# The Long and Winding Road to Open Banking

With more transactions taking place online one might think that legislation concerning [data privacy and security](https://www.hcaptcha.com/enterprise) would be paramount for governments. For some governments the answer is yes. For the two largest economies in the world, China and the United States, the answer is no. Understanding why is a befuddling speculation. Leaving Beijing alone, the real question is why is the United States, the world’s free market champion and leader, is dragging its feet on [consumer data protection](https://www.hcaptcha.com/post/why-captchas-will-be-with-us-always) and the ensuing open banking that would trail closely behind.

The journey into codified data protection rights within the United States begins in 2010 with section 1033 (D) of the *Dodd-Frank Wall Street Reform and Consumer Protection Act*.

STANDARDIZED FORMATS FOR DATA. The Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section.

The bureau referred to in this section is the Consumer Financial Protection Bureau (CFPB). Their progress on data protection regulation for open banking has been a cover of The Beatles *Long and Winding Road* sung by an out-of-tune bureaucratic choir.

Nothing concrete has as-of-yet emerged, however, it looks like that might be changing. As of October 25th, 2022, director Rohit Chopra released prepared remarks about the coming data protection rights act. One of the principal and justified concerns about open banking is the security, and the CFPB is acutely aware of this.

One reason that the current ecosystem is unstable is that many companies currently access consumer data through activities like screen scraping. However, such methods are not secure, and they are likely not sustainable, especially as data security standards potentially evolve to a point that such activities may become blocked.

## Diminishing Security Concerns

These concerns are valid, especially for the United States, the financial market that brought us the subprime mortgage debacle of 2007, destabilizing global markets for years and bringing us into the age of quantitative easing (QE). But it’s time for the US to take leadership again.

The private sector is way ahead with artificial intelligence (AI) and machine learning (ML) offerings which profoundly mitigate the risks of open banking. These concerns have been aptly covered by legislation in other countries and economic blocks. The United Kingdom passed the [Payment Services Regulations Act](https://www.legislation.gov.uk/uksi/2017/752/contents/made) in 2017 and introduced an open banking standard. The European Union has the [Payment Services Directive 2](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366) (PSD2). Australia passed the [Consumer Data Right](http://./Consumer%20Data%20Right) legislation in 2019. Singapore introduced guidelines for open banking through the [Monetary Authority of Singapore](https://www.mas.gov.sg/) (MAS) in 2016.

## Conceptualizing Data Security in Open Banking

Imagine having responsibility for every blade of grass on an eighteen-hole golf course, including the greens, and imagine responsibility for every grain of sand in the sand traps. From the perspective of the human mind it’s incomprehensible. A greenskeeper can take care of the general health of the fairways, the greens, and the sand traps can be raked regularly, but human capability ends there. Now imagine that a single blade of grass could pose a risk to the entire golf course, or a single grain of sand. How could anybody possibly take responsibility for the golf course? This is an apt metaphor for the security risks in open banking. Every blade of grass and grain of sand is the private data of an individual human being or corporation, and if the data of one participant is compromised, the integrity of the entire system is compromised. What can be done once can be done twice, and once reputational integrity is lost it’s very difficult to regain.

## ML and AI Risk Mitigation

ML and AI make human responsibility obsolete. To understand the power of ML and AI in data security you have to understand what they are, the level they operate at, the speed and efficiency, and volume at which they can operate. These computational capabilities are difficult for the human mind to comprehend, and this is why metaphor is required. Imagine operators in the blades of grass moving around and communicating with them to make sure their molecular structure is consistent and their nutritional metrics are good, and imagine the same for the sand traps, operators checking the moisture and viscosity of the sand at regular intervals, documenting all anomalies and reporting back to the human mind, — the greenskeeper — who can comprehend. This is ML and AI as it pertains to fraud detection, behavior anomalies, and predictive modelling, and it’s why open banking is not nearly the risk the CFDB is allowing it to be by their prolonged procrastination.

The [Open Banking Rule](https://www.federalregister.gov/documents/2020/11/06/2020-23723/consumer-access-to-financial-records) has been in draft format for over a decade since the Dodd Frank. Their main concern is articulated perfectly in section G, paragraph 38 of their own Open Banking Rule.

How effectively does existing law that bears on data security mitigate data security risks associated with data access and, in particular, authorized data access? What steps, if any, should the Bureau take to improve the effectiveness of existing laws that bear on data security in the context of data access?

Excellent question, hopefully they’ll be able to answer it soon before the rest of the global economy leaves them behind.