services sector handles sensitive information about individuals and enterprises. With the emergence of fintech, more data is now available in digital formats, which makes it easier to analyse and generate insights but also makes the data more susceptible to security breaches. According to PwC's Global FinTech Survey 2016,[4] almost 56% of the respondents identified information security and privacy as threats to the rise of fintech.

As more services go online, **data ubiquity**, and consequently data security, are proving to be a major challenge for fintech. As the penetration of online and phone banking services increases, enterprises are able to gather tremendous amounts of data about customers and visitors, which is analysed to generate insights

4. http://www.pwc.com/gx/en/industries/financial-services/fintech-survey/report.html

into customer buying patterns and acquisition and retention strategies. Some of this data also includes personally identifiable information and financial and health information. Protecting this data and providing it to customers and third parties in a secure manner and when required are a challenge for the industry.

Partnerships between traditional financial institutions and contemporary businesses have helped consumers get better products at better prices and have improved access to existing products and services—**seamless data sharing** forms the backbone of such partnerships. Moving forward, organisations will need to enforce stronger mechanisms for seeking consumer consent for data sharing, and reuse and implement technologies and processes for data life cycle management in order to ensure data is not misused or exploited in the grey market. Further, the challenge of establishing **data ownership** must be overcome through a combination of technical and legal measures. One way in which companies could overcome the potential threat of litigation (over leak or misuse of data) is by enforcing mechanisms which securely dispose of customer data once he/she de-subscribes from the use of fintech services. Further, **managing customer access** to solutions and services becomes increasingly perplexing. Cyber security concepts like data labelling, selective data sharing and identity-aware data sharing hold possible solutions to this problem.

Managing the digital identities of individuals and enterprises is a major challenge for fintech companies as organisations aim to provide an integrated omnichannel experience to users by extending a host of banking, wealth management and payment services in a seamless fashion. Increasingly, devices such as mobile phones equipped with biometric sensors (e.g. fingerprint scanners) are being used to provide authentication and authorisation services. The use of mobile phones as authentication devices, through the use of biometrics, one-time passwords (OTPs) and code-generating apps (e.g. Google Authenticator), has reduced the reliance on conventional authentication mechanisms such as passwords and PINs. While digital identities have become safer at one level, given the ubiquitous nature of their use in the evolving fintech world, cloning of these identities can lead to amplified risks. Adaptive authentication or risk-based authentication, which analyses user behaviour in making decisions on granting access could be a countermeasure to address the risk of misuse of digital identities.

Interfacing systems through application programming interfaces (APIs) that communicate with multiple enterprise applications has made it possible to share data seamlessly, but this has also created prospects for malware propagation. **Cross-platform malware contamination** is an imminent threat with the increased integration of systems in the financial services sector. As proof-of-concept viruses have suggested in the past,[5] it is possible to create malware that can infect and propagate from one platform to another. Combating such a threat requires not only the adoption of the latest technology but also a re-examination of conventional security architectures.

Embedding security as part of the initial design phase by identifying business use cases and developing threat models and associated controls is one possible method to ensure the development of secure technologies. This would be important given the start-up nature of the fintech world and hence the risk of **insecure coding practices** being adopted in pockets.

5. https://www.symantec.com/security_response/writeup.jsp?docid=2001-032719-0644-99

Conclusion

As the industry continues to evolve and leverages the increasing computing power available to consumers through smartphones and laptops, cyber security specialists are revisiting conventional security models. Security architectures at organisations need to be redesigned while taking into account these trends, as there are implications for fintech as well as other industries and device manufacturers. From the consumer's point of view, security is an integral part of fintech solutions, the onus for which lies with the provider. Moving forward, security and data privacy are going to play a key role in winning consumer confidence and catalysing the adoption of fintech. The time for action is now.

About the authors

This point of view has been co-authored by Siddharth Vishwanath, Amol Bhat and Abhishek Chhonkar. Siddharth Vishwanath is a Partner and leads the Financial Services focus for the Cyber Security practice. Amol Bhat is a Director with the Cyber Security practice and works with several banks.

To have a deeper conversation, please contact:

Sivarama Krishnan
Leader,Cyber Security
+91 (124) 626 6707
Email: sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Partner, Cyber Security
+91 (22) 66691559
Email: siddharth.vishwanath@in.pwc.com

Manu Dwivedi
Partner, Cyber Security
+91 (0) 80 4079 7027
Email: manu.dwivedi@in.pwc.com

Sundareshwar Krishnamurthy
Partner, Cyber Security
+91 (22) 6119 8171
Email: sundareshwar.krishnamurthy@in.pwc.com

Hemant Arora
Executive Director, Cyber Security
+91 (124) 626 6717
Email: hemant.arora@in.pwc.com

PVS Murthy
Executive Director, Cyber Security
+91 (22) 66691214
Email: pvs.murthy@in.pwc.com

Notes

Notes

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

pwc.in

KS/July2016-6735