RSA

WHITE PAPER

Banking's Digital Transformation

The confident pursuit of opportunity in the face of rising risk

Executive summary

The age of digital transformation has arrived, revolutionizing the financial services industry with new ways of doing business anytime, anywhere. With a growing array of digital banking channels available, customers seemingly have infinite possibilities for conducting financial business. At the same time, this expansion of banking channels increases the risk of fraud. The latter is a prospect that weighs heavily on financial institutions (FIs); according to the business management consulting firm McKinsey & Company, 70 percent of banks have digital risk "prominently on their radar."[1]

RSA believes the critical question is whether FIs will confidently pursue the opportunities digital transformation presents, or focus instead on the risk it creates. This paper describes a third alternative in which opportunity and risk are not either-or choices, but rather two sides of the same coin. From that perspective, the ability to manage the risk of fraud can become what frees organizations to embrace business opportunity. To put it simply, digital risk management can be a way for banks to win, not just a way to avoid losing.

> *"Our customers don't benchmark us against banks. They benchmark us against Uber and Amazon."*
>
> Hari Gopalkrishnan, CIO
> **Bank of America Merrill Lynch**

Winning in the digital era means rising to the challenge of meeting an entirely new set of customer expectations. As the CIO at one of the world's largest FIs puts it, "Our customers don't benchmark us against banks. They benchmark us against Uber and Amazon."[2] To succeed, FIs must manage digital risk so that it doesn't stand in the way of digital opportunity. In the pages that follow, we will explore new areas of opportunity and risk that are the result of digital transformation in the financial services industry, including:

1. FinTech
2. The API Economy
3. 3D Secure 2.0
4. Mobile
5. The Internet of Things

Just as importantly (if not even more so), we will look at specific enabling technologies that can help create a hospitable environment for growth and opportunity by keeping risk at bay.

Top 5 areas of digital opportunity for today's FI

1. FinTech

In every financial services space from payments to insurance, FinTech—short for financial technology—has been exerting competitive pressure on FIs by offering innovative digital alternatives to traditional offerings. Digital wallets, cryptocurrency, blockchain and other FinTech phenomena are redefining banking and financial services in a multitude of ways, putting traditional FIs at risk of losing business to them. But in this, as in the larger picture of digital transformation, on the other side of risk lies opportunity.

- **The opportunity** for FIs is to beat FinTech at its own game, by innovating and providing more of the kinds of digital services FinTech companies offer. This move toward FinTech among traditional financial services providers has already begun. JP Morgan, for example, has invested $600 million in "emerging fintech solutions," according to a recent annual report.[3] And Reuters reports that Wells Fargo has started an artificial intelligence (AI) initiative to provide more personalized customer services and strengthen its digital offerings.[4] (The data analysts at CB Insights have mapped out where these and other top U.S. banks are investing in FinTech.[5])
- **The risk** is that by embracing FinTech to offer more services and create more channels for customers to conduct financial business, FIs create more avenues for fraud. The very diversification that affords them more opportunities to deliver services to customers also creates new openings for fraudsters. As a result, FIs will find themselves in the position of having to manage fraud risk on a greater scale than ever.

2. The API economy

Developing technology to compete with FinTechs, or acquiring large stakes in FinTech companies, may make sense for large enterprises like JP Morgan and Wells Fargo. But for smaller organizations with fewer resources, another option is to take the "if you can't beat 'em, join 'em" approach and partner with third-party application providers to deliver innovative offerings. A growing open API economy provides the technology foundation to support this.

- **The opportunity** for FIs in the API economy is to be able to offer customers capabilities such as being able to link their accounts with other services (utility payments, for example) without the FI having to build out a complex technology infrastructure to support the new capability. In some cases, this may be more than an opportunity; it may be an obligation. For example, the European Union's (EU's) Payment Services Directive II (PSD2)[6] requires banks doing business in the EU to open access to their systems to payment services and data aggregators.
- **The risk** is that the growing use of third parties can cause a security weakness, with open APIs potentially opening a new attack vector. As the U.S. Office of the Comptroller of the Currency (OCC) warns, increased use of third-party service providers, particularly for critical operations such as merchant card

processing, "can create concentrated points of failure resulting in systemic risk to the financial services sector."[7]

3. 3D Secure 2.0

FIs in the business of issuing credit cards have started or are planning to embark on the journey to adopting 3D Secure (3DS) 2.0,[8] the newest version of the 3DS security protocol for online credit and debit card transactions. Unlike the previous version of the protocol, 3DS 2.0 supports a more frictionless shopping experience through the use of risk-based authentication to identify potentially fraudulent transactions.

- **The opportunity** with 3DS 2.0 lies in its adoption of consumer-friendly features such as the elimination of enrollment pop-ups, full integration into the shopping experience and faster authentication. By reducing the annoyance factor, these changes have the potential to reduce the current high rate of cart abandonment online—thus leading to more completed transactions and more revenue for issuing banks.
- **The risk** is similar to that posed by FI adoption of FinTech, with more transactions being associated with more risk of fraud. Even though authentication improvements in 3DS 2.0 are expressly designed to improve security, its adoption by merchants can be expected to bring dramatic growth in transaction volume, which inherently means greater fraud risk.

4. Mobile banking

Since the first mobile banking service was announced nearly 20 years ago, mobile banking has become a staple of FI consumer offerings. Recent data from Federal Reserve surveys shows that 89 percent of FIs already offer mobile banking services, and 97 percent expect to be doing so by the end of 2018.[9] And according to a recent survey by Bankrate, 63 percent of smartphone users have at least one banking app (and more than half have at least one full-service banking app).[10]

- **The opportunity** with mobile banking is it offers yet another channel for FIs to provide new services to their customers while meeting their demands for secure, convenient account access. Mobile banking has become the predominant and preferred channel for consumers to interact with FIs. In 2017, 55 percent of transactions originated from a mobile app or browser, and in the last three years, transactions from mobile banking apps have increased more than 200 percent.[11]
- **The risk** with mobile banking is clear, given that 64 percent of overall fraud originates from mobile devices.[11] As mobile transactions continue to grow, FIs will need to address the risk of mobile banking fraud if they want to avoid financial losses and loss of customer confidence.

of overall fraud originates from a mobile device

Source: RSA

5. The Internet of Things (IOT)

You're not likely to find banking leading the list of today's top IoT applications,[12] but the prospects for IoT-based financial transactions look good nevertheless—particularly in the payments segment. Citing a survey of global banking and insurance executives, the Financial Brand reports that 59 percent expect wearables

to become a common payment mechanism within two years.[13]

- **The opportunity** for FIs in the payments segment is multifaceted, as humannot-present transactions become more prominent in the next evolution of shopping convenience. RSA expects IoT devices to ultimately interact directly with payment systems in a variety of areas to enable personalized services, make automatic payments, facilitate usage-based fees and much more.
- **The risk** of IoT in payments is that when a human is not present for a transaction, there's no way to directly confirm the person's identity. There's literally no one there to answer qualifying questions that establish that the transaction is authentic and intentional. Moreover, there may be multiple entities buying on the consumer's behalf, and they may not all be well-secured. FIs in the IoT economy will have to establish ways to determine that a transaction has been authorized and to detect fraud by entities.

Enabling technologies: Embracing opportunity by managing risk

In the areas of digital opportunity described in this paper, security technology has an essential role to play in enabling FIs to pursue the opportunities without putting themselves or their customers at risk for fraud. The following types of security capabilities will be key to preventing and detecting fraud in ways that are frictionless for customers.

Next-generation authentication: Stop fraud—not customers

As the array of digital banking channels grows, so does the need for risk-based authentication, which gives FIs the ability to confirm in more than one way that they are dealing with legitimate customers attempting legitimate transactions.

There's just one problem: If FIs ask every customer to provide additional authentication upon every transaction attempt, the process will become cumbersome for the customer. Since one of the main reasons for offering digital banking options like mobile banking or 3DS 2.0-based payments is to make things faster, easier and more convenient for customers, one could argue that the imposition somewhat defeats the purpose of having digital banking capabilities in the first place.

The solution lies in risk-based authentication, sometimes referred to as adaptive authentication, or the ability to assess fraud risk based on contextual information such as device identification, IP address, user behavior and fraud intelligence. Risk-based authentication leverages various machine-learning models that enable new fraud patterns to be learned quickly by the risk engine, and it accepts additions of new predictors such as data from other channels or cybersecurity tools. The self-learning capability of risk-based authentication is crucial to keep up with the speed at which cybercrime evolves and, more importantly, to minimize false positives and customer friction.

Its nonintrusive nature, flexibility and ability to manage fraud risk across multiple channels makes risk-based authentication an ideal solution for FIs looking to deploy strong security to large customer populations. Fraud detection rates of 95 percent

Risk-based authentication rate of fraud detection at a 5% customer challenge rate

Source: RSA

can be achieved with minimal customer intervention, whereby the risk engine will only recommend another authentication factor, such as biometrics or SMS, when the probability of fraud is high.[11] This ability is a hallmark of standards such as 3DS 2.0, where a positive customer experience is promoted as the central theme.

Figure 1: Risk-Based authentication weighs numerous risk indicators to determine the probability of fraud with high accuracy

Secure omnichannel architecture: Toward a more efficient, effective whole

A critical consequence of the proliferation of digital banking channels is the problem of having multiple channels that operate independently of each other. Back when "multiple channels" at most meant a branch bank and an ATM network, this wasn't so much an issue. But today's banking channels are also likely to include online banking, chat support, mobile banking, call center and third-party services, with more channels likely on the way. In this environment, independent operations are both ineffective and unsustainable.

What's needed is an omnichannel architecture in which assets are centralized and shared, so that operations can be carried out as a whole rather than an array of discrete parts. This eliminates the need to build and maintain a separate infrastructure (including separate point solutions for fraud detection and

Case study: Leveraging data from the phone channel, one large U.S. financial institution was able to enhance risk assessments across its web and mobile channels, increasing fraud detection rates by 2.2 percent and saving an additional $500,000 in potential fraud losses.

Source: RSA

prevention) for every channel. Instead, all channels—both online and offline—can share knowledge and awareness of the customers' interaction. This will lead to more streamlined operations, a more secure banking environment and a smoother customer experience.

Within the omnichannel architecture, technologies such as deep entity profiling and machine learning specifically help improve fraud detection. Deep entity profiling involves gathering information from across multiple consumer channels and touchpoints and analyzing it to assess whether a given activity is likely to be fraudulent. Machine learning works by detecting patterns and anomalies in activity that suggests potential wrongdoing—for example, when someone uses a computer for a banking-related task in a way that departs from their typical behavior.

Automated fraud case management: Keeping pace with growth

As the sheer volume of digital transactions increases, the growth in fraud means the burden on analysts who review potential fraud cases will grow, along with the likelihood that they will be unable to keep up.

The answer to addressing this problem successfully lies in using automation to prioritize case alerts for analysts based on risk and business impact, so they can direct limited resources to cases that pose the most risk. But that may not be enough to compensate for increased transaction volumes. Automated case handling based on advanced machine-learning capabilities will be needed to make it possible to accurately detect fraud without even engaging analysts.

By increasingly relying on technology to detect and stop fraud, FIs can keep pace with the growth in fraud that will likely accompany the growth in transactions ushered in by the digital banking era. That's a necessary goal that may well be otherwise unattainable, given that transactions are likely to grow far more rapidly than the resources FIs have to respond to an expanded caseload.

Conclusion

Digital transformation presents FIs with unprecedented opportunities to win new customers who are eager to enjoy more of the ease and convenience that are the hallmarks of the digital experience. Those FIs that are fully equipped to manage digital risk are the ones that will find themselves prepared to freely embrace these opportunities. By adopting next-generation authentication, building secure omnichannel architectures and using automation to detect and stop fraud, they can position themselves perfectly to make the most of the opportunities banking's digital transformation offers.

Learn more about RSA fraud prevention solutions at **rsa.com/fraudprevention.**

[1]McKinsey & Company, **"The future of risk management in the digital era,"** December 2017

[2] Susan Nunziata, **"Bank of America's Digital Transformation: Where IT Fits In,"** InformationWeek, October 27, 2016

[3] JPMorgan, **2016 Annual Report**

[4] Anna Irrera, **"Wells Fargo sets up artificial intelligence team in tech push,"** Reuters, February 10, 2017

[5] CB Insights, **"Where Top US Banks Are Betting On Fintech,"** February 1, 2018

[6] European Commission, **Payment services (PSD 2)—Directive (EU) 2015/2366**

[7] National Risk Committee, U.S. Office of the Comptroller of the Currency, **Semiannual Risk Perspective,** Fall 2017

[8] Sadra Boutorabi, **"3D Secure 2.0: What it means to Card Issuers,"** Financial IT, May 9, 2017

[9] Marianne Crowe et al., **"Mobile Banking and Payment Practices of U.S. Financial Institutions,"** Federal Reserve Bank of Boston, December 2017

[10] Robert Barba, **63% of smartphone users have at least one financial app,** Bankrate, February 8, 2018

[11] RSA Adaptive Authentication Data Science Analysis, February 2018

[12] Padraig Scully, **"The Top 10 IoT Segments in 2018—based on 1,600 real IoT projects,"** IoT Analytics, February 22, 2018

[13] Jim Marous, **"Should Banking Build an Internet of Things (IoT) Strategy?"** The Financial Brand, January 16, 2017

Content and liability disclaimer

About RSA

RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to **rsa.com**.