# The Hope and Fear of Open Banking

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

Banking is a siloed industry. All 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 go for the loan you have to provide the data again. It becomes like a recurring nightmare — credit reports, verbal explanations, employment history, clean suit, attitude focus, hope and expectation — and you have to just keep going until you find a financial institution that will work with you and see what you’re proposing.

Open banking could change everything we know about the fluidity of money. In brief, open banking is a conceptual model for financial services wherein banks and other finance entities allow customers access to their data and account information through application programming interfaces (APIs). In theory, this would allow customers to securely share their data with third parties who can then employ the data to innovate and provide products and services more tailored to the customer, like the microcredit model in India. This would take the loan applicant out of the congested New York traffic and be more akin to getting into an Uber that takes 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 the images and information are bonded.

Open banking could make money and financing much more kinetic. We could go from the congested traffic of New York City to the German Autobahn in the blink of an eye. It could change the landscape of financing in so many ways and be beneficial to so many sectors of our global economy they’re almost too enumerable to list.

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 loan landscape, spring boarding multitudes of people into independence and entrepreneurship with the smallest of loans 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 exponentially more 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 open banking architecture is built upon third party providers (TPP). Think of them as a broker. They connect banks and consumers. They have two functions: to get 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, for this to happen there needs to be a significant confidence in 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 with TPP. For this ecosystem to exist there has to be legislation to support and enforce it. Measures like the European Payment Services Directive Two (PSD2) mandates the requirements for TPP to exist in that ecosystem. It entered into force between January 2018 and September 2019, and it requires critical changes in the financial ecosystem to allow TPP access to bank infrastructure. But still there is hesitation in the market.

The number one concern by a significant stretch is data security. How can a global ecosystem moving this fast guarantee protection against the multitude of low, medium, and high sophistication data thieves operating in the world? How can we possibly move into a world of open banking when these risks exist?  
The digital world has completely replicated the original World of international trade replete with pirates.

And what about regulation? What comparable office will emerge at a national and international level to 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 have yet to be worked out. Legislation is moving along and the motivation does exist in parliaments around the world, but we’re not quite there yet.

But before we can even get to the stage of legislation and financial data security with risk underwriting, we have to clean up the completely unstandardized world of APIs which govern TPP. For that to take place there has to be a new system of accounting and notation in banks that gets them out of their legacy systems and processes and into a data exchange format commensurate with the open banking ecosystem.

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 — but the standard does insist that banks have capable data management systems and that they capture and report data in a specified way. For open banking this is a step forward because consistent data formats will necessitate TPP operate in the same data format. Most importantly, the committee has provided strong leadership on the use of open APIs in banking, and this can be leveraged toward open banking and the participation of TPP.

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 the endpoints of the API are the vulnerabilities for user security. This means that when you go to authenticate on a TPP the vulnerability is at its highest. How can this be mitigated with AI or machine learning? By presenting options to the users that only a human being could answer, a set of pictures out of which only one commonality is to be selected. This eliminates all the digital intruders. A digital intruder operating at the level of code would not be able to visualize what the end user sitting at a desktop or on a tablet would see. After human verification is established an authentication process which consolidates the identity of the user through two or three steps is absolutely necessary. These are the remedial steps for endpoint security. But what about the data itself as it flows freely through the digital universe? The data itself is so voluminous rendering meaning out of it would be like trying to differentiate between one drop of water and another in the Atlantic Ocean. In fact, the data is so extensive that AI is required to render meaning and aggregate the data into groups of metadata that can be further refined into data sets that 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.