

Open Banking and the Data Privacy Dilemma

開放銀行與數據私隱的矛盾



Open banking encompasses a set of rules and protocols that allow customers to permission third parties to access the banking and financial data of customers using application programming interfaces (APIs).

開放銀行涉及一套規則和協定，讓客戶容許第三者透過應用程式介面查閱其銀行及財務數據。

Open banking has been touted as a solution for increasing competitive pressure on traditional financial services providers and reducing the friction and inertia that often prevents customers from moving between banking providers, even where the second banking provider may provide a better product and service offering. Open banking increases competitive pressure on incumbent banks as it allows

customers to be shown a wider range of financial products and services from competitors – such as better savings accounts or credit offerings – and potentially allows customers to more easily move to such competitors by reducing the time and effort needed to transfer ongoing arrangements such as direct debits for recurring bill payments.

Open banking is also helpful to incumbent banks: where there is a two-way flow of data, incumbent banks can also get a more accurate picture of their customer's profile. They can also help incumbent banks increase customer stickiness by allowing trusted third parties to collaborate with banks and connect with the bank's ecosystem to offer a range of complementary products such as budgeting tools, lifestyle tools and financial wellness services.

At the heart of open banking is the power of data and the balancing of the sharing of that data to achieve win-win outcomes for banks and customers, while at the same time protecting the privacy of individuals. Such is the competitive power of open banking that many unofficial app products – which try to mimic the effect of open banking by asking customers to share their banking login credentials (and hence pose a serious security and integrity risk) – have already driven a number of incumbent banks to improve and match features such as budget trackers and dashboards to view finances at a glance.

開放銀行一向被視為一種解決方案，有助增加傳統金融服務提供者的競爭壓力，減低客戶轉換銀行的阻力，克服客戶面對另一家銀行提供更佳的產品及服務下，也不願改變的惰性。開放銀行向客戶展示競爭者的多種金融產品及服務，例如較佳的存款帳戶服務或信貸服務等，又減少更改日常帳單自動轉帳等常行安排所需的時間和精力，有機會讓客戶輕易地轉移至這些競爭者，因而增加對現有銀行的競爭壓力。

開放銀行對現有銀行也有幫助：由於數據雙向流動，現有銀行也可更準確了解客戶的情況；現有銀行也可透過開放銀行，讓可信賴的第三方與銀行合作並與銀行的系統聯繫，提供一系列的輔助產品，例如開支預算工具、健康生活工具、財務健康服務等，以加強客戶對銀行的忠誠度。



“
At the heart of open banking is the power of data and the balancing of the sharing of that data to achieve win-win outcomes for banks and customers, while at the same time protecting the privacy of individuals.”

Why has open banking stalled in Hong Kong?

One of the key reasons that open banking is so difficult to implement is that in most jurisdictions – including Hong Kong – incumbent banks are the data controllers of their customers' data. That means that incumbent banks are the safe-keepers of customer data and there are serious consequences for inappropriately sharing data outside of the bank's internal ecosystem and even within the same banking institution. Open banking is also often a one-way data flow from incumbent banks out to new players; as such, incumbent banks providing access to personal data assume a level of risk that currently has little tangible financial reward when compared to the risk of opening up their IT systems and allowing third party providers (including competitors) to obtain commercially valuable information about their customers, as well as exposing incumbent bank's IT surfaces to cybersecurity risk and potential impact on the confidentiality and integrity of the system held by the bank.

開放銀行的核心，是數據的力量；同時須在兩方面取得平衡：一方面藉着分享數據，為銀行和客戶帶來雙贏效果，另一方面則保障個人私隱。開放銀行促成了強大的競爭，許多非正式的應用程式產品模仿開放銀行的效果，要求客戶分享其銀行登錄資料（因而帶來嚴重的保安及數據完整性風險）；這些產品已促使一些現有銀行改進產品，提供類似的功能，例如預算追蹤、財務狀況圖表等，有關資料一目了然。

為何香港開放銀行的發展停滯不前？

開放銀行難以實施的主要原因之一是，在大部分司法管轄區（包括香港），現有銀行都是客戶資料的管控人，這意味著銀行需要安全保管客戶的資料。假如資料不當分享至銀行內部系統以外，會引致嚴重後果。開放銀行亦往往是由現有銀行流向新參與者的單向數據流動，如此一來，容許他人查閱個人資料的現有銀行，須承擔一定程度的風險，同時只帶來甚少的可見財務回報，等同於開放資訊科技系統以容許第三方供應商（包括競爭對手）取得有商業價值的客戶資訊，並讓現有銀行的資訊科技系統承受網絡保安風險，可能影響銀行系統的機密性和完整性。

How can parties solve for privacy-related hesitancy? Regulatory mandates

The key is clear regulation that ensures that both the incumbent bank and the recipient of open banking data share the risk and the cost of implementing trusted railroads for the exchange of data and clarity of liability should there be an unauthorised incident relating to customer data – much the same way that there are existing protocols and standards set up for payment railroads (such as the Faster Payment System in Hong Kong) – in short, creating a framework of uniform guardrails for parties to confidently share open banking data.

In the UK and Australia, a regulation-first model has been adopted. What this means is that the governments in those jurisdictions have set out legislative frameworks requiring incumbent banks to engage with the open banking mandate, along with setting up standards by a central standards-setting body to ensure that there are clear guidelines on how open banking APIs should be designed and minimum requirements on security – such as user authentication and consent management as well as additional layers of security. For example, in the UK, the Financial Conduct Authority (FCA) and government bodies create standards that all third parties who want to access open banking data need to comply with in order to participate in the open banking ecosystem. Such third

如何釋除有關私隱的疑慮？

監管要求

清晰的規定是關鍵所在，確保現有銀行與開放銀行數據的接收方共同承擔設置可信通道交換數據所帶來的風險與成本，並清楚訂明在發生有關客戶數據的未經授權事件時雙方的責任，如同目前有關支付通道（例如香港的快速支付系統「轉數快」）的協定和標準一樣。簡言之，就是為各方制訂劃一的保障制度，以便放心地分享開放銀行數據。

英國和澳洲採用了規則先行的模式，亦即由司法管轄區的政府制定法律，要求現有銀行參與開放銀行，同時由負責制定標準的中央機構制定標準，確保有清晰指引，說明開放銀行應用程式介面應如何設計，以及保安方面的最低要求，例如用戶認證和用戶同意的管理，以及額外的多重保安等。例如在英國，金融行為監管局及政府機構制定標準，所有希望查閱開放銀行數據的第三方均須遵守，才可加入開放銀行系統。這些第三方必須接受獨立審核，證明其系統及保安從一開始便符合最低標準，並須接受定期測試，才可繼續接達開放銀行的環境。同時，開放銀行規則清楚訂明整個行業通用的規定，開放銀行系統的所有參與者均須遵守。同樣，澳洲法例註明消費者的數據權利（澳洲開放銀行制度的基礎），清楚訂明消費者數據分享的規定，另有數據標準組織訂立的分享格式及程序；而在有關制度下，只有獲當地競爭及消費者監管機構認證的第三方，才可以進入消費者數據權系統。

這些地區的開放銀行相對成功，有賴法規的保障，重要的是亦有賴第三方按整個行業均清楚明瞭的制度審核個案。即使仍有改進空間，制度可讓現有銀行有信心地分享數據，並清楚知道所涉的責任風險。相比之下，香港的開放銀行制度受到較少法規監管，主要依靠市場參與者商討有關數據分享的雙邊安排。本地市場情況獨特，少數大型銀行佔據市場，加上對於如何實施開放銀行缺乏清晰的行規，也欠缺政府認可的第三方作為安全網，以致現有銀行與第三方分享數據的風險極大，與潛在好處不成比例。簡言之，由於現有銀行須與有意運用開放銀行數據的第三方私下進行雙邊討論，因此要大規模實行數據分享安排十分困難。即使是已開始真正參與開放銀行的銀行，也概數挑選獲認證的第三方服務提供者是一項繁重工作，需要投入不少努力。

parties must undergo an independent audit to demonstrate that their systems and security meet the minimum standards at the outset and undergo periodic testing to maintain their access to the open banking environment. At the same time, open banking regulations set out clear rules that apply industry-wide to all participants in the open banking ecosystem. Similarly in Australia, legislation setting out the consumer data right (which forms the basis of the open banking regime in Australia) creates clear requirements regarding consumer data sharing, alongside standards for the format and process of sharing that are set by the Data Standards Body, all underpinned by a system of only allowing third parties accredited by the local competition and consumer regulator to access the consumer data right ecosystem.

The relative success of open banking in these jurisdictions would not be possible without the legislative and regulatory guardrails and importantly, the vetting of third parties based on a well-understood industry-wide system. Though there is room for improvement, the system allows incumbent banks to share data confidently and with clear visibility of liability risk of doing so. By contrast, in Hong Kong, the open banking system is far less regulation-heavy. Instead, the Hong Kong model relies on market participants to negotiate bilateral arrangements to facilitate data sharing. The dynamics of the local market – and in particular, the dominance of a handful of major banks – combined with the lack of clear industry-wide regulation on how open banking should be implemented and the lack of a safety net of government-accredited third parties, means that the risk of sharing data by incumbent banks with third parties is disproportionately high compared to the potential benefits. Simply put, the ability to scale any data sharing arrangements is limited by the need for bilateral private negotiations between the incumbent bank and a third party wishing to leverage open banking data. Even those banks that have already started the process of truly engaging with open banking have lamented that choosing third party service providers (even where they have received accreditation) is a major undertaking and requires a substantial level of diligence and effort.

In Hong Kong in particular, open banking has stalled at phases 3 and 4 of the Hong Kong Monetary Authority's (HKMA) open banking plan. Phases 1 and 2 were not particularly difficult to achieve, as the information to be shared related to generic product information that could be gleaned from public sources and price comparison websites. Phases 3 and 4 are much more difficult to surmount as they involve the sharing of identifiable customer data and transaction history – which is also where the real promise of open banking lies.

特別是在香港，開放銀行在香港金融管理局（金管局）的開放銀行計劃第三及第四階段停滯不前。而實現第一及第二階段並不特別困難，原因是這兩個階段分享的資訊與一般產品資訊有關，只要用點功夫，在一定程度上可以從公共資訊來源及格價網站找到。第三及第四階段涉及分享可識別客戶的數據和交易紀錄，因此困難很多，但這也正是開放銀行的真正前景所在。

“
開放銀行的核心，是數據的力量；同時須在兩方面取得平衡：一方面藉着分享數據，為銀行和客戶帶來雙贏效果，另一方面則保障個人私隱。”

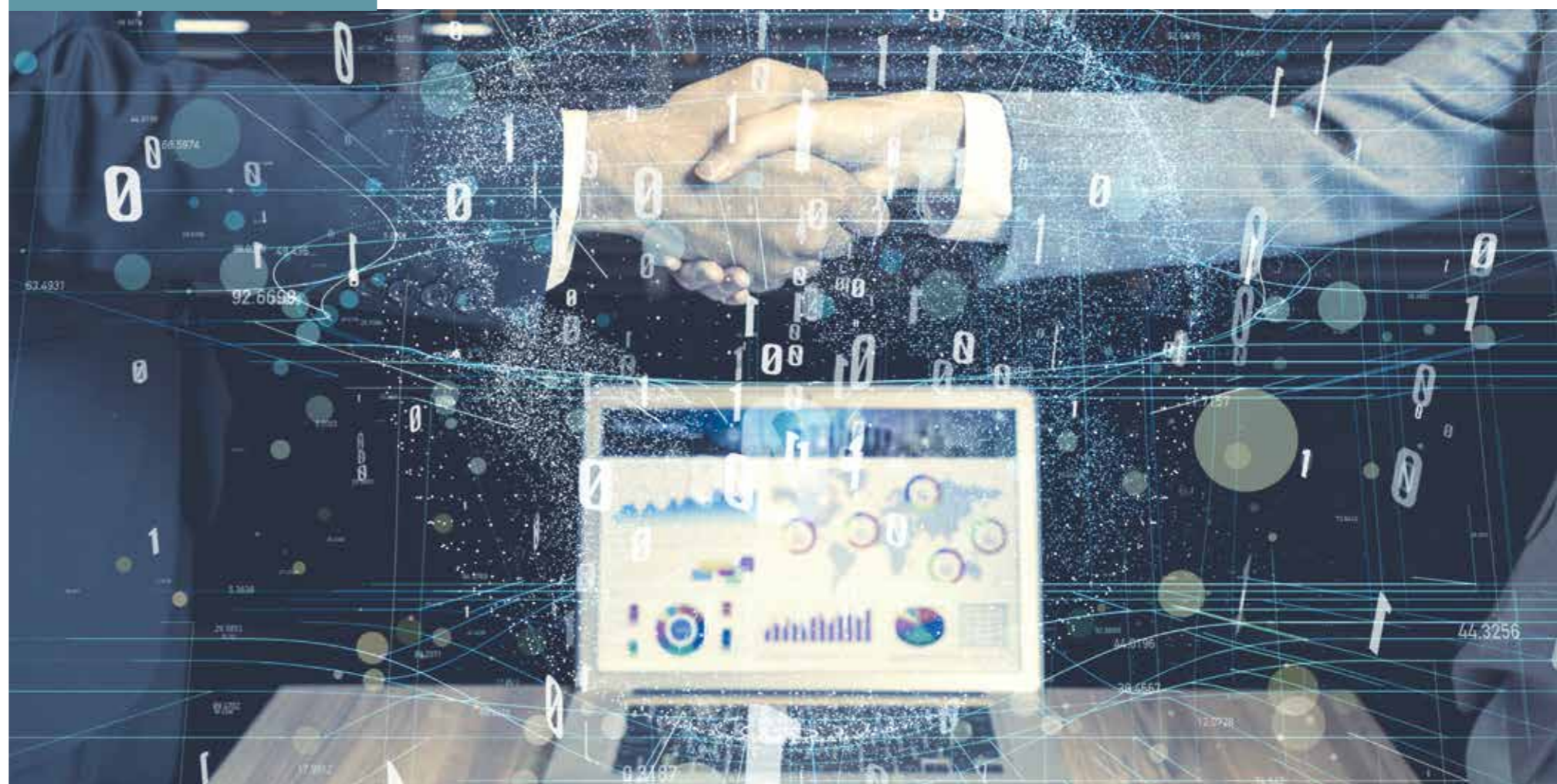
Other solutions

Rather ingeniously, the HKMA has approached the glacial pace and reticence of incumbent banks to engage in the process by flipping the open banking concept with its Commercial Data Interchange (CDI) initiative. Rather than focussing on incumbent banks being required to open up their data to new third parties – the conventional way in which open banking is thought about and which does not give incumbent banks much commercial incentive to engage – the CDI is about obtaining data from small-medium enterprises, with their consent, and sharing the data with the banks. In other words, banks receive a new data stream that translates far more easily into a business case and return on investment evaluation practices. Given that Hong Kong has authorised eight virtual banks, that in addition to incumbent banks add a new layer of dynamics and choices in the retail market and are likely to expand further into the SME and private wealth markets, this approach complements the HKMA's strategy of creating an innovative, yet trusted, banking ecosystem.

其他方案

金管局巧妙地透過其「商業數據通」項目翻轉開放銀行的概念，提升現有銀行的進度及打破沉默僵局。局方的焦點不是要求現有銀行向新的第三方開放數據，這是傳統以來對開放銀行的理解，對於現有銀行來說商業誘因不大；反之，「商業數據通」是在中小企同意的情況下向其取得數據，並將有關數據與銀行分享。換句話說，銀行可得到新的數據，這便很容易成為開展業務的理由，也很容易作投資回報評估。香港已認可八家虛擬銀行，加上現有銀行，便為零售市場增添動力和選擇，並有可能把業務進一步擴展至中小企和私人財富市場；這項發展，與金管局建立創新而可信的銀行系統的策略相輔相成。

這發展方向令人振奮，有機會形成有意思的經營模式，例如根據中小企過去的開支、財務需要和預期業務發展等數據，配合人工智能評估風險和信用狀況，便可主動向中小企推銷



“
Simply put, the ability to scale any data sharing arrangements are limited by the need for bilateral private negotiations between the incumbent bank and a third party wishing to leverage open banking data.”

“
簡言之，由於現有銀行須與有意運用開放銀行數據的第三方私下進行雙邊討論，因此要大規模實行數據分享安排十分困難。”

This is an exciting direction as it allows for interesting business models to emerge – for example, rather than waiting for the SME to seek credit of its own accord, credit could be proactively sold to SMEs that are right-sized for the specific enterprise based on the data of their past spend, financing needs and predicted business growth in combination with the use of artificial intelligence to assess risk and credit. Many innovative challengers are already looking at ways to do this, and creating a government-endorsed channel for doing so via the CDI. In the process they are challenging the dominance of e-commerce platforms that currently hold the vast majority of alternative credit scoring and SME data, which can help to move innovation in the right direction.

Private data trusts

To help facilitate the progress of Phases 3 and 4 of the open banking roadmap, what can parties do? As already discussed, the biggest risks for these phases are data security, authentication authorisation and controlled access to APIs. While Hong Kong operates with a relatively hands-off style of government, the HKMA is wary of allowing the sharing of customer data without the comfort of knowing that the data will be adequately safeguarded.

One method of resolving this is a market-driven data trust construct. Data trusts are a method of sharing data via an independent third party trustee or board of trustees charged within a coalition of members using common rules for data

額度恰當的信託產品，而無須等待中小企自行申請。許多有創意的市場挑戰者已經探討這類經營方式，並尋求透過「商業數據通」，以政府認可的渠道進行。目前電商平台持有大部分的另類信用評分和中小企數據；在新的發展過程中，這些市場挑戰者挑戰現時支配市場的電商平台，推動創新，朝着正確的方向進發。

專用數據信託

各方如何推動開放銀行第三及第四階段的發展？正如上文所述，這兩個階段的最大風險，是數據保安、驗證授權和控制接達應用程式介面。香港市場較少受政府干預，但金管局對於在不能確保客戶數據得到充分保障的情況下容許分享客戶數據的做法有所警惕。

一個解決方法是以市場驅動的數據信託模式處理。數據信託分享數據的方法，是讓聯盟成員之間透過獨立第三方受託人或受託人董事會分享數據，並遵照有關數據保安、私隱和保密的共同規則，互通系統，形成新的共享數據庫。換句話說，有興趣向數據信託提供數據，以及從數據信託取用數據的各方訂立私人協議，以合約形式規定協議各方的責任、期望和法律責任。信託的最終目的，是作為信託數據的受託人，從而保障數據相關個人的權益。這與金管局目前透過私隱協議實行數據分享的路線圖相符，但並非透過難以擴大規模的雙邊安排

security, privacy and confidentiality to connect their systems and form a new shared repository of data. In other words, a private agreement between interested parties that sets out a contractual framework of responsibilities, expectations and liabilities of entities that contribute data to the data trust and entities that access and use the data in the data trust. The trust would be charged with the ultimate goal of acting as a fiduciary of the data in trust and therefore protecting the interests of the individual to whom the data relates. This dovetails with the HKMA's current roadmap for privacy agreements between parties to implement data sharing, but rather than relying on hard-to-scale bilateral arrangements, it allows parties to agree at an industry level on uniform rules. It could also allow for the contributors of data to obtain a fair payment or commercial return in exchange for the contribution of data – for example, a sliding scale of commercial return depending on the volume and quality of data contributed by a party. While a market-driven data trust construct is likely to raise eyebrows among proponents who are against the selling of data for gain, in truth, the exchange of value or commercial benefit for data already occurs (albeit in less explicit ways) throughout the business world. To shift the data sharing needle forward, data trusts may well be a way of ensuring that data can be shared in a transparent way for the mutual benefit of both businesses and consumers. **BT**

進行，而是容許業內各方協定一致的規則。這也容許數據提供者因提供數據而獲得公平的收益或商業回報，例如根據所提供數據的質與量，按比例給予回報。對於由市場驅動的數據信託，反對出售數據圖利的人可能不以為然，但實際上，就數據交換價值或商業利益的做法，在商界已經存在，儘管並不明顯。若要推動數據分享，數據信託可能是確保以透明方式分享數據的一個方法，讓商家和消費者同樣得益。 **BT**

ABOUT THE AUTHOR

作者簡介



Michelle TA
Managing Associate
Simmons & Simmons
西盟斯律師行資深律師