2021 Outlook: Emerging Technologies

Faster adoption of API’s, PaaS, Cloud, and other technologies is driven by the shift in consumer behavior and by investments and acquisitions of fintechs.

The pandemic has shifted consumer behavior, and as a result operations of financial institutions must also shift. Processors, networks, and financial institutions are making decisions to either add more online oriented technology partners for key functions or to fully embrace the cloud. These decisions may slow the adoption of technologies that are not central to this dilemma.

by Tim Sloane,
Vice President, Payments Innovation
The 2020 Pandemic

2020 was a difficult year for everyone worldwide. The pandemic forced financial institutions to implement emergency plans and react to gaps in those plans. Everyone involved in payments has had to respond to the new consumer behavior driving faster mobile device adoptions, perhaps five years’ worth in 2020 alone. That shift to mobile adoption impacts almost every process in the payments landscape: from onboarding, to payments, to customer service. You won’t find any of this in my 2020 Outlook: Emerging Technologies, published in November 2019.

No one could have foreseen the effects of the pandemic, but I will argue that we did identify the technologies. Last year we predicted that application programming interfaces (APIs), cloud computing, authentication, tokenization, digital payments, blockchain and cryptocurrencies would have the most impact on the payments industry in 2020. Those predictions were accurate, but did not reflect the scale and pace of adoption driven by the pandemic: the adoption continues unabated.

It is not surprising that the payments industry continues to wrestle with the impact of the pandemic. Implementing emergency procedures is not the same as addressing the shift in how consumers shop, open accounts, pay, and otherwise interact with merchants and financial institutions. While emergency plans may change operations in the branch, they can’t reimagine the way homes are re-financed or new mortgages issued. Financial institutions that once considered online and mobile-based competitors as small upstarts suddenly realized that the pandemic would drive consumers to those same online-ready businesses. The booming refinance market has required a more immediate action to move operations online. To be clear, Mercator research indicates that this shift in consumer behavior is unlikely to recede post pandemic.

So the question becomes, How quickly can these new consumer-driven requirements be addressed by financial institutions and what will be the path to adoption? In general there are three potential approaches. Businesses can find new partners that provide these new online-focused services and integrate to the core, determine that the time has come to acquire a core that implements cloud-based architectures, or wait for their existing core supplier to move to the cloud. A recent surge in the adoption of new online and cloud-based identity and document verification solutions indicates that the addition of new partners is an important adaptation to the current environment, but there have also been significant new wins announced for entirely cloud-based architectures, from cloud-based digital channel upgrades to entirely new core solutions – so both options appear to be gaining ground.

What’s in store for 2021

Financial services will continue to be shaped by the pandemic. The impact on the investment community will continue as fintechs become more aggressive and visible across more operational areas, driven in part by investors ready to capitalize on their past investments through acquisition and via special-purpose acquisition companies
(SPACs). The following are the areas where Mercator expects to see increased attention. Many are holdovers from last year, but there are several new aspects, new applications, and new technologies to watch on the horizon.

**APIs, Cloud, and Platforms Deliver Speed and Diversity**

Recent research by Mercator indicates that 17 of 47 prepaid platforms, or 37%, have made a transition to become Payments as a Service (PaaS) providers. These platforms support multiple payment types, including physical and virtual cards, faster payments and even ACH. The payment service is made available through APIs that are published on their developer web site. All 17 include a sandbox used by developers to test their payment applications.

This transition to API as a primary form of customer acquisition and retention is growing rapidly within financial institutions. Mercator estimates that more than 25% of the top 100 U.S. bank holding companies have implemented some form of API access and that another 25% are likely planning to implement an API portal. It is less clear how many of these financial institutions have taken the bold step of publishing their APIs online through a sandbox environment.

*Figure 1: APIs require significant management to operate safely and efficiently.*

*Source: Mercator Advisory Group*
Financial institutions are moving faster than one might typically expect to embrace APIs. At the same time, they are moving more rapidly than expected to support operations in the cloud, typically utilizing a hybrid cloud approach to address the shifting needs of customers while also improving ROI during the pandemic. The implementation of a service oriented architecture (also called microservices and often implemented in the Kubernetes environment) requires that every basic function be exposed as an API. These APIs are then linked together to create higher level services. This approach makes it easier to modify the application and add new capabilities. Mercator has witnessed a growing number of smaller financial institutions that are adopting this approach, sometimes implementing the entire digital channel in the cloud or even a full blown core implementation. With more financial institutions adopting these technologies, Mercator fully expects competitors will recognize the need to follow suit. These conversion efforts are likely to grow through 2026.

Even as financial institutions move to the cloud, there is the ongoing need to lower the costs associated with integrating a new class of service providers while also enabling the ability to work across them. Mercator expects API platforms to continue their steady growth as more and more financial institutions adopt new service providers and recognize the need to manage properly that connectivity. On a related front, the rapid growth of PaaS solutions represents additional partnering opportunities for financial institutions and fintechs.

**Identity and Authentication: Managing Risk While Delivering Consumer Convenience**

We have already discussed how the pandemic increases the need to improve how financial institutions, businesses and merchants onboard new customers and verify personal information via mobile devices and browsers. This is a market in which many fintechs promise to deliver solutions and several have already been acquired by the large traditional identity suppliers. Because the need to support mobile and online onboarding will continue to intensify post pandemic, digital onboarding will continue to be an urgent need. Of course there are a range of different needs and solutions that target those needs. Some meet the most stringent identity requirements but operate in a single geography, while others may be less stringent in the identification but cover more geographies. Both businesses and financial institutions will be adopting these solutions more broadly in the next several years, especially as new cloud-based identity solutions that utilize consortium data enter the market.

While acquiring digital onboarding solutions, the business would be wise to consider one additional implementation detail. Some of the new solutions operate similarly to the existing model where the authenticator is in full control and the customer must collect and deliver the information the authenticator requests. Other fintechs have entered the market with solutions that help the consumer create a digital identity that can be re-used across multiple authenticators. In fact, some of these solutions go a step further and support the principles of self-sovereign identity (SSI). Several major suppliers, including Microsoft, IBM, and Mastercard, as well as government agencies and credit unions have deployed solutions that support the SSI concepts. However, due to the pandemic, the urgent need to implement online solutions that embrace paper-based identity is likely to drive
adoption of less complex solutions and that may slow down adoption of SSI-based solutions (see Distributed and Self-Sovereign Identity-Solutions Part 1 and Part 2).

Cybersecurity

It should come as no surprise that the shift in consumer behavior to mobile and online-based transactions has generated more criminal activity related to synthetic identity fraud, phishing to extract private information from consumers, and the use of fake or stolen payment credentials in e-commerce and commercial transactions. While Europe is implementing PSD2 in an effort to reduce online payment fraud and account takeovers, the U.S. has no national implementation plan and so our response is less focused and less coordinated.

The payment networks are trying to implement variations of EMV 3D Secure in the U.S., but adoption has been slow, perhaps in part because the incentives offered merchants to adopt are insufficient. Even as the technology is brought to the U.S., it is being modified and extended in Europe with delegated authentication. This in essence takes a page from FIDO that enables a biometric on a mobile device to be used by any entity that wants to authenticate the mobile user. In the case of delegated authentication, it enables any merchant to authenticate the user on behalf of the issuer. While this gives merchants more control, it still remains unclear if the networks are providing sufficient incentives for its adoption. Against this backdrop are fraud prevention platforms that are becoming much more accurate in identifying bad actors and helping merchants protect accounts, eliminating fraudulent transactions while keeping false positives to a minimum.

Figure 2: The SRC Cardholder Wallet Implementation Diagram

Source: Mercator Advisory Group
Authentication technology and adoption grew at remarkable rates in 2020 and will continue to grow over the next few years with biometrically capable smartphones continuing to penetrate the market, and pushed in part by PSD2 and EMV 3D Secure. The next few years will also see improved identity solutions that support digital onboarding and improved mechanisms for linking identity and authentication mechanisms to the device (improved provisioning).

The game of cat-and-mouse between technology suppliers and criminals will continue, and some companies will invest to safeguard customers’ assets while others will hope their existing techniques hold up under fire. The outcome will certainly be the emergence of even more hacks that create fear in the public. The industry still needs technology suppliers to develop standard testing methods and metrics that embrace the FIDO standard so that different implementations of the new technologies can be easily compared.

Machine Learning Moves Forward

Machine learning platforms are now so automated that they are capable of ingesting data, building models, and even automating the best feature selection for the specific task at hand. The result is that machine learning based products and services continue to penetrate every operational area of business. This trend will continue and speed up over the next few years. More business processes will become automated or guided by machine learning and, as machine learning tools are designed to access the data stored in documents and databases, voice-activated assistants will become significantly smarter for a wider range of customer and employee issues.

These advances will not be limited to voice assistants or high-end customized solutions. There will be significant progress made in applying these advances in machine learning to more basic tools such as Robotic Process Automation (RPA). RPA democratizes machine learning because it is specifically designed to learn the business process utilized by white collar workers performing repetitive tasks, such as evaluating applications received or managing expense reports. As RPA solutions become capable of learning faster and taking on more complex data driven decisions, they will begin to lower the cost structures and increase accuracy for those businesses that utilize them.

As with any new tool, there are often mistakes made in application. This is even more likely to happen when the tool is driven by data from past operations, which may have past mistakes and biases encoded in the data. These biases and errors buried in the training data are hard to identify and require specific expertise and scrutiny to uncover.

QR Codes and Alternative Payments

Older technology is springing up in new areas due to issues that are mostly unrelated to the pandemic. QR Codes are increasingly being deployed in smartphone applications and the top general purpose wallets. These codes are
then scanned by the merchant to implement a range of new payment related activity. Initially implemented in countries lacking a robust payment infrastructure, QR Codes have made recent advances in the U.S.

There are two primary advantages to the QR Code implementation. First, the QR Code solution can be easily implemented at the POS by the merchant using existing hardware. Second, QR Codes enable transactions to bypass easily the traditional payment networks. These two advantages have not been lost on loyalty and rewards suppliers or suppliers of alternative payments. Several Buy Now Pay Later (BNPL) solutions are implemented using QR Codes as are payment solutions associated with crypto transactions while a range of merchants from CVS and Walgreens to Crate & Barrel and Uber Eats have all adopted QR Codes.

But it isn’t just merchants and alternative payments suppliers moving to QR Codes. EMVCo has issued a standard that enables traditional payment rails to use QR Codes, and PayPal has been using QR Codes to enroll smaller merchants. It is even rumored that Apple is adding QR Code capability to Apple Pay, although that implementation may come with the usual Apple monetization strings attached.

It is clear that there are advantages in using QR Codes for some payment participants, especially those that find it difficult to implement solutions over the existing payment rails. Mercator expects to see these solutions continue to grow and to challenge traditional payment models from online and POS transactions to P2P and bill pay.

**Pandemic Driven Behavior Changes**

Mobile, contactless, order for pickup or delivery, and video conferencing are behaviors driven by the pandemic that are likely to remain even after we’ve all been vaccinated. The pandemic has driven a huge increase in video meetings and singlehandedly halted industry events. While there is an expectation that conventions and traditional face-to-face meetings will resume in the future, many workers will continue to work from home and both internal company meetings and B2B meetings will continue to be conducted by video. This opens up a raft of possibilities while also highlighting infrastructure and technology issues.

The pandemic will expand consumer interest in video conferencing with financial institutions and drive even greater interest in digital onboarding. This will in turn highlight the lack of a consistent method of conducting authentication across all the different physical and digital channels, which will either limit innovation or drive increased adoption of fintech solutions.

**Tokens That Bind**

Not all technology developments are impacted by COVID, many simply remain on a steady growth trajectory and will continue to gain traction in the new environment.

For example, in an effort to better secure e-commerce and mobile transactions, the payment networks have adopted tokenization, and their deployment of tokens continues to expand. The payment networks are
implementing the EMV Secure Remote Commerce (SRC) specifications (see Securing E-Commerce: Competing Technology Crowds the Market). This EMVCo standard will deliver a unique network-based consumer wallet for every cardholder. That wallet will contain any and all payment cards added by the consumer.

In theory this SRC wallet could include merchant-based solutions, although this is not a part of the EMVCo specification. The network holds the details of the payment credentials and other personally identifiable information (PII) and presents only non-PII information to the consumer. The consumer’s data is held by the network in its Access Control Server (ACS). SRC will deliver stronger security and authentication of the cardholder on the front end and deliver the PII and card data to the merchant using a secure communications channel on the backend, thus avoiding traditional e-commerce vulnerabilities. More important, unless the merchant explicitly requests the primary account number (PAN) data, the SRC implementation will always replace the cardholder PAN with a network provided token. From the merchant’s perspective, this means network-defined tokens will now be entering the merchant’s environment when the consumer uses a mobile wallet at the physical point of sale and increasingly also during every e-commerce transaction if SRC is widely adopted. In addition, tokens are being used as a gateway between different networks.

In June 2019, Visa announced the acquisition of the Rambus payments and ticketing lines of business. Rambus has already implemented tokenization on other payment networks including the ACH. Visa has stated that it intends to use its tokenization service in combination with Rambus to enable access to ACH-based accounts:

Today, Visa offers these capabilities through Visa Token Service for card-based payments on the Visa network. Rambus’ token technology will enable Visa to extend the security and convenience of tokenization to all types of transactions beyond Visa cards, including those on domestic card networks, account-based and real-time payments systems.

It is important to note that Mastercard also intends to broaden its payment network to enable transactions well beyond its own card network based on its 2016 acquisition of VocalLink. This suggests that both Mastercard and Visa are very likely to deploy some pilot versions of this strategy soon. The result will be multiple invisible tokens across the merchant and consumer environments that can only be mapped to an account by the payment networks. When different tokens are used across multiple payment networks, such as P2P or ACH, only the token vault provider will be able to link the transactions together and back to the account holder. In this scenario the token vault holder is in a very valuable position.

A Breakout Year for Cryptocurrencies

2021 will likely continue to see growth in cryptocurrencies. Existing exchanges have created walled gardens that enable them to address the regulatory requirements in the U.S. PayPal was the first major payments provider to
take the plunge, but Visa and Mastercard are opening up their networks a little at a time, so that issuers willing to take the risk can connect traditional payment cards to the crypto assets held in properly run exchanges. This enables crypto to be burned anywhere Visa or Mastercard is accepted.

Still, challenges remain. The SEC maintains that crypto is an asset that must be reported as a holding for tax purposes, but some fintechs have figured out how to collect the necessary data and deliver it for filing. Note however that all cryptocurrencies continue to be highly volatile, except for those less popular cryptocurrencies that are pegged to the dollar. Facebook’s Libra, now called Diem, will initially be pegged to the U.S. dollar and is expected to be deployed as a pilot this year. China’s digital yuan, or more officially the eCNY, is already being piloted in cities across China, including Beijing and Shanghai. With roughly 40 countries now racing to deliver digital currencies, it appears safe to predict the time is near for crypto to be more generally available.

Data Management

What was already difficult is now harder. New approaches to data management will be required to prevent training data from creating erroneous and damaging machine learning models, to prepare for the European Union’s General Data Protection Regulation and the California Consumer Privacy Act, to prepare for major shifts in the way we manage identity and the advent of ISO 20022.

The change required will be significant. It isn’t simply adding a few more metadata tags. Rather, solving the data management problem demands rethinking how to document the data that is collected and stored. Consumers have the right to be forgotten. The data used to train machine learning models needs to be evaluated specific to each model’s purpose, which simply can’t be known today. ISO 20022 requires data elements be documented via the process model that created the data.

Although Mercator Advisory Group doesn’t know yet how all of this will be managed, it seems clear that all of these new data requirements are coming at us like a freight train. 2021 will be the year when participants in the payments industry gain a better understanding of the challenges and suppliers begin to construct and offer solutions.

Creating Value by Reassembling the Payments Value Chain

Even as the payments landscape appears stable to consumers, the structure is undergoing significant change. Payment processors and issuers are arranging traditional payment components in entirely new ways, driven by innovative fintech business models.

The Clearing House (TCH) has petitioned the Fed to create a new method by which bank assets are measured in order to remove what is perceived to be an unfair advantage. At one level this appears to be driven by API access to payment networks that makes it far easier to select a network based on understanding the account structure
and business case. By making it easy to connect to new environments, such as faster payments, sources of credit, P2P, or cryptocurrency, it is becoming possible to drive higher acceptance and higher volumes, all at lower cost. However, this also challenges our existing notions of risk and creates challenges associated with existing price structures.

Consider the multiple ways that a BNPL solution integrated to a merchant’s pay screen might operate. After the consumer provides bank account information, the BNPL partner might use a virtual card to pay the merchant and then deduct quarterly payments from the consumer’s account. Alternatively, the BNPL partner might settle with the merchant at end of day or end of week using ACH. Or perhaps all of these are used depending on merchant preferences, volume and business arrangements.

Crypto creates another interesting scenario. PayPal is enabling crypto be spent at merchants that accept PayPal. Visa and Mastercard have similarly partnered with issuers that are willing to manage the risk associated with burning crypto from properly registered crypto exchanges. Yet these two solutions from PayPal and the payment networks will be very different. While PayPal has its own settlement services with merchants that accept PayPal, the networks will need to settle between the issuer and the merchant with the issuer settling with the crypto exchange. Of course crypto has no ability to dispute a transaction while the payment networks do, so time will tell which approach consumers prefer. All of this is the tip of the iceberg. 2021 will surely introduce even more interesting network connections.

The Internet of Things

What do you conjure up when you think of the term internet of things (IoT)? Typically the first items payment geeks think of are cars and watches, but these are just payment-enabled devices with Near Field Communication (NFC) capability. These are provisioned in a fashion similar to a mobile wallet using a payment token; these really are not IoT at all.

Mercator has established the following definition for IoT Payments that focuses on the true intent of any IoT solution, which is to make a data-driven decision:

An IOT transaction is a real-time data-driven payment decision that at the time of the transaction does not involve a buyer decision. Instead, the buyer has previously authorized a plan for payments to be made automatically based on feedback from a sensor or automated data source. Examples include a smart ink order from a printer, a smart electricity payment, or a car insurance payment based on telematics devices.

The dollar volumes in payments that are already associated with IoT will likely surprise you. Our current estimates show that residential electricity accounts for $66 billion in IoT payments. Some $11 billion in IoT payments is made
for IoT-based insurance. Approximately $7 billion in IoT payments is made for residential water service. In short, the IoT payments sector, while small compared with the larger payments market, is larger than most expect and is growing fast.

*Figure 3: IoT uses real-time data and AI to authorize transactions on behalf of consumers.*

Of course, the next question is, How fast is fast? Mercator has begun creating an IoT benchmark, similar in concept to the Prepaid Benchmark we started in 2005. We will identify each industry implementing the IoT infrastructure and then use the definition above to capture the payment volume associated with each segment. Our goal is to create a taxonomy that identifies all industries and segments generating IoT payment transactions. Creating the taxonomy will enable us to measure total IoT dollar volume, specify the contribution made by each industry, and identify primary use cases.

Today, multiple industries are already heavily investing in IoT infrastructure. Currently Mercator is evaluating the agriculture, logistics, insurance, home, health, municipal, utilities, and manufacturing sectors. One example of how quickly IoT can be deployed into the market is epitomized by Amazon’s IoT API, which enables any smart appliance automatically to order consumables based on gathered data. Fortune 500 companies such as Samsung, Philips, and General Electric are already using it today. 2021 is expected to bring exponentially more IoT devices, and Mercator will be tracking their penetration into the payments landscape.

**Conclusions**

Payments are exciting again. The changes are coming faster than ever. Cloud implementations of APIs create Payments as a Service and, as new payment networks come on the scene with expanded use cases, they can be interconnected in ways that dramatically change the world of payments. Many of these new payment
arrangements are driven by fintechs, so study the business models they use and carefully evaluate the value proposition they offer. The payment rails are typically below the surface and so the unique structure might be hidden from view, but if you look at a solution and wonder why it works in the market, you will simply need to dive beneath the surface to get a better view.

References

Related Research by Mercator Advisory Group

Distributed and Self-Sovereign Identity Solutions: Part 2, Implementations and Suppliers (September 2019)

Distributed and Self-Sovereign Identity Solutions: Part 1, Technology Overview (August 2019)

How Banks Can Safely Do Cryptocurrency (April 2019)

Securing E-Commerce: Competing Technology Crowds the Market (February 2019)

Tracking Mistakes in AI: Using Vigilance to Avoid Errors (August 2020)

Card Networks Deploy Delegated Authentication: Everybody Wins! (December 2020)

Endnotes


iv https://www.mercatoradvisorygroup.com/Viewpoints/Card_Networks_Deploy_Delegated_Authentication__Everybody_Wins!/


Copyright Notice

External publication terms for Mercator Advisory Group information and data: Any Mercator Advisory Group information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate Mercator Advisory Group research director. A draft of the proposed document should accompany any such request. Mercator Advisory Group reserves the right to deny approval of external usage for any reason.

Copyright 2021, Mercator Advisory Group, Inc. Reproduction without written permission is completely forbidden.

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, Merchant Services, Commercial and Enterprise Payments, Emerging Technologies, and Global Payments practices.

Primary Data. North American PaymentsInsights series presents eight annual 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. Two other Mercator survey series—Small Business PaymentsInsights and Buyer PaymentsInsights—each receive coverage in three reports annually.

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.