VIEWPOINT

December 2017

8 Mill and Main Place, Suite 150 | Maynard, MA 01754
www.mercatoradvisorygroup.com |phone 1-781-419-1700 |email: info@mercatoradvisorygroup.com

2018 Outlook: Emerging Technologies

Continue investing in technology as outlined in 2017 with minor refinements.

In last year's Outlook for the coming year, Mercator Advisory Group' Emerging Technologies Advisory Service argued that payment solution providers should immediately invest in tokenization, machine learning, and application programming interfaces (APIs). This year we argue for more of the same. Of the three, machine learning has become entangled in major hype, yet it has demonstrated that it can be applied very broadly, not just applied to Big Data and fraud, and so it demands even greater attention. The networks continue to deliver new tokenized services to market that require new tactics and will further enable e-commerce. Banks, networks, and processors offer APIs through developer websites.

by Tim Sloane,
Vice President, Payments Innovation, and
Director, Emerging Technologies Advisory Service

Artificial Intelligence (AI) and Machine Learning (ML) Continue to Be Major Drivers of Innovation

Artificial intelligence (AI) and machine learning officially became buzzwords at Money 2020. Although they are not well incorporated into most products exhibited at that show, the buzz is merited. Machine learning technology has dramatically changed both payments and consumer behavior. Consumers are rapidly adopting use of natural language interfaces to interact with their surroundings, and many are using voice-assisted interfaces to make purchases.[i] Machine learning has become the go-to technology for authentication (through biometrics) and for detecting fraud and avoiding false positives.

The misconception is that AI is only associated with big data and fraud detection, when in fact it will have an impact on a much broader range of business processes. AI is the basis for new user interaction channels enabled by natural language processing, bots that can answer users' questions, and process automation and software development that learns through observation (as can be seen in a short video at the Fortune website demonstrating the Kindred Sort robot in operation at a Gap warehouse[ii]). Implementing such AI solutions can lower costs associated with onboarding customers, supporting customers, and in other areas where multiple people perform rote tasks.

Although this technology has typically been adopted at financial institutions as a tool associated with big data, FIs need to view AI and machine learning much more broadly in 2018 and make additional investments in their implementation. Within the organization, machine learning not only can perform menial tasks more effectively and efficiently than humans but also can speed up processes for customers and prospects and streamline operations. Consider, for example, typical "day two" clearing operations at banks, which include validating items from the ATM, mobile devices, online deposits, back-counter images, and incoming electronic files from other financial institutions and the Federal Reserve. Many of these clearing decisions can be automated utilizing machine learning to process low-risk transactions in the same day if not close to real time.

Another example of application of machine learning is for contract management at law firms. Solutions based on machine learning feedback can review laws and judicial proceedings to enable faster, more precise searches. They can also be used to review standard contracts and flag missing or problematic clauses. This makes the legal review of repetitive contracts (such as those associated with third-party management of payment partners) much easier and less time consuming.

APIs and Cloud Computing Are Finding Multiple Use Cases

Visa has introduced application programming interfaces (APIs) through the Visa Developer Center website that enable access to Visa network services. It has also introduced a new business unit called Visa ID Intelligence that offers financial institutions a full range of identity solutions via the same portal. Visa ID Intelligence is an effort to create a Visa-controlled and -managed marketplace for identity management solutions. Visa validates the suppliers

8 Mill and Main Place, Suite 150
Maynard, MA 01754
info@mercatoradvisorygroup.com

and directly bills the financial institutions that utilize the services, making this a one-stop-shopping experience for institutions looking to offer advanced identity solutions. While it is unclear if this expansion into a full-blown identity supplier will be broadly adopted by financial institutions, this is clearly a new market that other branded networks will want to watch closely, as will Mercator Advisory Group.

Financial institutions from ANZ, BBVA, Capital One, Citi, PNC, to Wells Fargo have all worked to create developer portals to some extent and made efforts to support open banking, an approach that is being driven by European Union banking regulations and the United Kingdom's Open Banking Working Group (OBWG), established in late 2015. OBWG promotes the Open Banking Standard, which identifies APIs that provide access to bank data.[iii] U.S.-based financial institutions recognize that a similar standard is needed in the United States. Most current APIs offer limited functionality, restricting access for example so an APIs can only be used to read customers' account and transaction history and perhaps branch and ATM locations rather than to enable payments to be made.

While the Open Banking Standard approach may support the Open Banking model, it doesn't enable much innovation by financial technology (fintech) companies, which may need to be able to update accounts, originate loans, as well as create and modify business accounts and card account data and notifications.

This limited access reflects the fact that implementing APIs is difficult. While conceptually APIs are easy to understand, highly capable implementations are much harder to achieve since a good API demands a specific use case. The use should be tied to a business model that can, at minimum, cover the costs of maintaining the API platform or otherwise further a strategic objective. These costs aren't small when the implementation is done right. Developing a working sandbox where developers can test new software, documenting the APIs, managing back-end performance, assigning resources to security, and providing debugging resources are all expensive propositions.

The challenge is to identify use cases that make sense for a financial institution, which might be focused on managing account access according to Open Banking principles or focused on commercial accounts that have the wherewithal to integrate directly to the bank. Regardless where the FI's effort starts, it will likely quickly become apparent that its internal systems were not designed to be accessed by outside applications and some re-engineering will be required. The good news for smaller banks that utilize processors such as D3, First Data, FIS, or i2c is that those companies have developed APIs to their core systems that can help. FIS recently launched its own API-based developer portal, FIS Code Connect,[iv] which should be usable by both FIS clients and third-parties that want to integrate to FIS products and services.

Tokenization and Digital Payments Continue to Evolve

E-commerce and m-commerce will continue to grow much faster than traditional commerce and new technologies (including more internet of things, or IoT). New competitors and new potential partners will continue to appear at a breathtaking rate. Tokenization as a means of safeguarding actual account numbers by replacing them in a device with proprietary numbers (a "token") that can change depending on context will prove critical to participation in these new markets. A token can take various forms. It can take the form of a number that looks like

a card number but can be changed if stolen without requiring the reissuance of a card. Other forms that a token can take are as a bar code for display on a mobile device, an e-mail address, or an encrypted account number that can only be decrypted with the proper pointer that associates the token to the hidden data. Tokens will be used to enable everything from payments embedded in mobile apps and browsers to ATM withdrawals arranged through mobile apps, chatbots, Amazon Alexa, Apple Siri, Microsoft Cortana, or Google Assistant.

3-D Secure 2.0 (3DS2) is a successor to the orginal 3-D Secure standard by Visa and Mastercard for verifying e-commerce transactions. It collects more information regarding the customer and the customer's device, and may enable tokenization of a device that has the appropriate intelligence and security built in. The web browsers Google Chrome, Microsoft Edge, and most smartphones today have this capability, and Apple Safari and Firefox are expected to have it soon. First Data is piloting a Token Service Provider platform with Mastercard and expects the solution will close the loop between the token provisioned into the device and the handoff of that token at the merchant location. This approach will enable new capabilities at the point of sale (POS) and allow tightening of fraud management. Meanwhile, the World Wide Web Consortium (W3C) has been developing its own standard for securing e-commerce transactions, so the card networks will need to convince merchants and card issuers to support their standard rather than (or in addition to) the W3C one. This may be difficult, since many merchants and card issuers are already concerned about the market power that Visa and Mastercard have accumulated through their early dominance in issuer-oriented tokenization solutions. By the end of 2018 we should see if 3-D Secure 2.0 will be able to drive consolidation of e-commerce and m-commerce payments or if card-on-file and the new (W3C) payments standard will fend off Masterpass and Visa Checkout solutions. (For more detail, see the Mercator Advisory Group research report titled *Mobile Payments Platforms and Markets: How High Is Up?* released in February 2017.)

As deployment of payment credentials into more devices becomes more common, it will soon become apparent that online banking tools need to be improved greatly to support the breadth of new tokens being deployed. These new tokens can restrict usage to specific stores, specific dollar value, and date ranges. The networks and processors are beginning to address these additional capabilities and embedding these new solutions into online banking and mobile apps, which means that banks should have plans to expose these controls to their cardholders now.

The Changing Authentication Landscape Demands Attention

Recent announcements by Visa[v] and Mastercard[vi] regarding authentication and biometrics clearly indicate that biometrics will ultimately be the standard for authentication. The only two questions that remain are when and where biometric authentication will be implemented. Mercator Advisory Group already delivered its forecast for broad consumer adoption of biometrics in the research report *Biometrics: A Market Forecast for Consumer Adoption*, released in January 2017. This is not the same, however, as identifying when banks and networks will utilize that mobile authentication infrastructure for authorizing payments, because so far biometrics have been used primarily for secure access to mobile devices and apps.

Adoption of biometrics for secure payments is more difficult to predict because of the complexity of the payment value chain. Prior to broad adoption of 3-D Secure 2.0, the networks will continue to apply machine learning tools to manage fraud and will require that merchants provide additional data regarding customer transactions as input for the feedback loop or iterative learning through which those tools continuously improve. This additional information in the authorization message should reduce the frequency of a challenge that requires the consumer to pass additional authentication. Today that additional authentication is the user's online banking credentials. When banks adopt biometrics in the mobile device, that online challenge can migrate to a biometric response.

Note, however, that physical biometrics such as fingerprints and face recognition may eventually either be reinforced or dropped altogether with the introduction of behavioral biometrics, depending on the effectiveness of behavioral signals . Behavioral biometrics utilizes a broad range of signals a user generates when carrying or using a smartphone or other personal computing device. This may include voice, gait, background noise, location, typing patterns, gestural idiosyncrasies, and a wide range of additional unique signals that people generate in the normal use of their devices. In time we will learn whether these signals are sufficiently reliable to be used as an adjunct to transaction-based fraud scoring or as a total replacement for it.

Regardless of the success or failure of behavioral biometrics, any financial institution considering whether to deploy a stand-alone biometric solution in the branch or ATM should reconsider that decision, since the trajectory is clear that the mobile device will ultimately contain the new authentication mechanism, which will lower implementation costs and eliminate the honeypot associated with storage of customer biometric information.

Monitor Two Blockchain Use Cases Carefully

Implementations of blockchain are picking up steam and should be monitored carefully. There are two key areas relevant to payments—cross-border payments and identity solutions. Of these two use cases, over 100 financial institutions are evaluating Ripple,[vii] while USAA and several credit unions are evaluating identity solutions that include Evernym[viii] and its deployment via the Sovrin Foundation.[ix]

Ripple, which has its own cryptocurrency (XRP), created a network (RippleNet) and sells blockchain software using a special protocol (Inter Ledger Protocol) as essentially a bank-to-bank transfer system for international payments. Given the technology, it becomes real time and also initiates an automated foreign exchange auction for the lowest possible currency conversion rates. Ripple provides transparency, speed, and cheaper transaction costs. Mercator Advisory Group expects adoption to increase once more regulatory clarity exists and Ripple adds more banks to the network, which currently numbers 100 participants.

Less advanced and more recently in market are identity solutions that enable consumers to control the information they release about themselves. For example, Evernym is currently involved with the U.S. Department of Homeland Security, R3, and the country of Finland (through the MyData initiative), USAA, and credit unions to deploy such a solution. The code base of Evernym was added to the Hyperledger project, and the nonprofit Sovrin Foundation has enlisted an impressive set of "stewards" to operate and manage the network.

Conclusions, with Recommendations for 2018

The battle for dominance in e-commerce and m-commerce will be well underway in 2018, and regardless of the outcome, banks need to consider how they will help their customers manage the many additional devices that are payment enabled. Machine learning has reached a level of maturity that could never have been predicted just three years ago, and its use transcends big data. The new capabilities are amazing and the cost so low it can already be described as a commodity. Organizations that failed to follow our advice last year and failed to invest in machine learning to lower costs and better engage customers will find themselves already starting to fall behind those competitors that do.

Regarding APIs, your institution should have a strategy to either deploy a development website or integrate to a platform (supplied by a processor or third party) that can add value to your products and services. These solutions need to be in market today within the European Union to comply with requirements of the Open Banking initiative, and U.S. banks should start to implement pilots in 2018 or early 2019 if they wish to better collaborate with corporate customers and fintechs.

New biometric-based authentication mechanisms should be under development in 2018. Behavioral biometrics should be deployed to monitor online banking sessions to detect criminal activity and bots. Plans should be well along regarding how the biometric capabilities built into mobile devices will be utilized to authenticate your online banking services. They should be implemented in a way that complies with standards of the FIDO Alliance (FIDO = Fast Identity Online), which requires the credentials to be stored in the consumer's mobile device. Gathering experience with the mobile security model will be important as the mobile operating system continues to be hardened and becomes ready to take over more of the authentication role at financial institutions without the institution having to deploy a large software footprint.

One last suggestion for financial institutions is: Make sure your team keeps a very sharp eye on the mobile operating system for actionable issues not related to authentication. The mobile OS has become your customer's primary entry point to every experience. Mercator Advisory Group tracks natural language interfaces as a part of machine learning, and these natural language interfaces are rapidly becoming contextually aware as noted above. Machine learning enables contextual recognition, which is already used to better understand questions asked by the user, but we expect that contextual information will also be surfaced to apps and back-end systems and your financial institution surely does not want to be the last to respond to your customers' contextual situations.

Endnotes

[i] https://www.cnbc.com/2017/12/06/amazon-alexa-customers-buy-more.html, accessed 12/14/2017
[ii] http://fortune.com/2017/10/24/gap-robots-kindred-warehouse/
[iii] https://www.abe-eba.eu/thought-leadership/open-banking-working-group/, accessed 12/14/2017
[iv] https://codeconnect.fisglobal.com/home/
[v] https://usa.visa.com/visa-everywhere/security/visa-id-intelligence.html, accessed 12/14/2017
[vi] http://investor.mastercard.com/investor-relations/investor-news/press-release-details/2017/Mastercard-Enhances-Security-of-the-Internet-of-Things-with-the-Acquisition-of-NuData-Security-Inc/default.aspx, accessed 12/14/2017

[vii] https://www.cnbc.com/2017/10/10/ripple-has-over-100-clients-as-mainstream-finance-warms-to-blockchain.html, accessed 12/14/2017

[viii] https://www.evernym.com/, access 12/14/2017

[ix] https://sovrin.org/, accessed 12/14/2017

Copyright Notice

For more information about this report, please contact:

Tim Sloane, VP, Payments Innovation, and Director, Emerging Technologies Advisory Service
tsloane@mercatoradvisorygroup.com
1-781-419-1712

Mercator Advisory Group is the leading independent research and advisory services firm exclusively focused on the payments and banking industries. We deliver a unique blend of services designed to help clients uncover the most lucrative opportunities to maximize revenue growth and contain costs.

Advisory Services. Unparalleled independent and objective analysis in research documents and advice provided by our Credit, Debit and Alternative Products, Prepaid, Customer Interaction, Commercial and Enterprise Payments, Emerging Technologies, and Global Payments practices.

Primary Data. *CustomerMonitor Survey Series* presents eight annual Insight Summary Reports based on primary data from Mercator Advisory Group's bi-annual surveys of 3,000 U.S. adult consumers to determine their behavior, use, preferences, and adoption of current and emerging payment methods and banking channels to help our clients identify and evaluate business opportunities and make critical business decisions. The Small Business service presents three annual reports based on Mercator's annual *Small Business Payments and Banking Survey.*

Consulting Services. Services enabling clients to gain actionable insights, implement more effective strategies, and accelerate go-to-market plans. Offerings include tailored project-based expertise, customized primary research, go-to-market collateral, market sizing, competitive intelligence, and payments industry training.

PaymentsJournal.com. The industry's only free, analyst-driven, online payments and banking news information portal delivering focused content, expert insights, and timely news.

For additional copies of this report or any questions, contact Mercator Advisory Group at 1-781-419-1700.