American
Bankers
Association®

Understanding the Internet of Things

In 2008, the number of Internet-connected devices surpassed the number of humans on the planet. By 2030, it is projected that more than **125 billion** things—nearly 15 for every person on Earth—will be connected online. We call this growing network of connected devices the Internet of Things, or IoT.

Just about anything embedded with a sensor capable of sending or receiving data can become part of the IoT ecosystem. As the size and cost of embedded sensors has decreased, the potential for smart device deployment has greatly expanded. We have thermostats that set themselves to manage energy costs, video-enabled doorbells that allow homeowners to answer when away and smart beds that maintain consistent temperatures throughout the night.

IoT promises to reshape every industry—and banking is no different. Payments will become seamless as digital wallets are embedded across multiple devices, and highly granular data collection will enable greater customization and smarter loan decisions. However, with opportunity comes challenges. The vast quantities of data produced by connected devices will require smart strategies around data management, security and privacy.

Opportunities

IoT has the potential to revolutionize how banks operate. The payments ecosystem will be transformed as more and more objects are paired with digital wallets, creating a "wallet of things." Connected devices will allow the capture of data and consumer preferences once considered unattainable. This new breed of big data will enable smarter loan decisions and change the way banks connect with customers—reducing loan losses and enabling highly tailored user experiences.

Wallet of Things

The term **wallet of things** refers to the concept that nearly any connected device can be embedded with payments functionality. Digital wallets have already been added to mobile phones, tablets, wearable devices like the Apple Watch and smart home assistants like the Amazon Echo. These devices enable a more unified payments experience both online and at the point of sale. IoT can extend this convenience to a broader range of devices, allowing customers to pay anywhere at any time.

The connected car is one such device on the frontier of IoT. They have digital dashboards that allow drivers to listen to music, get directions, and even make payments from behind the wheel. For example, in January 2019 Honda announced the **Honda Dream Drive**—an infotainment, commerce, services and rewards dashboard for drivers and passengers. The dashboard lets drivers pay for things like fuel, parking, tolls, movie tickets and food from within the vehicle.

In the future, self-driving cars could also be made to receive payments, allowing their owners to generate income. Rather than signing up to become an Uber driver, one might register their driverless car to chauffeur passengers.

The wallet of things is also making headway in the home. In 2016, Samsung launched the "Family Hub" smart fridge. The appliance's dashboard lets users order and pay for groceries, build shopping lists, browse recipes, peek inside the fridge without opening the doors and leave notes for family. The fridge also connects to entertainment apps and other smart devices in the home. Users can adjust the thermostat, monitor their baby's room, or even check who is at the front door. It isn't hard to imagine a smart fridge that could initiate authorized transactions on its own when it sees, for instance, that you are running low on eggs or that your milk has spoiled.

Payments are a critical touchpoint in a banking relationship. As payments become less visible, banks may need to find other ways to keep customers engaged. Some banks have done so with personal financial management tools that help promote financial wellness.

Connecting with Customers

Mobile phones have changed the way banks connect with customers by providing a new channel to engage and deliver value. Consumers can now bank on-the-go, from the palms of their hands. This increase in digital engagement has generated valuable data that can be used to improve personalization, refine existing products and build new services. IoT can act as a force multiplier in this space, expanding the digital banking ecosystem to any connected device with a user interface. The vast pools of data produced by these devices will provide invaluable customer insights and enable new kinds of value-add services.

As IoT becomes ubiquitous, banks will be able to reach customers in new and unusual ways. Auto manufacturers, **like Jaguar**, have already tested heads-up-displays that project virtual speedometers and other basic information onto car windscreens. Driverless cars with sophisticated user dashboards will broaden these possibilities. Customers could track savings goals, manage investments or conduct minor transactions while stuck in traffic. Likewise, customers can already order food from their smart fridges, it won't be long before they can also bank from them.

Much like mobile phones, connected devices will generate troves of valuable data. This data will provide a more detailed picture of customers, which will enable greater personalization and context-specific messaging. For example, consider a customer seeking a branch on the way home. A smart car dashboard could highlight convenient locations and associated wait times based on the driver's route to identify the best option.

IoT will also enable new kinds of banking services. Today, personal financial management (PFM) apps allow users to create budgets, track spending and set savings goals. In the future, customers will be able to link these tools to other connected devices to help manage spending. For example, a banking app could regulate the temperature settings of a smart thermostat to meet a customer's monthly spending limit for utilities.

Smart Loans

In addition to helping banks enhance the customer experience, IoT can enhance banks' credit underwriting processes. As more IoT sensors are deployed across industries, banks will be able to reach previously inaccessible data to inform lending decisions and mitigate losses.

In 2015, **State Farm** received Federal Aviation Administration approval to begin testing the use of drones to assess property damage. Banks, too, are exploring potential use cases of drones and other connected devices. For instance, before underwriting a commercial loan, a bank could estimate foot traffic at a local business from the number of cars in its parking lot. Likewise, for agricultural loans, a bank could combine drone data with sensor data in the fields to estimate crop output.

The granularity of IoT data can help banks better understand and control credit risks to reduce loan losses. In our farm example, a bank could offer competitive variable interest rates that fluctuate based in part on field conditions. Similarly, by monitoring the condition of leased assets (e.g., warehouse machinery), banks could proactively make credit offers as equipment reaches the end of their lifecycles.

Connected devices can also help banks combat fraud. In trade finance, banks already use radio-frequency identification to track goods in transit. Connected devices will allow banks to monitor more **granular information**—like tracking the temperature of a food container—to ensure contractual obligations are met.

Challenges

While IoT promises exciting opportunities, banks will face a number of challenges adapting to its infrastructure. IoT brings a whole new meaning to the phrase "Big Data." Banks will need systems capable of sifting out the noise to derive meaningful insights. Robust cybersecurity will be more important than ever, as each connected device represents a new potential surface of attack. Finally, the vast quantity of customer data collected raises privacy concerns.

Data Management

Managing the constant tide of data is a challenge faced by many industries today, including banking. This challenge will only be magnified by IoT. Connected devices will produce highly valuable insights, but not all information will be useful. Banks will need systems capable of sifting through the noise to derive meaningful insights.

Many banks are considering (or are already in the process of) cloud migration. By migrating to the cloud, banks can reduce physical server costs, better organize data, and more quickly deploy new products or services while maintaining strong cybersecurity. Given the sheer amount of data IoT will produce, these cost and efficiency gains will only increase for banks using on-premise servers.

IoT will require new strategies around data storage, management, and (as we will discuss below) security and privacy. In order to successfully leverage these opportunities, banks may require new skill sets. Experience with data management, coding, machine learning and other technical experience will become even more important than they already are today.

Data Security

Connected devices can pose serious cybersecurity threats, as every IoT object represents a possible surface of attack. Banks adhere to the strongest cybersecurity requirements. Advancements in IoT device-level security will be needed before banks can be comfortable with fully enabled IoT banking.

Non-secure devices could be used by attackers to access sensitive information, conduct fraudulent transactions or orchestrate distributed denial of service attacks (DDoS). In **October 2016**, attackers took control of home routers, digital video recorders and other connected devices to build a botnet used in a DDoS attack that shuttered access to thousands of websites.

In 2018, another nefarious use of IoT was revealed by Darktrace CEO Nicole Eagen during a conference panel in London. Eagen said that attackers were able to gain access to an unnamed casino's network by hacking a thermometer in a **lobby aquarium**. One non-secure thermometer granted access to the casino's high-roller database. A fellow panelist at the conference noted a similar case where a British bank was hacked through its CCTV cameras.

As the IoT levee breaks, firms from all industries will need ways to determine connected devices are secure. Supporting this effort, the National Institute of Standards and Technology (NIST) has drafted a report to help guide IoT standards. NIST has identified **seventeen technical trust-related concerns** for individuals and organizations before and after IoT adoption and **three cybersecurity objectives:**

> **Confidentiality:** Preserving authority restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
>
> **Integrity:** Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity
>
> **Availability:** Ensuring timely and reliable access to and use of information.

Data Privacy

IoT will raise important privacy questions. In a world where nearly every object collects and broadcasts data about its environment, consumers will find it increasingly difficult to opt out. While all industries will reckon with this challenge, this issue is particularly salient in the financial services industry.

Banks continue to maintain the highest level of privacy, security and control over their customers' personal information, and consumers trust that their financial data are being appropriately protected and handled. This trust is critical to a well-functioning financial system, and is the reason banks dedicate tremendous resources to safeguarding financial data.

Today, there are competing industry efforts to standardize how data is shared and moved from one system to another. It will be important for these efforts to consider how connected devices might fit into the data sharing ecosystem. ABA believes **three core principles** should set the framework for how data is shared and how consumer data is treated.

> **Security:** Consumers deserve bank-level security and protection regardless of where they choose to share their data.
>
> **Transparency:** Consumers must have transparency about how companies use their financial data. It should be clear to consumers what data is being accessed, how long is it being held and how it is being used.
>
> **Control:** Consumers should have control over the access and use of their data. Customers should have control over what information is shared and how it is used. Intuitive control would allow consumers to see easily who is authorized to receive their data, modify what access they have and revoke that access when a service is no longer used. If consumers can easily control the data being accessed, they can better understand what is being used to better protect themselves.

Policy

Many of the challenges related to IoT exist because this nascent technology is still under development. Regulators themselves continue to grapple with the implications and potential risks of widespread IoT adoption. To date, policymakers have largely focused on identifying the appropriate device-level security protections connected devices should require.

Congress

A bipartisan group of lawmakers introduced legislation in **March 2019** that would direct NIST to establish cybersecurity standards for government use of IoT devices. The bill would also require the Office of Management and Budget (OMB) to create guidelines for the purchase and use of IoT devices. NIST and OMB would be required to revisit these policies every five years to ensure they are in line with best practices.

Consumer Product Safety Commission

Following a request for comment, the **CPSC** held a hearing in May 2018 related to the potential safety issues and hazards associated with internet-connected consumer products. The Commission has clarified that it does not plan to consider personal data security and privacy issues related to IoT devices, but rather physical security threats. Potential hazards of faulty IoT devices identified by the Commission include fire, burn, shock, tripping or falling, laceration, contusion and chemical exposure.

Federal Trade Commission

In June 2018, responding to the CSPC's request for comment, the FTC's Bureau of Consumer Protection (BCP) warned that poorly secured IoT devices could pose consumer safety hazards. BCP staff emphasized that poor security in IoT devices might create technology-related hazards associated with the loss of critical safety function, loss of connectivity or degradation of data integrity. For example, a car's braking system might fail if infected with malware, or carbon monoxide or fire detectors could stop working if they lose their Internet connection. BCP staff advised that the CPSC consider how companies might provide consumers with the opportunity to sign up for communications about safety notifications and recalls for IoT devices.

Final Word

IoT promises to transform how entire industries function, and banking is no exception. The rise of the "wallet of things" will completely change the way we conceptualize money, payments and banks' central role in the ecosystem. Connected devices will unleash avalanches of information that make today's "Big Data" seem quaint by comparison. This data will enable brand new ways of connecting with customers and managing credit risks.

However, there are still some daunting challenges facing IoT. As with any new technology, banks will require systems that can interface with IoT in a secure and efficient manner. Moreover, banks will need systems that can derive meaningful insights from the constant flow of information. Banks may require prioritizing new types of skills as they grapple with these challenges.