Advances in Social Science, Education and Humanities Research, volume 517
Proceedings of the 6th Annual International Conference on Social Science and Contemporary Humanity Development (SSCHD 2020)

Unauthorized Transactions and Unintended Transactions in Open Banking:
Loss Allocation Based on Predictably Irrational Customers

Junqi Wang[1,*] and Duwei Deng[2]

[1]*Jiluan Academy, Nanchang University, China*
[2]*Faculty of Public Administration, Nanchang University, China*
[*]*Corresponding author. Email: 7701119002@email.ncu.edu.cn*

ABSTRACT
Open Banking allows for faster data flow data to flow faster and more widely. At the same time, a variety of risks have emerged as a result. This paper examines two major types of risk: unauthorized transactions and unintended transactions, both of which take place when consumers provide authorization for and confirm transactions. Although many safeguards have been adopted to ensure the safety of a transaction, existing surveys show that the effectiveness of these safeguards is not satisfactory. Through theoretical analysis and experimental report, this paper will demonstrate an important concept called "predictable irrationality", explaining why the problem is still unresolved despite the presence of a large number of protective safeguards. Irrationality exposes consumers to greater risks, especially in the context of open banking; it makes consumers unable to fully realize the consequences of their authorizations, which potentially leads to the occurrence of unintended transactions. To reduce this risk, this paper first puts forward suggestions for all aspects of authorization. However, considering that procedural suggestions alone cannot effectively address this risk, this paper also puts forward suggestions for the current legislative model as well. It is the hope that more effective safeguards can be adopted at the authorization stage and a more reasonable loss allocation principle can be applied after loss happens to reduce the two major types of risk and protect the interests of customers.

Keywords: *Open banking, Unauthorized transaction, Unintended transaction, Loss allocation.*

1. INTRODUCTION

Case 1: *A malicious actor managed to access a customer's log-in credentials and take control of their account. They used this account to initiate a transaction through a third-party company for their own interests.*

Case 2: *A company provides services for managing bank accounts and selling aggregated data to other companies. The company's 2000+ word "plain English" privacy policy includes a statement which states that the company "may collect and use your commercial data to build anonymous market research products". Customers gave their informed consent for the management of their bank accounts without fully understanding they had consented to both the primary service as well as the secondary data analysis for additional, market research products. However, the company still used the data it obtained for unlawful means.*

In *Bank 4.0*, Brett King notes that due to the current trend of Fintech (financial technology), banking's pattern is changing rapidly and dramatically, transforming into Bank 4.0 – "Banking is everywhere, never at a bank" (King, 2018).

One of the most significant technological developments in banking to occur in recent times is open banking.

In September 2014, the UK government delivered a report titled "Data Sharing and Open Data for Banks," which was written by ODI and Fingleton Associates to improve competition in retail banking and financial services (Open Data Institute & Fingleton Associates, 2014). In 2015, the Open Banking Working Group (OBWG) was established by the Competition and Markets Authority (CMA) to lead the Open Banking Initiative, and the OBWG's Open Banking Standard was published in 2016. That same year, the European

Copyright © 2021 The Authors. Published by Atlantis Press SARL.
This is an open access article distributed under the CC BY-NC 4.0 license -http://creativecommons.org/licenses/by-nc/4.0/.

Union passed Payment Service Directive 2 (PSD2) (When talking about Open Banking, you will often hear references to PSD2. However, it is important to note that they are not exactly the same. In simpler terms, PSD2 is a regulation which allows projects such as open banking to take place and PSD2 goes further than open banking, so it makes sense that this paper uses similar concepts in following arguments.), which urged European banks to make customer data available to third parties. Besides, the EU's General Data Protection Regulation (GDPR), which came into force in 2018, is the basis for the EU's push towards open banking. At the same time, in 2017, the U.S Consumer Financial Protection Bureau (CFPB) released *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* for the sharing of financial data.

The industry has not yet agreed upon a unified definition for what an open bank is. Open banking is a new type of banking. According to PSD2, its services can be generally divided into two types: payment initiation services (PIS) and account information services (AIS) (PSD2, Article 4, (15)-(16)).

Individual customers, banks and third parties establish their own contractual relationships. Individual customers (data subject) first sign a customer service agreement with the bank (data controller. Based on this service agreement, banks then collect the customer's data through corresponding services, and as the data controller, they should assume responsibility for data security. Third parties (data users) reasonably use the data and fulfil the obligation of information disclosure to the extent which is permitted by law and authorized by the customer.

2. UNAUTHORIZED TRANSACTIONS AND UNINTENDED TRANSACTIONS IN OPEN BANKING

Having discussed the basics of open banking, in the context of third-party intervention, data flow is much more flexible and swift. Undoubtedly, in an environment where data is much more open and everything is novel, the major areas of risk for open banking ecosystem users are as follows (Institution of international finance, 2018)(The classification adopted in this paper is basically consistent with its viewpoints, but has made some modifications (the addition of unintended transactions) for the purpose of argument.):

Data breaches: unintentional leaks or external attacks may expose sensitive information, including financial transactions and balances, bank account numbers or even online banking log-in credentials

Unauthorized transactions made without an account holder's authorization can be the result of a data breach – particularly if untrustworthy parties manage to access log-in information, though errors in (or attacks to) the functioning of PIS can also be the cause. (Case 1)

Unintended transactions made with an account holder's authorization are seemingly valid. In fact, due to some complicated factors, customers aren't aware of the meaning or consequences of giving such consent. (Case 2)

Defective transactions requested by a customer but which are mistakenly processed by the providers involved can also harm consumers when they are liable for charges from the intended recipients of payments.

Such problems are undoubtedly important to address and require further discussion, including data breaches (TLT's Financial Services team, 2018) and defective transactions (Australian Government, 2018). This paper chooses to focus on unauthorized transactions and unintended transactions as the subjects of discussion.

There are two additions to the definitions put forth in this paper:

1. In general, transactions tend to flow with money, but in the context of open banking, there is a significant increase in the data flow, such as a large number of AIS services. Therefore, the transaction extension of this paper will be expanded to include the exchange of data.

2. It is undeniable that many transactions conform to the above definition in form, but will not bring losses to consumers in essence. For example, a third party could simply use the data scale value of consumers to do something that will not cause any harm, such as data analysis and advertising. This paper deals only with situations where there is a real cost to the consumer (monetary or otherwise).

2.1. The Necessity of the Two Types Being Discussed in Parallel

To argue the necessity of these two types of transactions being discussed together, we must first establish the meaning of authorization, which is: the "official permission for something to happen, or the act of giving someone official permission to do something." (In an open banking context, the meaning of the words "consent" and "authorization" are similar. When referring to a transaction's characteristic, "authorization" is most often used; when referring to customers' actions, "consent" is most often used. In the following discussion, both words are used to better fit the original context.)

Taking into account open banking's operation process and the relationship between participants, this paper defines authorization as: "customers providing official permission to third parties to access to their data."

When a banking service is embedded into a business scenario by an API interface, the third-party accesses the customer's personal data through it, and the customer invokes their personal data stored at the bank through the API designed and operated by the third party. During this process, the API interface is analogous to a valve, and data flows through this valve to a third party. In conclusion, open banking services are allowed to process personal data as customers have provided their consent for it to be used by a relevant online service (London School of Economics and Political Science, 2018).

Recognizing the importance of authorization, these two types of risk are discussed together for later comparison. They are all problems which occur at the authorization stage (Some readers may have doubts such as to why there are only two possibilities. Realistically, we cannot feasibly list all possibilities, but this paper holds the view that there are two typical risks which can occur during the authorization stage. Unauthorized transactions are mainly caused by external factors; unintended transactions are mainly the result of internal factors (irrationality).): one is caused by information leakage, meaning that authorization was not given by the customers themselves; the other is the result of a customer's inability to properly understand their authorization behaviour.

3. SAFEGUARDS TAKEN TO GUARANTEE VALID TRANSACTIONS

To allow for safe and secure operation in open banking, authorities have issued a number of documents which established several mechanisms for guaranteeing valid transactions.

Smart Data: To give consumers control of their data and enable innovation (HM Government, 2019), the HM government regulates that:

TPPs should only be able to access consumer data once explicit consent has been provided and their identity has been verified by a secure authentication process.

General Data Protection Regulation (GDPR) (It is of note that there is no direct relationship between GDPR and open banking, as is the case with the previous PSD2, one is at the European Union level and the other is at the UK level. At heart, both regulations are concerned with customers having greater control of their data, and that data should only be used to support the customer's interests. Therefore, the requirements of consent for GDPR are used to clarify the standards of a valid consent.)further expands upon the requirements of consent to be: ***unambiguous, informed and freely given*** (GDPR, Article 4(11)).

Detailed explanations are also provided (Wolford, 2019), for instance, "**Unambiguous**: the consent should be made clear what type of data processing activities will be conducted, and the subject should be granted an opportunity to consent to each individual activity."

To guarantee its validity, two stages are also mentioned in some complementary documents (The European Parliament and the Council, 2018) for safety purposes:

1. The controller explains that he asks for consent for the use of a specific set of information for a specific purpose. If data subjects agree to the use of their data, the controller asks them for an email reply which contains the statement 'I agree'.

2. Once the reply is sent, the data subject receives a verification link which must be clicked, or an SMS message with a verification code, to confirm the agreement.

The regulations at first glance appear to be detailed enough to guarantee the validity of authorization. However, most existing empirical studies have discovered that individuals who consent to services which process their personal data often do so ineffectively, unaware of what exactly they have explicitly consented to (Data on unauthorized transactions is not available on the Internet. This paper assumes that the security of transactions in the context of open banking has been guaranteed, regardless of whether or not it is safe, but there are still some problems which will be discussed later.).

One recent study on open banking conducted by the Financial Services Consumer Panel, a UK member of the BEUC, showed that consumers are not providing informed consent when sharing their financial data. Most people do not read the terms and conditions or understand them even when they do. It was found that terms and conditions are too long and complicated, full of legal jargon and "not written with consumers in mind" (The Financial Services Consumer Panel, 2018).

Another recent study, conducted by a European Consumer Organization (BEUC) German member, *Verbraucherzentrale Bundesverband* (vzbv), reached a similar conclusion. The survey assessed what consumers thought they were consenting to with e-payment providers, based on their knowledge of the terms and conditions (vzbv, 2018).

4. DIFFICULTY IN MAKING A FULLY AUTHORIZED TRANSACTION – PREDICTABLE IRRATIONALITY

In order to explain this dilemma, this paper will draw on the important reason behind "predictable irrationality". As is already widely known, the basic hypothesis of economics is "rationale people" – one

who is sensible and able to make decisions based on intelligent thinking rather than emotion. This definition has been the pillar of classical economics.

However, after the 1980s, economists led by Richard Thaler took cues from evolutionary psychology, that most people are neither perfectly rational nor entirely selfish, but due to limited time and cognitive resources, they become inclined to make bounded decisions which are not objectively the most rational (Jolls, Sunstein, & Thaler, 1998). Based on this theory, behavioural economics, which is devoted to the study of irrational human behaviour, was established. The field of behavioural economics has made great contributions to our understanding of human decision making by refining neoclassical assumptions and developing models which account for psychological, cognitive, and emotional forces. The insights of this field have important legal implications (Joshua & Zeiler, 2003).

As with classical economics, the law is based on rational people and its inner mechanism is comprehensive. However, in an open banking context, the foundations of human nature can be shaken. The likelihood is high that third parties could create a complex environment to affect the decision-making of customers for the sake of more profit as a significant number of customers are unaware of what they are doing, or what the value of their data due to asymmetric information or limited knowledge when faced with a complicated context. These people can be regarded as "irrational people".

This paper argues that when it comes to open banking, customers are often irrational to a certain extent:

1. Today's online fraud methods are much more unpredictable. It can even be impossible for customers to prevent malicious parties using their identities to create false authorizations in the digital arena. Data sharing is inevitable to a certain extent, and private information may be seen by others, but this is not an excuse for outright refusing data sharing.

2. Furthermore, the progress of big data and blockchain technology has made data processing methods more professional and complex. Even if customers carefully read the relevant clauses, they will be unable to accurately understand the contents due to a limitation of professional knowledge, which thereby affects their risk assessment.

3. Due to privacy policy clauses being excessively wordy, and because of the current fragmented reading prevalence on the Internet, many customers do not have the patience or even the ability to read long passages of text.

4. In addition, how a bank performs its obligation of offering full explanation and presentation is quite perfunctory, making it difficult for individual customers to know exactly which clauses relate to their own vital interests.

As a result, customers can often not fully understand the terms, and the likelihood of consenting to the use of an online service is contingent upon social forces and the reputation of the service rather than an intentional act of human agency as a service may appear more acceptable if many people are already using it (London School of Economics and Political Science, 2018).

In order to mitigate the impact of this irrationality, the following safeguards must be taken prior to authorization:

Recommendation 1: Financial institutions or third parties should increase the number of authorization methods, rather than limiting it to digital passwords. Personality-dependent modes of authorization, such as a combination of audio and visual authorization, should be added, as they cannot easily be imitated or stolen.

Recommendation 2: Consumer consent should be explicit: 'by ticking this box, I agree that company "XXX" will have access to the following financial data (list data for which the access is being requested) managed by the ASPSPs (bank) "YYY" (The European Consumer Organization, 2018***).***

Recommendation 3: Adding additional delays to enable a more informed and thoughtful consent process would help customers think more about the consent they give (London School of Economics and Political Science, 2018***).***

5. LOSS ALLOCATION BASED ON THE LOSS CAUSED BY DIFFERENT TYPES OF UNAUTHORIZED TRANSACTIONS

Obviously, the present problem cannot be resolved immediately and completely in this manner. Irrational consumers are largely unable to offer effective authorization, which may have consequences that are different from the expected. Taking Cases 1 and 2 as examples, Case 1 resulted in direct monetary loss, as a transaction was initiated; the loss in Case 2 is uncertain, but even with the unseen loss, it is difficult to know what the company would do or if it would simply share customers' data with others, the value of which cannot be calculated directly.

In this situation, in order for the relevant loss allocation rules to apply, we must first consider the different loss types.

According to the property nature of the loss, this paper divides the loss into two categories: pecuniary losses and non-pecuniary losses. Pecuniary losses refer to losses which are simply quantifiable. They can be

measured in financial terms, such as by a decrease in the amount of money in the holder's account. Non-pecuniary losses cannot be clearly quantified in monetary terms. They are often difficult to measure as the costs are more subjective and not straightforward. In the context of open banking, the value of data or the value of personality and identity interests hidden beneath the data are important, but they are not quantifiable, so when we want to talk about loss allocation principles, we may need to provide an artificial standard for quantification. Therefore, in this paper, while non-pecuniary losses are not the key point, we also hope that this question will prompt scholars to investigate further and make breakthroughs (Lahe & Kull, 2016).

Next, this paper explores the principle of loss allocation in unauthorized transactions and unintended transactions, which will be analyzed separately.

5.1. Type 1: Unauthorized Transactions

Currently, the rules on unauthorized transactions in mainstream areas are generally similar in many aspects, as they are in the United States, the United Kingdom and the European Union. They all set a liability cap (Cooter & Rubin, 1987) ("One possible liability cap would be the median amount of cash withdrawn by consumers when they go to their bank, which is currently about eighty dollars." the paper guesses owing to Professors Cooter and Rubin's credit.), for example, in the U.S. the cap is $50 (Electronic Fund Transfer Act and the Regulation E, Section 205.6), and in the European Union, the cap is EUR 50(Payment Service Directive 2, Article 74, § 1).

The condition of the exemption is generally limited in such cases to "loss or theft of an access device" (Id, at Section 205.6) or "the misappropriation of a payment instrument" (Id, at Article 74, § 1). There is no doubt that the unauthorized use of customers' funds constitutes infringement and the customers should be entitled to compensation. The tort liability is mainly insistent upon fault liability. Fault liability is a type of liability whereby the plaintiff must prove the defendant's conduct to be either negligent or intentional. Apparently, an efficient open banking liability system must make it clear that open banking participants are liable for their own conduct, but not the conduct of other participants (Australian Government, 2017).

When such transactions occur, it is often difficult to catch the infringer as finding someone through online data alone is not easy, and even if they are caught, there is often no compensation for the loss. The current core issue is whether the financial institution, third parties or cardholder should bear the losses of unauthorized transactions.

When considering the irrationality of customers in relation to the other parties or shared fault (it is difficult to define exactly whose actions causes the unintended consequences), according to the current mainstream legislative model, customers should apply for a "capped consumer liability". In PSD2 (Id, at Article 73, § 2), financial institutions shall provide an immediate refund to customers, and if a third party is liable for any unauthorized payment transaction, it shall immediately compensate the financial institution at its request.

It is of note that this method of loss distribution has proven to be relatively beneficial for consumer protection, and the discussion should have ended here. However, we believe that some problems remain within these rules: How does a financial institution request compensation from a third party which is at fault? How are their losses distributed? What if the TPP claims it is not liable and the bank also believes that it is not at fault? These are all problems which require consideration (Solicitors regulation authority, 2018).

5.2. Type 2: Unintended Transactions

In Case 2 and the research mentioned above, customers are largely unable to make a fully effective authorization transaction, as they do not understand the mechanism behind open banking, and generally just provide direct consent. As previously discussed, many solutions have been attempted for guaranteeing valid consent, so the mainstream international legislation for unauthorized transactions is generally limited to the first case (Type 1). Consent which is based on irrational context is not applicable in the exemption clause. In other words, such a transaction is generally consistent with a valid authorized transaction.

The three parties involved form a contractual relationship. In the common law system, contractual liability insists on strict liability. In civil law, strict liability is a standard of liability under which a person is legally responsible for the consequences of an activity, even in the absence of fault on their part.

Giving customers strict liability, due to the supposedly secret nature of digital authorization, appears to improve customers' level of caution. However, considering the characteristics of customers, there are two major defects in this arrangement: information asymmetry and predictable irrationality.

An individual user of a bank has limited experience in banking and even less understanding of the bank's technical aspects. At the same time, considering a person's bounded rationality, their level of caution is limited. Once a certain level of caution is reached, regardless of how hard a person tries, their level of caution cannot be improved, as they do not possess the knowledge to understand this aspect.

Recommendation: Therefore, this paper believes that if such a situation were to occur again, the liability cap should also be applied to offer customers greater protection, which could also prompt participants to simplify their terms (if the terms of authorization meet the formatting requirements mentioned above, consent should be presumed to be valid).

6. CONCLUSIONS

The paper believes that consumers' irrationality results in many authorizations that not made by themselves or based on their own free will. Therefore, to solve this problem to a certain extent, this paper provides two complementary ideas: the first is to increase the diversity of authorization methods or increase the thinking time of authorization, so as to reduce the risk to a minimum in the authorization stage; the second is that authorizations which lead to unintended consequences, based on unclear authorization terms, should not be applicable to strict liability for the sake of customer protection.

REFERENCES

[1] King, B. (2018). *Bank 4.0*. Marshall Cavendish Business, Singapore

[2] Open Data Institute and Fingleton Associates. (2014). *Data Sharing and Open Data for Banks*, p.11.

[3] Institution of International Finance. (2018). *Liability and Consumer Protection in Open Banking*, p.1.

[4] TLT's Financial Services team. (2018). *Opportunity Knocks - The future of Open Banking*, pp.5-8. Available: https://www.tltsolicitors.com/insights-and-events/publications/open-banking-opportunity-knocks/

[5] Australian Government. (2017). *Review into Open Banking: giving customers choice, convenience and confidence*. (ISBN 978-1-925504-72-9), p. 69.

[6] London School of Economics and Political Science. (2018). *Report on a study of how consumers currently consent to share their financial data with a third party*, p.4, p.10, pp. 11-12.

[7] HM Government. (2019). *Smart Data: Putting consumers in control of their data and enabling innovation*, p.29.

[8] Wolford, B. (2019). *What are the GDPR consent requirements?* Available: https://gdpr.eu/gdpr-consent-requirements/

[9] European Parliament and Council. (2018). *Article 29 Working Party Guidelines on consent under Regulation 2016/679,2018*, p.19.

[10] Financial Services Consumer Panel. (2018). *FSCP position paper and recommendations*. Available: https://www.fs-cp.org.uk/press-release-consenting-adults-consumers-sharing-their-financial-data

[11] Vzbv. (2018). *FSCP position paper and recommendations*. Available: https://ssl.marktwaechter.de/digitalewelt/marktbeobachtung/e-paymentwie-sicher-sind-unsere-datenbeimbezahlen-im-netz

[12] Jolls, C., Sunstein, C., & Thaler, R. (1998). *A Behavioral Approach to Law and Economics*. Stanford Law Review, Vol. 50:1471.

[13] Teitelbaum J. & Zeiler, K. (2003). *Research Handbook on Behavioral Law and Economics.* Princeton University Press, U.S. p1-2.

[14] European Consumer Organization. (2018). *Consumer-Friendly Open Banking Access to Consumers' Financial Data by Third Parties*, p.7.

[15] Lahe, J. & Kull, I (1987). *Compensation of non-pecuniary damage to persons close to the deceased or to the aggrieved person*. International Comparative Jurisprudence, Volume 2, Issue 1, 2016, pp. 1-7.

[16] Cooter, R. & Rubin, E. L. (1987. *Theory of Loss Allocation for Consumer Payments*, p. 92. Texas Law Review, Vol. 66:63.

[17] Solicitors Regulation Authority. (2018). *Open Banking, Open Liability: accountability issues for open banking APIs*. Available: https://www.ashurst.com/en/news-and-insights/legal-updates/open-banking-open-liability-accountability-issues-for-open-banking-apis/