# The Hope and Fear of Open Banking

Applying for a loan can be one of the most frustrating experiences in life. It’s a series of patience-taxing stops and starts that closely resembles New York City traffic at 5:00 p.m. on a Friday afternoon. You go to the bank for a loan. The bank gathers data, crunches numbers, runs formulas, and then returns with a yes or a no. If the application is a close call that doesn’t meet all of the bank’s risk guidelines, then there’s the obligatory petition to get a credible co-signatory on the loan. It’s not as if the banks don’t want to loan money — *it’s their business* — but the process is the process.

Banking is a siloed industry. All of the records accumulated to process your application for a loan remain with the bank at which you applied. There is no information sharing. Each and every time you apply for a loan you have to provide the data all over again. It becomes like a recurring nightmare — credit reports, verbal explanations, employment history, clean suit, attitude focus, hope and expectation — and you have to keep going until you find a financial institution that will work with you.

## The Hope

Open banking could change everything we know about the fluidity of money. It’s a conceptual model for financial services wherein banks and other financial entities allow customers to access their data and account information through application programming interfaces (APIs). This would allow customers to securely share their data with third parties who could then leverage the data to provide products and services tailored to the end user. This would take the loan applicant out of the congested New York City traffic and would be more akin to teleporting them directly to the financial institution or service provider that can meet their needs - because those needs have already been addressed through a digital interface. Think of it like a dating application for loan clients and lenders, one in which all of the images and information are bonded. Open banking could make money and financing kinetic. It could go from the congested traffic of New York City to the German Autobahn in the blink of an eye, changing the global landscape of finance.

Access to capital is the largest inhibitor to the development of economies in the poorest sectors of the globe. Microcredit banks emerged in India a number of years ago and transformed the small business landscape, helping multitudes of people gain independence and entrepreneurship with microloans for things like weaving equipment. Traditional banking in India would not go near this sector. Open banking could fill this market gap and many others much more efficiently than the microcredit banks of India and extend the model across the globe if connected to international banking institutions. So what’s the holdup? Why haven’t we entered into the world of open banking already? In a word: security.

## The Fear for Open Banking

The open banking architecture is built upon third party providers (TPPs). Think of them as a broker. They connect banks and consumers. They have two functions, access to account information and payment. The account information service providers (AISP) and payment initiator service providers (PISP) are the rudimentary framework upon which a more complete open banking can be built. However, people would be sharing their most personal information, their personally identifiable information (PII) which, in the wrong hands, could be ruinous. For open banking to emerge, we must have confidence in the security.

The open banking ecosystem is populated with insurers, fintech, loyalty partners, service providers, financial management tools, accounting services, retailers, advice channels, pension providers, and of course banks. All of them connect to each other via TPPs. For this ecosystem to exist, there has to be global legislation to support it and the means to enforce it. Measures like the European Payment Services Directive Two (PSD2) create a framework for TPP to exist within their ecosystem. It came into force incrementally between January 2018 and September 2019, but there is still a great deal of cautious hesitation. The number one concern is the security of PII. How can a global ecosystem moving this fast guarantee [protection against the multitude of data pirates](https://www.hcaptcha.com/enterprise) operating in the world? How can we move into open banking when these risks exist?

Open banking has to respond to these concerns with strong authentication like multi-factor authentication (MFA), encryption technologies that protect data in transit and at rest, and robust access controls to permit only authorized users and applications to access sensitive data. The technology to fill these security gaps is emerging quickly.

But what about regulation? What comparable bodies at a national, regional, hemispheric and international level will provide the guarantees of the Federal Deposit Insurance Corporation (FDIC) in the United States or similar institutions in other countries? Is the open banking ecosystem going to be the wild west or will there be Marshalls?  
All of these questions are as-of-yet unanswered in any manner that could assuage the PII paranoia. Legislation is moving along and the motivation does exist in parliaments around the world, but we’re not quite there yet.

## AI and ML are the Hope

The first stage of any serious attempt to bring open banking to normalization in the global marketplace has to begin with cleaning up the completely unstandardized world of APIs which govern TPPs. For that to come to fruition, there has to be a new system of accounting and notation in banks that removes them from their legacy systems and processes and into a data exchange format compatible with the open banking infrastructure.

The industry finds itself stalled between authority-backed standardization as a starting point in the TPP market and the legislation to enforce the standardization. There are very few voices actively speaking to this authority gap. Banks are internationally governed by rules which are generally written by the International Monetary Fund (IMF), World Bank, or the Bank for International Settlements (BIS), but they have not been as vocal as they might be if they were strong open banking advocates. The only body tangentially addressing the problem is the Basel III Committee.

Basel III is a set of international banking regulations written by the Basel Committee on Banking Supervision. The third iteration of the standards avoids referencing the open banking system but, nonetheless, moves in that direction with strict and precise provisions on the management of data — most centered on risk management. The standard insists that banks have compatible data management systems or that they capture and report data in a specified way. Basel III is a tremendous step forward for open banking. Consistent data formats ensure that TPPs utilize the same data format, and the committee has provided strong leadership on the application of open APIs in banking, which can be leveraged by open banking andTPPs.

So where does security fit into all of this? The better question is where doesn’t security fit in? The agreed upon consensus in the computer science world is that API endpoints are the greatest vulnerability.

This can be mitigated through artificial intelligence (AI) and machine learning (ML). They can be used to gain a deeper understanding of threat signatures associated with specific types of security threats. Through ML, threats can be detected across applications, device types, ips and more - enabling clustering capabilities that would be impossible for a human to reproduce. With this technology, users - both bad, good, and automated - can be accurately fingerprinted to create a seamless experience for legitimate end-users and drive up attacker costs for the cybercriminals.

This approach dovetails into a strong MFA strategy. A password or personal identification number (PIN) can be used to further enhance security. A security token could be passed to a smartphone associated with the user.

These are the remedial steps for endpoint security. But what about the data itself as it flows freely through the digital universe? The data is so voluminous that rendering meaning out of it would be like trying to differentiate between one drop of water and another in the Atlantic Ocean. Only AI can render meaning and aggregate the data into groups of metadata that can be further refined into data sets which have meaning for data aggregators. The quartet of network vulnerabilities are web application and API protection (WAAP), secure sharing of sensitive data by author and authentication, effective handling of consumer consent, and the guarantee of data compliance.

Human risk mitigation is limited in that it cannot scale. Any operation looking at large-scale data transactions must rely upon ML and AI. It’s truly the only way to get us out of this traffic jam.