INSTITUTE of INTERNATIONAL FINANCE

SEPTEMBER 2018

LIABILITY AND CONSUMER PROTECTION IN OPEN BANKING

By allowing customers to grant third parties access to their bank accounts, open banking frameworks can give rise to a broad range of financial applications that aggregate data, provide valuable insights or initiate transactions. As a result, customers can benefit from new tools to manage their personal finances and, more generally, from greater innovation, competition and access to financial services. However, as with any innovation or new market development, it comes with accompanying risks. These must be appropriately identified and addressed to ensure customers are protected at all times and the stability and integrity of the financial system is preserved.

Key elements of such protection include a clear framework for the assignment of liability for breaches and errors and consequential financial loss and ensuring that market participants are sufficiently resourced to be able to compensate customers in such an event. While this is well-established for incumbent firms in the form of the operational risk capital requirements on banks, this aspect of consumer protection is still an evolving area in some open banking frameworks.

1. RISKS FOR CONSUMERS IN OPEN BANKING ECOSYSTEMS

New risks in the open banking ecosystem arise from the greater flow of customer data — no longer restricted to the entity where it was generated — and the new intermediation roles that can be performed by either financial institutions or other non-bank players. Fraud and scams are essentially based on information — they rely on unwanted and unexpected access to sensitive data. Even within what is currently a relatively contained ecosystem, sometimes just involving a bank and a customer, fraudsters can occasionally manage to obtain data and use it against customers. In an environment where data is much more open, the risk of data exposure is likely to grow. For instance, new categories of fraudsters and scammers can try to masquerade themselves as legitimate new third-party providers.

The major areas of risk for users of open banking ecosystems are:

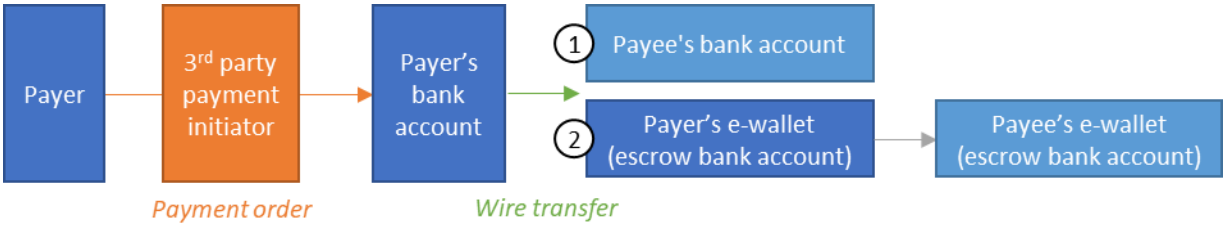
- Data breaches: unintended leaks or external attacks might expose customers' sensitive information, such as financial transactions and balances, bank account numbers or even online banking log-in credentials. In addition to violating customers' data privacy, the breach of personal identification can lead to identity theft, and subsequent financial losses for customers.
- Unauthorized payments or transactions made without the account holder's permission, can result from a data breach — especially if log-in credentials are accessed by untrusted parties — but also from errors in (or attacks to) the functioning of payment initiation services.
- Defective payments or transactions, requested by the customer but wrongly processed by the providers involved (due to mistaken amount or recipient, delayed timing or payment not executed) can also harm consumers if they are liable for charges from the intended payment recipients (e.g. providers or contractors of goods or services).

The risk of these potential customer damages varies significantly across open banking models and depends especially on two key features: (i) the services provided by the third parties, and (ii) the access or communication mechanism between the banks and the third parties.[1]

Firstly, the provision of payment initiation services involves not only retrieving customers' data (read-only access to bank accounts) but also transmitting transaction orders (write access), so this generally entails greater risks than data aggregation or account information services (see Figure 1). In addition, involving a third party in the chain transmitting a payment order between the customer and the bank actually holding the account can increase the risk of these orders not being transmitted correctly or in the appropriate amount of time. This becomes especially relevant if the initiator of a payment subsequently wants to reverse their initial transaction.

Secondly, third parties can access bank accounts either through the standard customer online banking interfaces — making use of so-called 'screen scraping' technologies — or through special dedicated interfaces, such as APIs.[2] In the former scenario, customers share with third parties their online banking log-in credentials, which increases the risk of customer damage in the event of a data breach.

Figure 1: Payment initiation services



Payment initiation services allow a third party to initiate wire transfers on behalf of a customer (i.e. mandate their bank to move funds from their account to another one). This possibility can fuel the provision of different types of payment services. Under the most basic one, the third party initiates the transfer of money directly from a payer's bank account to the bank account of the payee (e.g. a merchant or peer). In a version of this model, a merchant itself can become a third-party payment initiator and therefore mandate the customer/payer's bank to make the wire transfer to its own account.

On the other hand, payment initiation services can be used by payment institutions to allow customers to easily credit their own e-wallets, moving funds from their bank accounts to the escrow bank account of the payment institution (without using a debit or credit card in between). In this case, the third-party payment initiation is not used to make an end-to-end customer payment but to charge the e-wallets from which peer-to-peer to or merchant payments can then be made.

[1] For a more detailed explanation of the features of Open Banking frameworks in different jurisdictions, see the annex of the recent IIF paper 'Reciprocity in Customer Data Sharing Frameworks'.

[2] Screen or web scraping technologies mechanically extract data from human-readable websites for later automated use or analysis. On the other hand, APIs (Application Programming Interfaces) are a set of procedures that allow one software application or service to access the features or data of another application or service. Irrespective of the access mechanism, open banking services can either themselves perform the communication with the banks' systems or rely on third-party companies that specialize in establishing those connections, either through screen scraping or APIs.

2. MITIGATING OPERATIONAL RISKS

To protect consumers in open banking ecosystems, the identified risks need to be appropriately mitigated through sound operational risk management practices by all the players involved (i.e. banks and third parties) that address the security, business continuity and robustness of operations, both in the internal systems of the different parties and in the transmission or communication between them. This is particularly challenging in the case of third party players other than regulated financial institutions, who often lack the risk management frameworks that are common practice in the banking sector, with detailed policies, procedures and internal and external controls.[3]

This challenge is being addressed in different ways across jurisdictions, depending on whether their open banking ecosystems are more market-driven or regulatory-driven. On the one hand, in jurisdictions with no specific government intervention, such as the US or Singapore, bilateral agreements between banks and third-parties can set the conditions on the access to banks' APIs, including security and data protection requirements and other obligations for each party. However, in the absence of such agreements, access to bank accounts in unregulated environments generally takes place through 'screen-scraping' techniques, subject to no clear framework or external control on the third parties. This uncertainty, together with the exposure of personal log-in credentials, obviously increases all the aforementioned risks for consumers.

In other jurisdictions, such as Japan or Hong Kong, the authorities have developed general guidelines for open banking but rely on banks for the implementation of specific measures and controls. In Japan, since the amendment of the Banking Act in May 2017, banks are required to make public their policies and criteria for granting third parties access to accounts under bilateral agreements, that shall ensure the appropriate use and safeguarding of customer data.[4] Similarly, the Hong Kong Monetary Authority (HKMA) has established high-level principles for the governance of third-party service providers.[5]

Finally, in jurisdictions with mandatory open banking models, where banks are legally required to grant third parties access to bank accounts, this obligation is accompanied by a regulatory framework that sets a specific regime for the third parties. This is the case of the European Union, where the new Payment Services Directive (PSD2) and subsequent guidelines and standards set the authorization requirements for account information and payment initiation services, rules on the access to accounts and the provision of services, and liability conditions. Some key aspects of this relatively comprehensive framework are presented in Table 1.[6]

[3] For a detailed explanation of how the financial sector safeguards customers data, see the recent IIF paper 'Safeguarding Customer Data in the Financial Sector'.
[4] Given the high-level approach of the regulator, a private-sector initiative — the "Open API Promotion Study Group" — has recently published a draft model agreement.
[5] Banks are responsible for implementing onboarding checks, entering into bilateral contractual relationships with the third parties and conducting ongoing monitoring, based on a common baseline agreed by the industry. This baseline must address business and risk management issues such as the financial soundness of the third parties, the customer and data protection measures and the cybersecurity and IT controls. For a more detailed explanation, see the HKMA's document "Open API Framework for the Hong Kong Banking Sector".
[6] For further details, see the full text of the new EU Payment Services Directive (PSD2).

Table 1: EU Payment Services Directive (PSD2)

Authorization requirements for the third parties	• Governance arrangements and internal control mechanisms • Procedures to monitor, handle and follow up security incidents and security-related customer complaints • Processes to file, monitor, track and restrict access to sensitive payment data • Business continuity arrangements, including effective contingency plans • Security risk assessment and control and mitigation measures • Evidence that directors and persons responsible for the management are of good repute and possess appropriate knowledge • Professional indemnity insurance or some other comparable guarantee • *Only for payment initiation services:* evidence of an initial capital of at least EUR 50K
Rules on access to accounts and provision of third-party services	• Explicit customer consent • Limits on the access to, use and storage of customers data • Technical standards on authentication and communication, including mandatory strong customer authentication (i.e. two-factor authentication) • Limits on the access to accounts in case of unauthorized or fraudulent accesses • *Only for payment initiation services*: information for the payer and payee after the initiation of a payment order
Liability conditions	*Only for payment initiation services:* • In case of unauthorized, non-executed, defective or late executed payment transactions, the user shall obtain immediate refund from the account servicing payment service provider (i.e. the bank) and, then, if the payment initiation service provider is liable, this shall immediately compensate the bank • The burden shall be on the payment initiation service provider to prove that the payment order was received by the bank in accordance with PSD2 and that within its sphere of competence the transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency.

3. COMPENSATION AND DISPUTE RESOLUTION

In addition to sound operational risk management practices, protecting consumers in open banking ecosystems also requires adequate schemes to compensate them in the event of incidents or errors that lead to unauthorized transactions or defective payments. These schemes should have streamlined mechanisms to handle customers complaints and sufficient resources to deal with monetary reparations. This raises two key challenges due to the nature of open banking ecosystems. First, non-regulated financial institutions are generally not required to hold operational risk capital, and second, the involvement of different parties in the flow of data or in the initiation of transactions raises the issue of how to assign liabilities between the banks and the third parties, and how to resolve potential disputes between them. These challenges are being addressed in different ways across open banking models, depending specifically on whether they are more market-driven or regulatory-driven, in a similar way to the risk mitigation measures described in the Section 2.

In jurisdictions with no specific government intervention, such as the US, bilateral agreements between banks and third-parties can set the liabilities regime, including appropriate insurance or own resources and dispute resolution procedures. However, in the absence of such agreements and a dedicated dispute resolution mechanism, customers will usually have to rely solely on the respective civil liability framework in place. Should a customer suffer damages through an unauthorized transaction, it is considerably more difficult for them to seek damages under such frameworks.

As the plaintiff in such cases, it is not unusual that the customer must firstly identify where the parties involved might have made a mistake and try to hold the respective entity accountable, in a situation where the burden of proof is on them (for factors that are often outside the customer's reach, to which they must again first gain access). In a worst-case scenario, long-wielding and costly legal proceedings can follow. The difficulty of these proceedings, along with the costs and the uncertainty of success, can often lead to customers dropping their claim prematurely, even if it is well founded.

In jurisdictions with high-level regulatory principles but market-based governance, such as Japan and Hong Kong, the required bilateral agreements between banks and third parties must address the liability issue. In Hong Kong, the HKMA states that banks and third-party service providers should "define and agree a clear liability and settlement arrangement to protect customers in the cases of loss." In Japan, the industry has developed a draft model agreement that makes the third parties directly responsible for indemnifying their customers, but they may seek compensation from banks if those are liable.

On the other hand, in the regulatory-driven EU framework (see Box 2), PSD2 requires the third parties accessing bank accounts to hold professional indemnity insurance or some other comparable guarantee against potential liabilities, with a minimum monetary amount that depends on the type and size of activities.[7] In addition, payment initiation services shall also hold a minimum amount of capital. However, in case of unauthorized or defective transactions, banks are required to refund the customer first, and then receive compensation from the third parties if those are liable.

This raises the obvious concern around how to resolve potential disputes in the assignment of liabilities between banks and third parties. In this regard, the UK's Open Banking Standard (OBS) — which goes beyond PSD2 — has created a Dispute Management System (DMS) to handle requests, enquiries, complaints or disputes between account servicing providers (banks) and third-party providers (payment initiation and account information services). The DMS is a voluntary mechanism under which participants adhere to a code of best practices, including on how to handle cases at the first instance, and how those can be taken to mediation, adjudication or arbitration.[8]

But it also raises the issues of incentives, and perhaps moral hazard. The overall integrity and success of an open banking model needs for all market participants to apply the most robust security to their customers' data and finances, with a risk-conscious culture. They are greatly incentivized to do this if they are directly and explicitly subject to the potential for direct financial loss (and failing their customer) for failures in their own security. Relying on an intermediary to compensate the customer may weaken that incentive.

[7] For more details, see the EBA's "Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366 (PSD2)".

[8] For more details, see the OBS's code of best practice on "Dispute Management System (DMS) for ASPSPs and TPPs".

4. RECOMMENDATIONS

Protecting customers in open banking ecosystems requires a formal framework that appropriately mitigates the involved operational risks and provides redress to customers in case of unauthorized transactions or defective payments. This formal framework can take different forms depending on whether an open banking ecosystem is more market-led or regulatory-led, and therefore ruled by public or private governance arrangements, or a combination of both. However, even in mainly market-led environments, some regulatory guidance is desirable to provide certainty to the market and prevent the uncontrolled access to bank accounts by third parties.

A sound formal framework to protect users of open banking ecosystems should be based on the following pillars:

- Banks and third-party service providers undertake security, data protection and business continuity policies, procedures and controls that are consistent with these already in place in the financial sector and proportionate to the services provided and the information accessed. Security must be ensured both in the transmission and communication mechanisms and in the internal systems of the players.

- All parties hold adequate resources, whether in the form of operational risk capital, professional liability insurance or some equivalent guarantee, to deal with customer damages that result in financial losses. These resources should be related to the number of customers, the volume of operations and the type of services, being generally greater for payment initiation services than for data aggregation services.

- Customers have adequate channels to remit their complaints, and these are handled swiftly to quickly refund their accounts. This responsibility should lie first on the player (bank or third party) where the transaction took origin. Currently this is not the standard scenario in many open banking models, where banks are facing a responsibility that should be fairly shared across players. For instance, under PSD2, the responsibility lies always first on banks, even if the unauthorized transaction took its origin in the relationship between the user and the third-party.

- There are streamlined procedures to resolve potential disputes between all acting parties, including between financial institutions and third-party service providers when there is a disagreement over the responsibility of an unauthorized transaction or defective payment. Specific provisions should also contemplate the possibility of a player going out of business, and how liabilities are settled in such a scenario.

In addition to having a formal consumer protection framework, educating customers plays a critical role in open banking ecosystems, where they deal with a greater number of providers and more sophisticated products and service offerings. The narrative they have been rightly told to date — do not share your data, do not open yourself up to attack — is difficult to align with a market evolution based on opening data. In this new context, education must raise consumer awareness and understanding of what they are doing with their data, the functioning of consent mechanisms and the risks and benefits of the new products and services. Financial institutions, third parties and regulators can all play an important role in educating consumers (e.g. by displaying safety notices and guidelines).

Protecting and educating customers is essential to gain their trust, and this is a prerequisite for the successful development of open banking ecosystems. Otherwise, the potential of open banking could be undermined if customers are exposed to new risks of fraud and scams, and to products and services that do not meet the highest standards of quality and consumer protection.

Brad Carr
Senior Director, Digital Finance Regulation and Policy
bcarr@iif.com

Pablo Urbiola
Policy Advisor
purbiola@iif.com

Adrien Delle-Case
Policy Advisor
adellecase@iif.com