ENABLING THE INTERNET OF THINGS: WHY BANKS SHOULD BE PART OF THE FABRIC OF THE IoT
The term “internet of things (IoT)” is not new. Though its exact origins are disputed, it was probably coined in the late 1990s to connote the interconnectivity between devices which are able to send, receive and process data, and as a consequence “know” and can react to what is happening in their surroundings. The internet connects servers; the internet of things connects devices which are made smart by sensors — from thermostats to lightbulbs to fridges to container ships and beyond.

The explosion in the mobile internet gave the concept a major boost and in recent times, as the excitement about the IoT and what it means for the world has escalated, other hot technologies such as big data and analytics, artificial intelligence and even blockchain have been drawn into its orbit, creating a frenzy of anticipation and discussion about how together these powerful innovations will impact a number of industries, including the banking and payments businesses.

A now hackneyed but still useful illustration of the IoT in action is the example of the fridge which knows when you have removed the empty milk bottle and automatically orders more for you. This is interesting insofar as it makes it very clear what interconnected smart devices can do in the real world. It is also interesting, however, in that it demonstrates how easily a payment can become invisible — in the same way that much-vaunted disruptive businesses like Uber have made payments disappear.

While payments have always been a means to an end, at least when a consumer has to get out a card and tap — or insert it into — a device, he or she knows he is making a payment and may even think briefly about the bank whose brand is on the card. When payments happen without consumers even thinking about them, payment providers have a customer relationship challenge.

Without doubt, the IoT represents an opportunity for financial institutions to find out more about what their customers — retail and business — require, alongside a plethora of other useful information about behavior and environmental factors, which all together they can use to shape products and services accordingly. These new tailored offerings can then be presented to customers in context — so that banks are not pushing products they want to sell but rather products their customers need to buy. The resulting products and services should also be better for the customers, as personalized pricing becomes a reality, for example.

Indeed, this is already happening in the real world, as some providers are starting to offer usage-based car insurance which gives the most favorable premiums to the best behaved drivers, as determined by analysis of the information transmitted by their in-car communication devices. Emerging smart
home platforms could enable a similar tailoring of home insurance products based on the provision of information about key aspects of household management (door locking, turning off the oven, etc.) and fitness devices could obviously do the same for health insurance.

In the wholesale banking arena, connected field devices in manufacturing or agricultural sensors that monitor live stock could generate data that capital markets firms and commercial lenders could use to support investing and lending decisions — and sensors attached to goods in transit could enable the streamlining of banks’ cash management and trade services, enabling the better alignment of flows of payments and goods between sellers and buyers.

And the potential value of the IoT to financial institutions needn’t emanate from the power of machines alone. Take the example of chess. By 1997, IBM’s Deep Blue computer had been able repeatedly to beat the best human chess player. But in 2005, people playing alongside computers were able to beat both men and machines working separately. Apply this to the wealth management space, where the much talked-about robo advice phenomenon is already evolving towards a hybrid of robo and human advisory, and it is perfectly possible to envision financial institutions leveraging robos powered by vast amounts of relevant information gathered from IoT devices, working together with expert human advisors, to provide better informed and more effective decisions and strategies than either man or machine could do alone.

In the retail banking space, there are some interesting IoT applications to deploy in the branch, such as video tellers and kiosks with sensing technology which can monitor and take actions on the customer’s behalf — as well as the use of mobile geolocation capabilities in combination with beacon technology to introduce a customer on entry to the branch, enabling pre-queuing for improved service.

Of course, how much leverage banks can generate from such applications depends on how often their customers visit their branches — frankly an activity already in decline. The successful provision of truly contextual banking depends upon the embedding of financial services into a broader customer experience. Take the example of an IoT-powered shop, where a customer need only pick up an item and leave to automatically pay for it — or an IoT-powered gasoline station where the driver fills up and drives on, secure in the knowledge the payment has happened behind the scenes.

These would be greatly simplified experiences for the customer, but how does a bank go about ensuring it is the chosen payments provider, and how does it deal with the challenge of the payments experience disappearing and becoming something the customer doesn’t even think about?

In addition to these questions, there are other issues to consider. How on earth will banks — limited as they are in many cases by legacy systems which cannot cope with the amount of data available today — be able even to begin to store and analyze the amount that will be generated by a full-blown IoT?

What about the increased security risk created by the massive expansion in vulnerable access points? Security experts have already proven they can hack network-enabled light bulbs, in order to control them remotely, as well as access wi-fi user names and passwords. Clearly if automated payments were set up via the same smart home platform, payment details could be at risk. And there are data protection concerns as well — more instances of potentially sensitive data being shared with devices known and unknown is obviously a potential minefield.

**WHAT ARE THE BARRIERS TO IOT DELIVERING VALUE?**

It is clear that the IoT presents challenges for financial institutions, as well as opportunities — and the same is true on the wider stage. The concept of the IoT is not new, and indeed the reality of it is already substantial. Gartner forecast that 6.4 billion connected devices would be in use worldwide this year (2016), up 30% from last year (2015), and reaching 20.8 billion by 2020. The analyst has also estimated that services spending on the IoT this year would reach $235 billion.

However, it is also true that at the moment the IoT is not much more than a series of discrete pilot projects — such as the various smart city and smart home experiments under way around the world, and the individual IoT networks being put in place speculatively in countries such as the Netherlands, France, Germany, South Korea and others. These initiatives are typically independently funded, and therefore the question of who pays to develop the broader IoT has not yet been answered. They are also not interoperable. There is a plethora of initiatives under way to create the standard for communication between IoT devices —
GETTING IN FROM THE GROUND UP

The full potential of the IoT will take a good while to be realized, of course, and today the IoT is still immature. However, this in itself could create opportunities for banks with an ambition to embed themselves in its fabric. While the hopefully utopian IoT-driven future may be far out, there are opportunities to act and derive benefit today. There is much still to be decided in terms of how the IoT goes from pilot to prime time, and it could be that financial institutions’ native strengths fit them well to play a key role in its further development, thus securing an ongoing relevance in its operation in the real world.

For example, banks have a good track record of leveraging reliable, secure networks and communicating with globally recognized standards. It’s worth remembering that the consequences of a phone call dropping out are significantly less severe than a payment going astray. Though telcos no doubt see a great opportunity in the IoT, given the central role of networks in its realization, it could be that banks have a stronger pedigree in this context because they stand behind critical payments infrastructures. Banks — in contrast to tech start-ups, as an example — are also well-capitalized, deep-pocketed and highly regulated. As the IoT is being built, banks could bring a great deal to the table to help ensure the robustness, security and interoperability that is clearly required.

Another unresolved question is how identity is managed in an IoT world, where it applies not just to people or to companies, but to devices, all of which are not equal: some will be used by one owner, some by a number, some by the public at large, and different devices will have differing levels of built-in intelligence, local processing capabilities, battery life and even longevity. What happens to the identity of a broken smartwatch, a hacked lightbulb or telematics destroyed in a road accident? And is it actually legal to accept a payments instruction from a fridge?

Finally, there is a cultural hurdle to be overcome as well. As the popularity of dystopian novels and films demonstrates, there is a good dose of fear mixed in with people’s anticipation of what an IoT-driven world could look like. A resistance to Big Brother-like surveillance and an objection to the use of personal data to drive sales pitches could pose problems for the development and commercialization of the IoT, and this should certainly influence the choice of entities and brands relied upon to take the IoT mainstream.
The identity management aspect of the IoT’s further development could also be a natural playing field for banks. Identity management is already being posited as a new business line for banks in the wake of the changes being introduced by the revised European Payment Services Directive (PSD2) — the thinking being that as the regulatory environment opens up and banks are required to share account information with regulated third-party payment providers, they can reinforce their role in the landscape by managing their customers’ digital identities.

Trust and a reputation for strong data protection are valuable assets in the context of identity management, and though it is no small matter to tackle allocating and managing identity to billions of devices, this is certainly a viable route for banks to consider to ensure their role in the world of PSD2, IoT and whatever the next disruptive innovation turns out to be.

It is clear that a number of gaps need to be filled before the IoT can fulfill its potential, and it’s also clear that banks have natural attributes that could fit them well to help fill some of those gaps. The successful enablement of trillions of micropayments at a manageable cost for example seems a prerequisite for the IoT to work, and underpinning payments is the bank’s sweet spot.

Banks and payment market infrastructures worldwide are already focused on reinventing payment rails to cope with more and faster payments, in response to competition from new entrants and to demand from customers. At the same time they are looking to streamline their own internal process to ensure payments can be processed as speedily — and cheaply — as possible. As they do this, they need to work to accommodate not just the volumes that human beings armed with smartphones can generate, but the kinds of volumes billions of additional devices could produce. There is a very real possibility that over time the value of transactions could fall below the cost of processing them, and to be successful in payment processing in such an environment requires scale — which banks can bring. In the new world, banks may not get paid for making payments, but they may do so for enabling the commercial operation of the IoT.

In a similar vein, when they are planning their strategies for open banking and PSD2, banks should think about identity management, strong authentication and open, real-time APIs not just in the context of customers and third-party payment providers, but in the context of devices as well. The IoT can be viewed as taking the changes introduced by PSD2 further still, and as a result of the work banks do to prepare for PSD2, they will have a meta-framework on which to build. In the IoT world, there is a role to orchestrate and secure the interactions and data sharing that customers will need to ensure purchases are made and business is done, and the banks have an opportunity now to embed themselves in that orchestration at this early stage of the IoT’s evolution.

Clearly, the IoT creates new product and service opportunities for banks and to leverage those they must fit their data analytics capabilities for the new world. But before any company in any industry can truly benefit from the IoT, it has to be made industrial strength, so as they think about how to benefit from this development, banks should also think about how to contribute to it.

They will not be the only ones eyeing the opportunity. The story of telcos threatening banks on their home turf is an old one, but the IoT phenomenon could breathe new life into it. In light of this, securing a role in the fabric of the IoT and making themselves central to its commercialization — and the way in which their customers experience it — is arguably not so much an attractive option for banks as a strategic imperative.

In short, banks need to leverage their native strengths in payments, trust, security and identity and take a proactive approach to the IoT at this early stage to ensure that they are not disintermediated by yet another wave of technology — or beaten to the punch by the telcos. If they act now, the banks have a powerful opportunity to play a leading role in taking this exciting development mainstream and making the IoT a reality, to the benefit of industry and consumers alike.
ACI Worldwide, the Universal Payments (UP) company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software solutions delivered on customers’ premises or through ACI’s private cloud, we provide real-time, immediate payments capabilities and enable the industry’s most complete omni-channel payments experience.