

STUDY

Requested by the ECON committee



What are the wider supervisory implications of the Wirecard case?



External authors:

Giorgio BARBA NAVARETTI

Giacomo CALZOLARI

Alberto Franco POZZOLO



Economic Governance Support Unit (EGOV)
Directorate-General for Internal Policies
PE 651.384 - October 2020

EN

What are the wider supervisory implications of the Wirecard case?

Abstract

Beginning with a discussion of the Wirecard case, this study highlights several lessons for the regulation and supervision of Fintech companies. Innovation in the financial industry brings both efficiency gains and new risks. To balance these two elements, regulators need a deep understanding of Fintech's technologies and business models. Because Fintechs can be very complex companies, there is a need for an approach combining the oversight of both entities and activities. The global scope of Fintech's activities also calls for convergence and coordination of rules and supervisory practices at the European level and beyond.

This document was requested by the European Parliament's Committee on Economic and Monetary Affairs.

AUTHORS

Giorgio BARBA NAVARETTI, University of Milan, Department of Economics, Italy
Giacomo CALZOLARI, European University Institute, Department of Economics, Italy
Alberto Franco POZZOLO, University of Roma Tre, Department of Law, Italy

ADMINISTRATORS RESPONSIBLE

Cristina DIAS
Kristina GRIGAITĖ
Rebecca SEGALL
Marcel MAGNUS

EDITORIAL ASSISTANT

Donella BOLDI

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

The Economic Governance Support Unit provides in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact Economic Governance Support Unit or to subscribe to its newsletter please write to:
Economic Governance Support Unit
European Parliament
B-1047 Brussels
E-mail: egov@ep.europa.eu

Manuscript completed in May 2020
© European Union, 2020

This document and other supporting analyses are available on the internet at:
<http://www.europarl.europa.eu/supporting-analyses>

DISCLAIMER AND COPYRIGHT

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.
Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

CONTENTS

LIST OF ABBREVIATIONS	6
LIST OF BOXES	7
LIST OF FIGURES	7
EXECUTIVE SUMMARY	8
1. INTRODUCTION WIRECARD AND FINTECH	11
2. THE COMPLEXITY OF FINTECH FIRMS AND THE OBJECTIVES OF FINANCIAL REGULATION AND SUPERVISION	16
2.1. Complexity in financial intermediation and Fintech	16
2.2. Supervising complex financial intermediaries	17
2.2.1. The objectives of financial supervision: investor protection	18
2.2.2. The objectives of financial supervision: customer protection	20
2.2.3. The objectives of financial supervision: financial stability	22
3. REGULATION AND SUPERVISION OF FINTECH	23
3.1. Regulation and Supervision: from entities to activities	24
3.1.1. From “comfort zone” to uncharted territories	24
3.2. The risks of compartmentalising Regulation and Supervision: entities vs. activities	25
3.3. “Know the technology”	27
3.3.1. Artificial Intelligence and Supervision	27
3.3.2. Technology for Regulation and Supervision: RegTech and SupTech	29
3.4. “Know the business model”	30
3.4.1. Regulatory Sandboxes	32
3.5. “Know the global picture: International cooperation”	32
CONCLUSION	34
REFERENCES	35

LIST OF ABBREVIATIONS

AI	Artificial intelligence
API	Application Programme Interface
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities and Markets Authority
EY	Ernst and Young GMBH
FREP	Financial Reporting Enforcement Panel
FSB	Financial Stability Board
FT	Financial Times
ICT	Information and Communication Technology
MAS	Monetary Authority of Singapore
ML	Machine learning

LIST OF BOXES

Box 1: Definitions: Fintech and technologies	11
Box 2: Exemplary of most common types of Fintech by activity	17
Box 3: Types of Fintech by business type	25

LIST OF FIGURES

Figure 1: Credit card payments	13
--------------------------------	----

EXECUTIVE SUMMARY

Although the case of Wirecard appears to be an accounting fraud of the more classical type, many lessons can be drawn for the design of Fintech regulation and supervision. To some extent, the inability of the authorities to detect such a misconduct in a prominent and well-known company is the result of regulatory loopholes, which may leave room for future transgressions.

There was no comprehensive and integrated oversight of Wirecard activities, both in terms of lines of business and geography of its operations. There was neither an adequate vetting of its accounting practices, nor an effective oversight and enforcement of accounting and auditing practices. Probably this was possible also due to a generally inadequate understanding of the business model and of the technology of Wirecard. Because of its status as a high-tech Fintech company, Wirecard was left to operate under a veil of regulatory ignorance, with no effective challenge to the viability of its business model. Also, the geographical span of its operations, frequently carried out through third parties and under different regulatory and supervisory regimes, made the oversight of its activities even looser. At the same time, Wirecard could also pass the hurdle of the scrutiny of large investors and banks, which provided massive funding to its operations.

The complexity of Fintech companies, their technologies and the broad span of their operations, both in terms of bundled services and geographical scope, raise concerns for both investor and customer protection, as well as for financial stability, as discussed at length in this briefing paper.

In general terms, there is a growing need to balance the efficiency gains of technological innovation in the financial industry with possible additional risks for its stakeholders. Regulation and supervision must be effective but, at the same time, they must not stifle innovation in the financial industry. This briefing paper makes a number of proposals and identifies few clear “imperatives” to address “the new challenges and risks associated with the digital transformation” – one of the four key priorities of the Digital Finance Strategy for the EU recently published by the European Commission (EU Commission, 2020a-c) and to address the concerns and resolution on digital finance put forward by the European Parliament (2020):

1. *Avoid regulatory arbitrage.* Cover uncharted territories when businesses are running ahead of regulators, and ensure a level playing field between Fintech companies and traditional businesses. Make sure that entities carrying the same activity follow the same sets of rules, however they carry them out (e.g., providing credit through on-line credit platforms or traditional banks).
2. *Understand clearly what Fintechs do and what their business models are.* Regulators need to understand the potential enhancing or disruptive impact of Fintech activities and how they interact with other parts of financial and non-financial markets. Sandboxes – well identified, temporary and light regulatory frameworks for new experimental products, lines of business or technologies – are useful in this respect, as far as they do not create unhealthy links between the regulators and the regulated.
3. *Combine the oversight of entities with the oversight of activities.* On the one hand, unbundled financial activities should be supervised independently of the form of incorporation adopted by the company and of the other activities that it performs in parallel.¹ On the other hand, just focusing on regulating and supervising activities generates a significant risk of compartmentalising the oversight of financial markets. The Wirecard lesson is that a partial oversight of an entity may create substantial regulatory loopholes. These loopholes may especially emerge for companies like Wirecard, with a complex and

¹ According to EBA 2017, more than 30% of online payment services are unregulated.

intricate web of activities, unbundling part of their services to third parties in different countries (e.g. third party acquirers in Asia), carrying out their operations through independent entities within the group in different lines of business, under different regulatory and supervisory regimes (e.g. Wirecard AG, the holding, considered as a technology non-financial company, and Wirecard Bank in Germany) and carrying out services for financial clients based again in many different countries (e.g. small banks or other Fintechs). Although supervisory failures in the Wirecard case were mostly in the domain of accounting enforcement and thus of investor protection, loopholes may emerge in all regulatory domains, pertaining to customer protection, investor protection and financial stability. In this respect, we do share the underlying rationale of the proposal of the European Commission (European Commission, 2020a), which grants adequate oversight powers with respect to technological third-party providers, also within the same group. This approach overcomes the problem of the identification of financial conglomerates with the right of oversight just depending on the actual risks that technology companies or activities may cause on financial intermediation.

4. *Master the technology used by Fintechs.* At the core of Fintech expansion there are a set of relatively recent technologies that allow for better information extraction from data, often classified under the hat of Artificial Intelligence (AI), and the use of a massive amount of data – Bigdata – that can be effectively exploited with AI. It should be clear that technologies are only tools to perform standard financial activities that up to now were carried out with other means. Although one can never understate the impressive efficiency that AI algorithms can bring to financial markets, any hype about AI and its applications should be avoided. Most important, for a safe use of AI in financial markets, supervisors and regulators must have the ability to monitor and assess the actual behavior and functioning of these algorithms. They must develop and acquire technological competences, to avoid losing sight of the true business model of the entities supervised, as it seems to have happened in the Wirecard case. Regtech and Suptech are interesting developments in this respect, but although they will certainly complement the activity of regulation and supervision of financial markets, they cannot completely substitute more traditional approaches.

5. *Know the global picture and harmonise and coordinate internationally rules and oversight of Fintechs.* Fintech players, especially those unbundling and specialising in narrow segments, have shown a natural tendency for cross-border activities. This is expected, since with specialisation firms need to tap new markets rather than new businesses. This broad span of the geography of business activities calls for a coordinated action of regulators and supervisors, certainly in Europe, hopefully more broadly. The case of Wirecard highlights how crucial this issue is. The global reach of the company was significant, with the obvious problem that in the payment systems we lack unified supervision and different national standards apply, for example, on the interoperability of enabling technologies. When a Fintech player in this business outsources part of its activities to a third-party, national supervisors have access to information about these external operators only if they are located within national boundaries. As soon as these activities take place cross-border, they become almost impossible to scrutinise in a unified way. Solutions to the issue of lack of coordination and harmonised standards are necessary, although not easy to find. The effort that is normally required is significant, but not impossible, especially in situations of crisis, as the case of Banking Union has shown. We see this process of harmonisation and coordination, in the case of Europe, as a necessary ingredient of the Capital Market Union.

6. *No need for a new regulatory agency, rather we need coordination among national competent authorities.* We do not believe that there is a need for a new regulatory body overseeing Fintechs. The regulatory loopholes emerging from the Wirecard case are to a large extent independent from the fact that the business was Fintech. Certainly, IT and AI technologies increase the complexity and the

intricacy of business activities and of new initiatives in unchartered areas. Also, they may induce supervisory indulgence under a veil of ignorance. Nonetheless this can happen in newly created Fintechs or also with the introduction of Fintech activities in traditional businesses. The objectives of regulation remain the same, investors' and consumers' protection and financial stability, whether operations are carried out by Fintechs, traditional businesses or a blend of the two. Fintech players and the Wirecard case do not provide, in our view, a compelling justification for such a new European Authority. In each of the key areas, investor protection, customer protection and financial stability, European authorities, EBA and ESMA may be put in the position of indicating harmonised and coordinated framework for Fintech across Europe, which will then be exercised by national competent authorities.

1. INTRODUCTION WIRECARD AND FINTECH

The bankruptcy of Wirecard raised many issues on the lack of an adequate regulatory framework and of supervisory actions overseeing its activities. It also raised the broader issue (hence this study) of whether the failure by the authorities to detect a fraud of such an extent in such a prominent and well known business is in particular related to Wirecard being a “Fintech”, using innovative technologies to carry out its activities and to bundle (and at the same time unbundle, as we will see later) several services. See Box 1 for a definition of Fintech and associated innovative technologies.

Box 1: Definitions: Fintech and technologies

Fintech is ‘technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services’. (FSB 2019)

See also <http://www.fsb.org/what-we-do/policy-development/additional-policy-areas/monitoring-of-fintech/>.

Innovative technologies in financial markets

Although it is difficult to systematically identify technological innovations that are relevant for financial markets, the following is a list of the most important ones. Section 3.3.1 further develops some of these with additional details.

Artificial Intelligence (AI) refers to a broad area, in computer science, but not only, that develops and provides systems able to perform tasks that traditionally require human intelligence.

Machine Learning (ML), a form of AI, is a collection of methods and algorithms that are designed to solve specific problems (e.g. classification and prediction) and that improve with experience, with limited or no human intervention.

Cloud computing is a system that allows on-demand use of computing capability such as, processing and data storage, that is hosted online by cloud providers. It allows increasing the scale and flexibility of computing capacity.

Application Programme Interfaces (APIs) are set of rules and interfaces for communication and interaction between different software programmes that allow for a more flexible solution to specific applications involving several software intermediaries.

Source: Authors’ analysis.

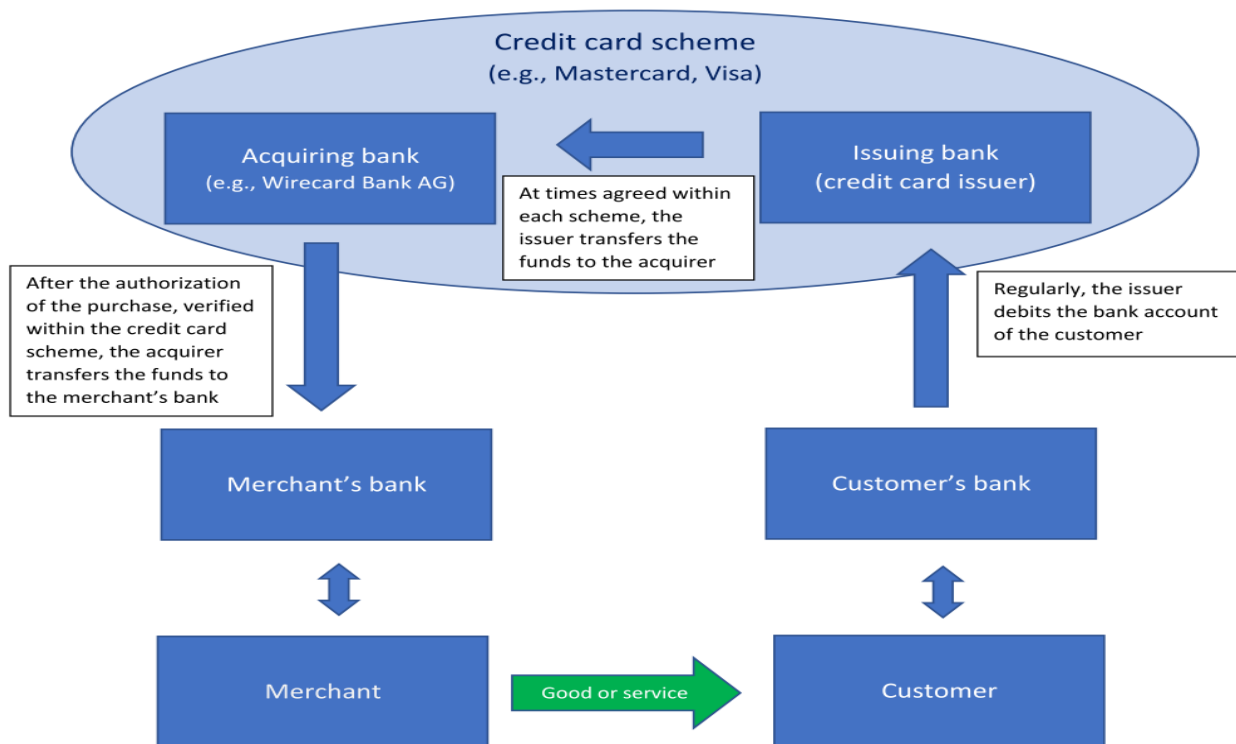
In its official narrative, technology was at the core of Wirecard business model. “*The Wirecard is a global technology group that supports its customers and partners in accepting electronic payments from all sales channels and also in the issuing of payment instruments. (...) The uniform platform approach and seamlessly integrated value added services such as data analytics, customers loyalty programmes and digital banking services support customers and partners of Wirecard to successfully master the challenge of digitalisation*” (Wirecard, Annual report 2018). In 2018, three quarters of its total revenues (€ 2,016.2 million) were generated by its payment and risk management and another quarter by its acquiring and issuing business. In essence, Wirecard processed payments and provided infrastructure and services for payments.

More specifically, Wirecard acted as an acquirer of payment transactions (most of them online), operating as an intermediary between merchants and their banks, on the one hand, and customers, their card issuers and their banks, on the other (See Figure 1 for a simple representation of card based payment transactions). According to the European Securities and Markets Authority (ESMA) (2019) (see also Zeranski and Sancak, 2020) Wirecard “connected to more than 200 international payment networks (banks, payment solutions, card networks), which resulted in 34,000 customers from various industries, and offered its services in over 100 transaction currencies”. In many countries, it operated directly with licensed subsidiaries, e.g. Wirecard Bank AG in Germany. In other countries, it operated through supposedly independent licensed third-party acquirers (mostly in Asia).

Its operations were supported by online platforms and a technological framework, which, according to Wirecard’s claims, were instrumental in implementing an effective risk management of a complex network of payment transactions. But, overall, the type of activities carried out were pretty standard routine payment services. In this respect, given publicly available information so far, Wirecard appears to be a case of standard accounting fraud (which makes its being undetected for so long even more surprising), with little to do with the alleged technological complexity of its operations. In other words, Wirecard’s bankruptcy did not happen because of undetected problems or mismanagement of the technology. Rather, the Fintech status created a screen of presumed complexity, a possible diversion for the supervisors, and, as we will see below, a fragmented supervisory framework, in a company that already in itself had a pretty intricate web of activities and operations worldwide (see Figure 1 below).

In what sense does it appear to be a standard accounting fraud? According to the public information available as of now, a large share of Wirecard revenues and profits, especially in Asia, were apparently forged through a network of companies, indirectly controlled by Wirecard’s management and acting as third party acquirers, falsifying documents and money flows (see Mc Crum, 2020, for a comprehensive report of the Financial Times findings on Wirecard between 2015 and 2020). Additionally, according to reports of the Financial Times, only a minority of its operations were generating revenue and were profitable (Storbeck and Mc Crum, 2020; KPMG, 2020). Finally, € 1.9 billion of alleged reserves supposedly held in escrow accounts in Asia, were in the end not found by the auditors, Ernst and Young GMBH (EY) and in an investigation by KPMG.

Figure 1: Credit card payments



Source: Authors' description.

In this respect, what is surprising is the inability of all the layers of controls to detect such major frauds, especially as red flags of possible mismanagement of the accounts had been raised as of 2015 by the Financial Times (Mc Crum, 2015). Even more surprising is the fact that such red flags were instead considered as “fake news” channeled through the Financial Times by short sellers to manipulate markets: as late as February 2019, BaFin, the German authority for securities regulation and supervision, prohibited short selling positions in shares of Wirecard AG and the following April initiated a criminal complaint against the reporters of the newspaper².

The first level of internal controls in German listed companies is the supervisory board, followed by external auditors, like EY. According to public information, Wirecard AG, the parent company, submitted audited financial statements and management reports from financial year 2009 until 2018. EY also decided not to pursue an internal enquiry on an Indian branch of Wirecard, where evidence of accounts forgery had emerged through a whistleblower. Only a KPMG investigation in 2020 (KPMG, 2020), commissioned by the Supervisory Board of Wirecard itself, was finally unable to substantiate all of Wirecard AG's revenues in 2016-2018, and led the auditors not to sign the 2019 accounts and to acknowledge the non-existence of € 1.9 billion of presumed reserves in Asian trust accounts. The German Auditor Oversight Body (Abschlussprüferaufsichtsstelle), a relatively small agency under the Economic Minister, also did not detect anomalies in the EY management of Wirecard's auditing process.

² ESMA signed off the short sell-decision of Bafin in a short declaration on its website, alluding to “threats to market confidence” and “threats to the German financial market” without offering further explanations; see <https://www.esma.europa.eu/press-news/esma-news/esmaissues-positive-opinion-short-selling-ban-bafin>. (From Krahn and Langenbucher 2020).

The accounting enforcement bodies were also unable to detect fraud. In Germany, accounting enforcement for listed companies is normally carried out in two stages. As reported by Veron (2020), the first stage is undertaken by the Financial Reporting Enforcement Panel (FREP, known colloquially as the Bilanzpolizei - the Balance sheet police), and the second stage by the BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), which steps in only when it is perceived that the FREP has not been successful in solving the problem.³ Whereas the BaFin is a large public agency with a wide mandate over securities regulation and supervision, the FREP is a private entity, on a contractual relationship with Bafin operating with a small budget of €5.5 million in 2019 (Veron, 2020).

This fragmented structure of accounting enforcement, and consequently the inability in this case to provide adequate investor protection,⁴ is also partly related to the corporate structure of Wirecard. Wirecard AG, the parent company, was not classified as a financial holding company subject to direct Bafin supervision, but was regulated only as a technology company. Only Wirecard Bank AG was directly supervised by Bafin (Salway, 2020; Krahn and Langenbucher, 2020; Zeranski and Sancak, 2020).⁵ This implies that Bafin had no direct access to the activities of the group as a whole, but only to the activities of the bank, which provided only a partial picture of the company's operations. Finally, the Asian operations through third party acquirers and possibly difficult coordination between national supervisors added complexity and confusion to the Group's activity.

If Wirecard AG had been classified as a financial company, its accounting and its overall activities would have been probably supervised more tightly and directly by Bafin. Yet the issue of inadequate accounting oversight is of relevance for any listed company, not just those operating in financial services, in other words, no matter what the activities of Wirecard had been.

Even though this supervisory framework was probably not adequate to provide investor protection, and even though the global web of Wirecard's activities was quite intricate, it is still not easy to understand how a major fraud was not detected by several layers of controls.

As argued before, the reason cannot be technological complexity. Wirecard's appears to have been an otherwise pretty standard business model, simple enough to be benchmarked and adequately scrutinised to gauge the unsustainability of its operations. The presumed identity of "Fintech" and technological leader gave the company, instead, a status of "too complex to be challenged" and provided a veil of ignorance that possibly induced supervisors' complacency and diverted their attention. In other words, supervisors and markets appear to have accepted a superficial assessment of the activities performed.

As we will further discuss in the next sections, large amount of data and the use of AI can favour a better understanding of the customer base, a better screening of the quality of the business partners, and a more effective market risk management. But was all this enough to justify the quite extraordinary returns and the rate of growth of the company? Apparently, and according to the Financial Times, even

³ According to Zeranski and Sancak (2020), "The FREP acts on a random basis and in the event of concrete indications of a violation of accounting regulations and on the request of the BaFin (Bundesministerium der Finanzen, 2020). The BaFin may only act at the second level if the company does not voluntarily participate in auditing or does not agree with the result of an audit (Bundesministerium der Finanzen, 2020). It may also take action if there are serious doubts about the correctness of the examination results of the FREP or about the proper conduct of the examination by the FREP (Bundesministerium der Finanzen, 2020)". According to the Activity report of FREP on the year 2018, BaFin initiated three examinations because the companies had not accepted the FREP's findings and two examinations because companies refused to cooperate with the FREP.

⁴ I.e., ensuring an environment in which investors could make informed decisions.

⁵ According to Zeranski and Sancak (2020): "In February 2017, pursuant to EU laws, the BaFin and the Deutsche Bundesbank from the supervisory authority perspective examined Wirecard AG, as the parent company, and came up with the result that Wirecard AG was not to be classified as a financial holding company; therefore, the supervisory authority has no access to the entire Group. The ECB later agreed with this assessment (Bundesministerium der Finanzen, 2020)."

its IT infrastructure was not flawless, rather, it inherited weakness from companies acquired in the past (Storbeck and McCrum, 2020).

According to the Wirecard 2018 annual report, the last one issued, its payment and risk management business had a level of Earnings Before Interests Taxes Depreciation and Amortization (EBITDA) of 32.5%, and the acquiring and issuing business of 13.1%, resulting in a total EBITDA of almost 28%. Indeed, the business model of the company should have been thoroughly scrutinised to justify such high margins. Moreover, as part of its business was carried out by licensed third party acquirers in Asia, part of the margins of these activities had to be granted to these independent companies, at the expense of Wirecard margins.

Wirecard also claimed to use its technology to effectively bundle other financial services: *“by tapping on AI, credit solutions can be tailor-made to suit customer needs through flexible and rapid digital loan-approval processes. Last year, Wirecard introduced an AI-based credit assessment and decision system that is directly integrated into Wirecard's digital payment infrastructure. Powered by AI, real-time evaluation using data from long-term business relationships in the area of payment processing allows Wirecard's B2B customers to benefit from uncomplicated loan-approval decision-making processes and shorter waiting times for loan disbursements”* (Annual Report, 2018). Yet lending was a minor activity for Wirecard, from what we can understand today. Moreover, credit is a strictly supervised activity (and in fact Wirecard Bank was directly supervised by Bafin) where interest margins and defaulting loans are easily monitored. Also on this ground, the company's margins are hardly justifiable.

Hence, one of the consistent explanation of the supervisory failure here is probably related to an insufficient technological mastery by the supervisor, and the inability to assess that technology alone could not have improved the traditional business model to the extent claimed by the company. The lack of technological mastery and, possibly, the indulgence reserved to a fast growing national tech champion, may have induced supervisors, investors, and auditors into a complacency that prevented them from seeing what in fact there was (or actually there was not) behind Wirecard's exceptional figures.

Zertansky and Sancak (2020) and Pell (2020) assert that an explanation of the complacency could be behavioral biases (of the belief perseverance type, where one tends to remain on his/her original view even if evidence should ask for a revision) of those in charge of controlling Wirecard, and of investors as well. These interpretations of the case are just suggestive. Yet, there remains the fact that supervisors are experts and should be free from any bias.

The issue of national preference and the fact that one difficulty of supervising Wirecard is related to the weak coordination among supervisors in other countries, especially in Asia and in countries still protected by banking secrecy, like Singapore, brings into the picture the question of the international dimension of supervision. As for Europe, as we will discuss extensively below, this case calls for a strengthening of the coordination and even of a unification of the European regulation and supervision in the domain of investor protection and financial markets stability, along the lines of the Banking Union. And also the growth of the global dimension of Fintechs' activities requires an extensive coordination among authorities, beyond the European space.

It is also interesting that most of the debate on Wirecard does not bring into the picture the regulatory framework and oversight of payment systems. The company, as of its 2018 report, is subject to statutory and regulatory requirements for payment systems and payment products. Why were no irregularities detected also from this angle? For example, Salway (2020) states, *“As a provider of payment services that could be fulfilled by another provider, and which did not hold client money or engage in lending, Wirecard*

was not considered particularly risky from a regulatory perspective. Its risk was hidden in its interconnectedness across the market”.

The company was facing credit risk arising from receivables directly acquired by merchants or acquiring partners. This would arise from chargebacks, because of merchant insolvency or misbehavior, or time laps between the transaction and the product or service rendered (e.g. airline tickets) and possible chargebacks at a later stage. The company claimed to carry out comprehensive assessments of data to evaluate merchants and other business partners. But who was protecting the merchants, the business partners and the clients from Wirecard’s behavior?

As we will discuss below, avoiding loopholes in the supervision of payment systems, especially online, and especially when many different third parties in all layers of the value chain are involved, is very important and requires combining the double perspective of entities and activities.

In the next section, we discuss the Wirecard case and the complexity of Fintech’s activities from the point of view of their impact on investors and customer protection and on financial stability.

Taking stock of the observations about the Wirecard case, in section 3 we offer a broader view of the issues and possible solutions for the regulation and supervision of Fintech activities and operators.

2. THE COMPLEXITY OF FINTECH FIRMS AND THE OBJECTIVES OF FINANCIAL REGULATION AND SUPERVISION

2.1. Complexity in financial intermediation and Fintech

Until the end of the last century, financial intermediation used to be a rather simple activity: a bank collected short term deposits and used the proceedings to grant longer term loans (Rajan, 1998). Around the beginning of the 90’s a consolidation process took place in the banking industry, which led to the creation of larger and more complex financial intermediaries, often spanning different countries and activities (DeYoung et al., 2009; Pozzolo, 2009). In the following years, the diffusion of the “originate to distribute” model of financial intermediation was a first crucial step in the process of renovation of the industry. Unbundling their traditional activities, several banks sold their loans to outside investors, thus moving them outside the formal perimeter of their balance sheets (Farruggio et al., 2015; Panetta and Pozzolo, 2018). The next step was the spreading of the information and communication technologies in the financial industry, which allowed to further unbundle and recombine activities which used to be performed internally by a single bank (Barba Navaretti et al., 2017).

The Fintech revolution is still underway and it is allowing new players to enter financial markets and offer products which represent a single step in the value chain of traditional in financial intermediation (Boot, 2017; Dermine, 2017). See Box 2 for a list of prominent types of Fintech players.

The possibility to recombine the different activities which comprise financial intermediation has also led to the emergence of large players, bank holding companies which incorporate many subsidiaries spanning different aspects of financial intermediation. The boundaries of some corporations, such as Wirecard, have thus expanded to integrate the provision of financial services with highly technological activities, which have little to do with what in the past was considered as financial intermediation.

Box 2: Exemplary of most common types of Fintech by activity

Digital banks are deposit-taking institutions with insured deposits as traditional banks that operate with electronic interactions rather than physical branches. Examples include WeBank (China), Monzo (UK) and N26 (Germany).

Credit platforms are electronic platforms that offer an environment for the matching of lending and borrowing needs. A major distinction is between “sheet lending” and “crowdfunding”. In the former, the platform directly provides credit and as such becomes part of the loan contract, assuming the credit risk as long as the loans are kept in its balance sheet. With crowdfunding, the platform only facilitates the match between lenders and borrowers, but has no direct role in the contractual obligations, and thus assumes no credit risk. Fintech platforms may intermediate equity as well, typically with crowdfunding.

Robo-advising is asset-management advising performed by automated digital tools, with very limited human intervention. The services go from simple advices performed by means of “Recommender Systems” (i.e. one typical class of AI algorithms) to automated implementation of portfolio management. The small cost of serving additional portfolio advice and management (i.e. small marginal cost of operating) allows to offer financial advices also to small/medium portfolios that would be normally considered not profitable by traditional advice service providers.

Digital payments contemplate a vast set of activities related to the act of payment – such as transferring money and clearing or settling balances – which rely on digital technologies. These activities can go from simply initiating and checking order of payments via accounts held by payers and payees in other financial institutions, to more direct involvement in handling and transferring bank-money and electronic-money across accounts. As such different types of risks may materialise in the digital payment services.

Source: Adapted from FSB 2019.

As we will argue in more detail in section 3, compared to that of a traditional bank, the organisation and the business model of these new players is far more complex, making it difficult to understand where their comparative advantage with respect to the competitors lies, where their value added is generated, and what are the inherent risks in their activities. The last aspect is crucial to understand how and to what extent these corporations need to be regulated and supervised.

2.2. Supervising complex financial intermediaries

Regulation and supervision of financial markets and intermediaries became popular in the aftermath of the Great depression and is nowadays widespread all over the world (Calomiris and Gorton, 1991; Barth et al., 2008). While its general purpose can be seen as the protection of investors and clients from possible embezzlements of banks and corporations, it is important to disentangle the different objectives of regulation and supervision, so as to better understand how different authorities can cooperate in regulating and supervising complex financial intermediaries. To this purpose, a crucial distinction is between *investor protection* and *customer protection*.

We will deal with the more self-evident customer protection, in section 2.2.2 below. The rationale for investor protection can instead be found in the presence of asymmetries of information between investors, who provide the funds, and managers and entrepreneurs, who use them in accordance with the stated objective and mandate of a company. Guaranteeing that the users of funds provided by third parties offer clear, reliable and prompt information on their choices is crucial for the functioning

of the financial system. The more investors fear that their funds will not be used in such a way to guarantee the promised returns, the less they will be willing to invest, which ultimately hinders economic growth (Castro et al., 2004). With financial intermediaries, investor protection is partly related to customer protection, because investors can be seen as consumers who buy a financial product. However, three crucial distinctions must be made in this respect. First, making available reliable publicity of all information on the issuer of a financial asset – e.g., stocks and bonds – is commonly defined as investor protection, and it is what we will discuss in the next sub-section. Investor protection allows investors to make informed ex-ante decisions, but offers no guarantees on the actual ex-post returns. Second, guaranteeing that fair and transparent conditions are applied in the sale of financial assets to retail investors pertains to the service offered by financial intermediaries and can therefore be seen as the object of customer protection. Third, although bank deposits and some other means of payment available nowadays can be seen as financial assets, as it is the case also for cash, in practice they are held for the services that they provide, more than for the return that they offer. In other words, the investment component is less relevant than the service component. As such, the protection for bank depositors and users of other means of payments must be the one granted to customers, not to investors.

As it will explained below, in Wirecard's case, investor protection failed its role, while customers were left almost unscathed by the events. However, this is not really reassuring: the analysis of Wirecard's business model and of how it was regulated and supervised clearly uncovers a number of dangerous loopholes, which might have led to serious problems also for its customers.

2.2.1. The objectives of financial supervision: investor protection

Clearly, protection needs to be granted with respect to all possible investments, not only those in financial corporations. In this respect, limiting the possibility of fraudulent actions is as important in the case of energy or food corporations, like Enron or Parmalat, as it is for banks, like Lehman Brothers.

Regulation and supervision aimed at protecting investors is much less harmonised across the world than banking supervision, lacking, for example, a solid supra-national authority like the Basel Committee for Banking Supervision. In practice, there is no agreement on sound common standards, and the authorities responsible of investor protection in each country have very different powers and responsibilities. Indeed, authorities like the Security Exchange Commission in the United States have strong powers and a solid reputation, but this is not the case in other advanced countries. Even in Europe, investor protection is one of the least harmonised supervisory activities, being left to the responsibilities of national authorities, although under the coordination of ESMA.⁶

Strong investor protection can be a source of comparative advantages for a country's financial market, but it can also hinder attractiveness in the eyes of foreign actors. Strong supervision may be very attractive from the point of view of investors, but it may cause corporations to be less willing to list in a stock exchange. Indeed, many observers have suggested that the Sarbanes Oxley Act in the United States, approved after the occurrence of some major scandals such as that involving Enron, was one of the reasons why listing in New York stock exchanges lost attractiveness as opposed to listing in London (Piotroski and Srinivasan, 2008). On the contrary, a weak regulation and a lax supervision may be attractive from the point of view of firms, but less so for investors. This trade-off is particularly sensitive in the case of large financial centers, which compete to attract not only corporations but also international investors. Instead, it may be less relevant in the case of smaller countries, which could be

⁶ See in particular the description of the activities of ESMA on Corporate disclosure (<https://www.esma.europa.eu/regulation/corporate-disclosure>).

willing to guarantee laxer regulation and supervision to its own corporations, therefore giving them a comparative advantage when they face foreign competitors. This could be even more true when these domestic corporations offer their services mostly to foreign customers (as was the case for Wirecard's activities in Asia), whose welfare is less of a concern for domestic authorities. Countries which do not host large international financial centers may therefore find it more appealing to use weaker investor protection to provide a regulatory advantage to its corporations, both at home and abroad. In turn, if the competent authorities in foreign countries decide to also adopt weaker regulations and laxer supervision to favor the domestic corporations which face a stronger competition from abroad, this can cause a dangerous "race to the bottom" in regulatory and supervisory standards.

As we discuss more thoroughly in section 3, the diversity of international protection standards across the world is a source of regulatory arbitrage, and it has shown in the past to be a major cause of frauds: in most cases, from Enron to Parmalat to Wirecard, the embezzlements were made possible precisely by opaque or hidden international transactions. The lack of harmonisation and coordination at the international level is even more worrying because the supervision of corporate balance sheets is a responsibility left almost entirely to private auditing firms, with the notable exception of firms in the financial sector, which are subject also to the careful scrutiny of public authorities. As it is well known, auditing services are paid by the same corporations that require them, causing obvious problems of conflicts of interests, as in the largely debated case of rating agencies. While we do not deem it possible and effective to create a public authority responsible for auditing of all corporations, there is a strong case for increasing regulation and supervision of auditors, as Wirecard's case has made it clear, and we will argue more thoroughly below.

Wirecard's case shows four major weaknesses in investor protection. First, EY, the firm responsible of the auditing of Wirecard, seemingly failed to detect large accounting malpractices. Second, the German Auditor Oversight Body (Abschlussprüferaufsichtsstelle) inadequately supervised, according to publicly available information, EY's auditing practices at Wirecard. Third, Germany's Federal Financial Supervisory Authority (BaFin), which is also responsible for investor protection, and FREP, the first stage auditing supervisor in the case of Wirecard, had too weak powers to conduct a thorough investigation on Wirecard's activities. Fourth, it is not possible to exclude that in the trade-off between strong and lax supervision mentioned above, relevant actors were inclined towards the latter, possibly with the aim of favoring what appeared to be a successful Fintech "national champion".

Although it is unreasonable to suggest that a public authority should be able to know the business model of all corporations, let alone being responsible for the auditing and supervision of the balance-sheets, as we said above, Wirecard's case clearly illustrates several directions for improvements, along the lines that we will further explore in section 3.

In Europe, the oversight of auditors' activities is the responsibility of national authorities by Directive 2014/56. Chapter VII of the Directive calls explicitly for investigations and sanctions to "*detect, correct and prevent inadequate execution of the statutory audit*" (article 30). This is indeed a step in the right direction, although it is not clear that this is already a common practice among national oversight authorities in the EU (neither the Wirecard case has been reassuring evidence in this sense).

Coordination among national authorities at the European level is endured by the Committee of European Auditing Oversight Bodies (CEAOB), a new authority formed by representatives of the national oversight bodies and of ESMA, which held its first meeting in 2016. While it is premature to judge the activities of this authority, given the high level of concentration in the market for auditors of large corporations, a bold approach is needed to achieve strong coordination at the European level. Indeed, the creation of a brand-new supervisory agency, responsible of all aspects related to market

conduct (e.g., market abuse, insider trading), including auditors' oversight, might be a viable solution.⁷ Finally, as further explored in Section 3, stronger cooperation among supervisory authorities across the world should make it easy and swift to verify the very existence of the credits that corporations claim to hold abroad.

2.2.2. The objectives of financial supervision: customer protection

The rationale for bank supervision is that the value of customers' deposits needs to be guaranteed, because they are *de facto* an almost perfect substitute for cash.

The experience of many banking crises, especially in the form of bank runs, and a vast scholarly literature starting from the seminal contribution of Diamond and Dybvig (1983), has made clear why a financial system in which the value of bank deposits is guaranteed achieves a higher level of welfare. For this reason, deposit insurance schemes are widespread all over the world (Demirgüç-Kunt et al., 2014), and strong regulations limit the ways in which banks can invest their clients' funds.

A client who deposits his funds at a bank incurs both a liquidity risk and a credit risk. The liquidity risk is due to the possibility that, even if the bank is solvent, it is unable to make the funds available to the depositor, thus making it impossible to use them, for example to make a payment. Liquidity risk is limited to the possibility that a depositor cannot access his funds promptly, not that he loses them all together.

This second case is that of credit risk, that is the possibility that a bank is insolvent, and that the depositor definitively loses access to his funds. In the case of retail deposits of limited amount, deposit insurance schemes protect depositors from this risk. At the same time, bank regulation and supervision reduce the possibility that a bank becomes insolvent.

Although liquidity and credit risk are conceptually different, they are intrinsically connected, because they are typically caused by the same financial intermediary, banks.

The unbundling of financial intermediation services has added a degree of complexity to this picture. Consider, for example, the case of a financial intermediary specialised in offering payment services. Traditionally, this activity was performed by banks, which, in the case of transactions regulated using bank money, transferred the funds from the account of the debtor to that of the creditor. This is what typically happens when we make a bank transfer to pay a rent. Liquidity risk and credit risk of banks were therefore guaranteed by the protections described above.

Financial intermediaries specialised in offering payment services, such as PayPal or Wirecard's Boon, are instead subject to lighter regulations than banks, because they are not allowed to freely use the funds that their customers deposit in their accounts, but must invest them in reserves held in the form of highly liquid financial assets, such as interbank deposits or short term risk-free bonds. Credit and liquidity risk are thus virtually absent, because the customers' funds are always securely held and readily available. Regulation and supervision must therefore guarantee only that these financial intermediaries respect the provision that the customers' funds are set aside as reserves. Indeed, this is a much easier task than controlling the composition of loans and portfolio investments of a traditional bank.

In the case of card payment schemes (see Figure 1 for a stylised representation), retail customers are subjected to even less credit and liquidity risk. In this case, the acquirer collects the funds from the bank of the buyer and transfers them to the bank of the merchant which sold the good or the service. The

⁷ See Krahenen and Langenbucher (2020) for a more detailed proposal, also discussing how to create such an authority under European Law.

buyer is never in the position of having a credit with respect to a financial intermediary, and therefore faces no credit risk. If the buyer does not make the required payment, it is the issuer of the card that is liable to the acquirer, and therefore faces a credit risk with respect to his client. For this very reason, the issuer bank is typically very cautious in setting the limits of usage of the card. The acquirer obviously faces a credit and liquidity risk, if the customer does not make the required payment and the issuer in turn is unable to transfer the funds, but this would not be a problem for customers (unless it became a source of financial stability risk, an issue to which we will come in the next sub-section).

The risk faced by consumers is thus just that they may be unable to use their credit cards anymore, that is a liquidity risk. So far, suspension of credit cards has been a rare event, mostly because most countries regulate and supervise the activities of financial intermediaries which take part in card schemes. In addition, card networks such as Visa and Mastercard fix themselves relatively tight standards that all members of the scheme need to satisfy. In fact, Wirecard's default has caused virtually no problems to its payment subsidiaries, whose major activities were managed by financial intermediaries regulated and supervised in Germany and in the United Kingdom. Even the decision to suspend all payments made by Wirecard Card UK, taken by the Financial Conduct Authority (FCA) on July 26th, only lasted few days. Similarly, the decision taken by the Monetary Authority of Singapore (MAS) on September 30th to require that Wirecard's subsidiary in the island (Wirecard SG) ceases its payment services and returns all customers' funds by 14 October 2020 was preventive, and no customer in Singapore appears to have suffered from the default of Wirecard's holding company. Indeed, to further control the credit and liquidity risk of Wirecard SG, MAS had already helped customers to move to other providers also avoiding transfers of funds between countries.

Overall, the evidence so far available suggests that the regulation and supervision of payment services offered by the subsidiaries of Wirecard AG was in place. A different issue relates to the supervision of Wirecard group, the holding company. The issue of defining a financial holding company, which is ultimately subject to consolidated supervision as a financial institution, is the object of Directive 2002/87. It depends on the weight and relevance of the financial activities carried on by the subsidiaries which form the group. In the case of Wirecard, according to the "Recording for the finance committee of the German Bundestag" produced by the German Ministry of Finance on July 16th 2020, "*After a joint examination by the Deutsche Bundesbank and BaFin in 2017 and in accordance with a later confirmation by the ECB Wirecard AG due to the focus of its activity and that of its subsidiaries are therefore not a financial holding company*". With the benefit of hindsight, one might judge this decision as inappropriate. But, considering the limited impact of Wirecard's default on consumers, it seems excessive to adopt a pervasive definition of a financial conglomerate so as to apply stronger regulation and supervision also to non-financial holding companies having payment institutions among its subsidiaries. As we will discuss more thoroughly below, a better approach would be to grant adequate oversight powers on any technological third party provider offering relevant services to a regulated financial intermediary.

Credit card schemes have an additional large set of customers: the merchants. In a typical card scheme, the acquirer transfers to the merchant the funds of a purchase before it receives them from the bank of the customer. Since the acquirer may fail to do so, the merchant suffers from a potential credit risk. However, this risk is limited, for three main reasons. First, if the customer does not pay for a purchase, the payment must be made by the issuer, which in most schemes is liable with respect to the acquirer. Second, in most countries, acquirers are regulated intermediaries (in Europe according to Directive 2015/2366, known as PSD2). Third, even if an acquirer were to default, the merchant would only have to take part in the bankruptcy procedure for the amount represented by the flow of payments from the moment of the purchase to the moment of default, which is unlikely to be substantial. Nonetheless,

acquirers play a pivotal role in the system, and for this reason they are subject to specific regulation and supervision, which in Europe is defined by PSD2.

The complexity of Wirecard's business model points instead to a liquidity risk which is not caused by the unavailability of funds, but by the discontinuation of technological activities. The unbundling of specific services that were part of the traditional integrated model of financial intermediation is often associated with their re-bundling into new set of activities, depending on the position on the value chain in which the company has a comparative advantage. Many technological companies have no comparative advantage in the provision of financial services with respect to incumbent financial intermediaries, but they may have huge comparative advantages in the provision of technological services, such as data collection and management.

Understanding the business model and the related risks is crucial. Merchant account providers, for example (e.g., Payfirma), help merchants to set up their own dedicated account with acquirers, so that they can accept payments with debit or credit cards. Crucially, they are non-financial corporations offering only technological services. In principles, their default would only cause liquidity problems to customers and merchants. For this reason, they are not directly subject to the provisions of PSD2, as specified in Article 3/(j).

Payment aggregators, on the contrary, register and collect the transactions of large sets of merchants and make them available for processing to the acquirers, allowing the merchants to accept credit and debit card payments and transfers without having a direct relationship with a bank. As such, payment aggregators collect and hold funds that are meant to be transferred to the merchants, and therefore must be regulated as financial intermediaries. For this reason they are payment services providers subject to the regulations of PSD2. Interestingly, Wirecard was offering both services through its subsidiaries, some of which were in fact regulated, such as Wirecard Card UK and Wirecard Bank AG. However, as we will better explain below, a neat distinction between fintech and non-fintech activities based on a simple taxonomy, without having a holistic perspective on the entire business model would provide a misleading picture of the actual risks faced by customers.

2.2.3. The objectives of financial supervision: financial stability

The Great financial crisis of 2007-2008 has made it extremely clear how important it is to guarantee the stability of the entire financial system. In this respect, Wirecard's case has uncovered two issues that were possibly overlooked.

First, the default of a large issuer may cause financial stability problems. Even if they are financial intermediaries, and therefore should be in a better position than customers and merchants to evaluate the risk of holding a credit position with respect to issuers, some regulations might be envisaged to limit the possibility that the failure of a large issuer triggers a cascade of defaults of the acquirers, ultimately hindering the stability of the entire financial system. For this reason, issuers are considered as payment services providers and as such they are regulated and supervised.

Second, the discontinuation of technological services provided by non-regulated entities to many acquirers might be a substantial cause of systemic risk. This would have been the case if Wirecard had suddenly stopped providing its technological services to the many third-party acquirers to which it was linked in Asia. Merchant account providers may offer their services to many different acquirers, and therefore assume a pivotal role in the payment process. If they were to default or to be unable to continue offering their services, this could potentially hinder the operations of acquirers and merchants. Moreover, customers who assume that they can pay a merchant with their card would be unable to do so. While this is typically classified as operational risk, its effect is that of reducing the ability of customers and merchants to use some payment instruments, de facto causing a liquidity risk.

For customers, this is a simple service interruption, but nonetheless can be a possible cause of significant problems, for example in the case they need to purchase a medicine or a transportation ticket. For merchants, this may cause a loss of business opportunities, possibly materialising into insolvency (it is probably for this reason that gas stations, which make a large use of card payments and cannot recall the good once it has been provided to a customer, typically use multiple merchants for their card payments). In this regard, it is instructive that, in Singapore, the communication by Wirecard SG of the inability to processing payments has been considered a crucial argument by the authorities to require the company to cease all its payments services. At the same time, the Monetary Authority of Singapore offered advice to merchants on how to switch to alternative service providers. Finally, the liquidity problems of the acquirers may spread to other financial intermediaries through the interbank market, hindering financial stability.

To limit a possible source of substantial systemic risk, it is therefore crucial to gain a full understanding of the role of the providers of technological services to financial intermediaries. As argued by the European Commission (2020b) in its accompanying document to the “Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector” (European Commission, 2020a), financial intermediaries must disclose to the competent authorities their dependence on external providers of financial services and have contingency plans in case of disruption of services. In the proposed oversight framework, one of the three European Supervisory Authorities will act as Lead Overseer and will have the power to require information and also to conduct investigations and inspections at critical ICT third-party service providers.

A key characteristic of the Proposal of the European Commission (European Commission, 2020a) is that it grants strong oversight powers with respect to any technological third party provider offering services to a financial corporation, independent on whether the provider is part of the same business group as the financial corporation, it is directly controlled by the financial corporation, or it is independent. In this way, it, in our view, effectively overcomes the problem of the definition of financial conglomerates as opposed to non-financial conglomerates, making the right of oversight dependent on the actual risks that the technology company may cause on financial intermediation.

3. REGULATION AND SUPERVISION OF FINTECH

Fintech players enter financial markets for two reasons (Barba Navaretti et al., 2017) either to exploit process and/or product innovation, or to exploit regulatory arbitrage. The latter motive should not be underestimated. In fact, financial markets are probably among the most regulated markets nowadays, with many opportunities of regulatory arbitrage.⁸

Discrepancies may emerge, for example, in the treatment of incumbent traditional institutions, such as banks, that are already active in financial markets and of new entrants, especially when these two groups differ in the type and span of services they supply. When these discrepancies in regulation and supervision do not reflect different risks of different institutions, they open-up regulatory arbitrage opportunities.

⁸ EBA 2017 report on Fintech in EU shows that 31% of Fintech operators are not subject to any regulatory regime, although this does not necessarily imply that these companies are eluding regulatory oversight.

In this section we illustrate the difficulties that Fintech players bring about to financial regulation and supervision and we then present three elements that policy makers must have in mind, “imperatives”, for effectively dealing with the Fintech revolution.

3.1. Regulation and Supervision: from entities to activities

3.1.1. From “comfort zone” to uncharted territories

Banks and traditional financial institutions are nowadays the “comfort zone” of regulators and supervisors. As discussed in the previous section, when dealing with these institutions, supervisors have a lengthy experience on how to provide protection to investors and customers and guarantee stability. This does not mean that there will not be regulatory or supervisory failures of traditional financial institutions in the future. But, because of cumulated experience and knowledge about these entities, supervisors are able to implement sufficiently effective tools and guarantee well-functioning and relatively safe financial markets.

The advent of Fintech has opened-up new opportunities, that is, financial innovations both as new services/products and as new production processes (see Boxes 1 and 2). These are mostly uncharted territories, not only for entrepreneurs, but also for experienced supervisors and regulators.

It may be useful to identify at least four types of operators engaging in the financial innovation process, based on their specific attitude towards financial innovation. We term them “Enhancers”, “Unbundlers”, “Pursuers”, and “Bigtech”. As a matter of fact, some operators combine more than one or even all the features of these different types. For reasons that we will specify further, this categorisation of Fintech players relies on the distinctive economic motivation of these firms, i.e. their “business model”, and differs from the traditional one in Box 2 that instead refers to the line of activity.

Enhancers are operators that perform some key technology-based activities in financial markets, but they also cater to other industries. They build and rely on new and efficiency enhancing technologies or infrastructures, such as AI and ML (see Box 1). These entities need not be financial institutions, and often provide technological services that financial institutions have decided to outsource. In this respect they participate to the *vertical unbundling* of financial activities, that is the separation of some of these activities performed at different vertical stages of the value chain. For example, it is not uncommon that external and non-financial firms perform the data analytics necessary to activate some of the core business functions in Fintech. These are often technology or computer science companies that provide infrastructure, design algorithms not necessarily specific to financial applications, process the data analysis and sometimes store large amounts of data of Fintech players. This was the case, for example, of many subsidiaries of Wirecard’s group that, differently from Wirecard Bank AG, were mainly technology firms.

Unbundlers are new specialised financial operators, entering in specific segments traditionally served by all-round financial institutions. Their business model is based on financial innovation and specialisation. These entities thus perform *horizontal unbundling*, separating services to final users that traditional financial institutions would offer as a bundle, such as payment and credit service. They can manage all their activities in-house or outsource some of them to Enhancers. A typical example is that of issuers of electronic money, such as Wirecard’s “Boon.” and Satispay, a Luxemburg based company mainly operating in Italy.

Pursuers are traditional financial operators such as banks, that catch-up adopting new technologies, thus enhancing their process and products. These entities in fact expand the bundle of activities that

they offer, or replace some of them with innovative financial services, often by means of mergers and acquisitions of Fintech start-up. As such they are *horizontally bundling* additional financial services and processes. A paradigmatic example is the acquisition by JPMorgan Chase of the Fintech startup WePay in 2017.

BigTech are large companies that operate platforms in non-financial markets, such as business-to-consumers platforms (an example being Amazon) or social networks (an example being Facebook), and that enter financial markets leveraging on modern technologies, their vast amount of consumer-data and financial liquidity obtained in other non-financial markets.⁹ This is yet another form of *conglomerate bundling*, as they put together financial and non-financial services that are at least initially unrelated.

The very same presence of these many and different types of operators in financial markets makes existing regulations very often inadequate and supervision definitely more complex.

Box 3: Types of Fintech by business type

Enhancers: operators that perform some key technology-based activities for financial markets, but also cater other industries (e.g. data analytics services). They are instrumental to the *vertical unbundling* of financial activities.

Unbundlers: specialised financial operators, entering in specific segments traditionally served by all-round financial institutions (e.g. payment services). These entities perform *horizontal unbundling*, separating services that traditional financial institutions would offer as a bundle.

Pursuers: traditional financial operators such as banks, that catch-up adopting new technologies, thus enhancing their process and products, often by means of mergers and acquisitions.

BigTechs: large companies in non-financial markets, such as business-to-consumers platforms (e.g. Amazon), that enter financial markets leveraging on updated technologies, vast amount of data and financial liquidity obtained in other non-financial markets. This is yet a new form of *conglomerate bundling*.

Source: Authors' analysis.

3.2. The risks of compartmentalising Regulation and Supervision: entities vs. activities

Probably the most visible phenomenon in Fintech is the entry of *Unbundlers*. These new players are often very innovative startups that emphasize their ability to leverage AI innovations in financial markets (see Box 1) on specific segments of financial markets. Because of the rapid rise of this type of new operators, much emphasis has been put so far on the necessity of moving regulation and supervision from entities to activities (for example, Ferrarini, 2017). The rationale for this approach is that if a firm is performing some activity that is subject to regulation and supervision, then the firm should be subject to supervision and regulation irrespective of that firm's form of incorporation and of other activities performed in parallel. For example, a credit platform that intermediates credit by

⁹ These companies are also called TechFin.

assuming the risk of credit, even if temporarily, (that is the “sheet lending” platform discussed in Box 2), should be treated as any entity performing credit, on this dimension as any traditional bank. This approach has the merit of guaranteeing an adequate monitoring of risks, and at the same time levelling the playing field across different types of operators.

Although moving control from entities to activities has certain merits, it may not be enough to address the complications implied by the many different types of operators that we have discussed above. The main risk of this approach is that of losing the big picture of companies’ activities. As we have seen, in fact, horizontal unbundling is not the only strategy pursued by Fintech players. There are entities that in fact rely on incorporating and actually (re-)bundling new Fintech activities, such as the *Pursuers*, others that bundle possibly unrelated lines of business, such as the *Bigtech*, and others that rely in vertical rather than horizontal unbundling, such as the *Enhancers*.

As a matter of fact, just focusing on regulating and supervising activities generates a significant risk of compartmentalising the oversight of financial markets. This approach may end up with silos of independent and unrelated regulations and supervisions.

For example, with vertical unbundling strategies, non-financial *Enhancers* may escape oversight. Consider the payments business where Wirecard was operating. As discussed above, formally Wirecard was a third party to Wirecard bank, operating just infrastructure building, data storage and analytics for the latter. As a technology enhancer it was not subject to the required oversight. Apart from the alleged accounting frauds, moving operations related to financial activities outside of the regulatory perimeter is a considerable source of new risks, especially when these enhancers become very large players, running the operations of many financial companies at the same time. As already mentioned in the previous section, temporary disruption of the services of these enhancers, for whatever reason, may halt services of a very large number of clients in financial markets. This is an operating risk due to the concentration of critical services for financial companies in mostly unsupervised and in principle non-financial entities.

A similar risk emerges with the entry of *Bigtechs* in some segments of financial markets, such as the payment system. These companies leverage on their technological knowhow, big data and often large liquidity pools and may spread their activities quickly and globally. With these companies, activity-specific supervision may provide a very limited illustration of the business performed and the underlying risks. Indeed, some of the *Bigtechs* already have de jure independent, but controlled entities that are licensed as digital payment or electronic money institutions (e.g., Uber in UK and Netherland, Amazon in Luxemburg, Facebook in Ireland, Airbnb in UK). It is urgent to understand what the precise relations that these companies engage with their holding companies is. Incidentally we note that the entry of these players should be monitored also from a market competition perspective, because of their impact on other players’ profitability and the overall structure of financial markets. If exploiting efficiency across different markets is desirable, extending dominant positions from non-financial markets to financial markets should be avoided.

We now come to the *Enhancers*. From a regulatory perspective, it is crucial to understand to what extent providers of technological services should be supervised and whether there should be differences between technological providers that also offer financial services through their subsidiaries, such as Wirecard AG, and those which instead focus only on technological services. The debate on supervision of the activities outsourced by regulated financial intermediaries to un-regulated entities is not new,

but is it far from settled.¹⁰ In Wirecard's case, the evidence of significant disruptions for customers and merchants is so far limited. But this is no guarantee that problems will not emerge in the future if a large provider of technological services were to discontinue its activities. Stronger supervision on all non-financial corporations capable of causing a potential break-down of payment services is therefore necessary to protect customers from the liquidity risk associated by their electronic means of payments. Of course, this requires a thorough understanding of the technological and business model of each firm taking part in the payment value chain. Consistently, the recent proposal of the European Commission for a Regulation on digital operational resilience for the financial sector (European Commission, 2020a), goes in this direction.

For all these reasons it is certainly important to consider the specific activities performed but also, at the same time, to retain the big picture of the new financial entities.

Considering the novel and specific issues that Fintech operators of the different types will bring about, we now propose three "imperatives" for updated regulation and supervision that we consider necessary: "Know the technology", "Know the business model", "Know the global picture".

3.3. "Know the technology"

What are the actual technologies that Fintech players claim they rely on? There is a lot of discussion on this, but also too much hype (see Box 1). The risk is that we do not effectively understand what is going on behind the smoke screen of innovation.

3.3.1. Artificial Intelligence and Supervision

At the core of Fintech expansion there are two novel ingredients: (i) a set of relatively recent technologies that allow better information extraction from data, that often goes under the hat of Artificial Intelligence ; (ii) large data sets, or Bigdata, that can be effectively exploited with AI (See also Box 1).

The novelty with AI in fact lies in the dramatic reduction of the cost of computing and storing data in the past years. In fact, many of the algorithms used in AI were proposed decades ago. It is because of the subsequent reduction in the cost and speed of computing power that Bigdata and AI started to become important and usable for the digitalisation of human activities in markets and daily life.

AI algorithms, Bigdata and low cost of computing together make predictions, in several domains and not only in financial markets, more precise, cheaper and promptly available. The real important phenomenon is in the end the increased ability to predict future events and behaviours with more precision and more quickly. These better predictions in turn allow for an increase in the automation of decisions. One of the most important ramification of AI is ML (see Box 1). AI algorithms in fact learn from the data and in some cases (e.g. in the case of Reinforcement Learning algorithms) they autonomously learn by experimenting with trial and error.

An example of applications of these technologies in financial markets is an entity intermediating payments that can make better predictions on the risks involved in specific transactions and thus better prepares for adverse events, and or more easily nets out different transactions. These processes can also be seamlessly delegated to algorithms and automated, possibly involving different API interfaces (see Box 1).

¹⁰ See the proposal for regulation prepared by the Commission to the EU Parliament and the Council, about digital operational resilience in the financial sector (European Commission, 2020a).

Another notable example is Robo-advising, that is the possibility to automate the advising on portfolio management (see Box 1). In this case too, the application of AI is to better predict what could be the needs of a specific household that would normally be left with no financial advising at all. Reduced costs of prediction here allow to perform and serve segment of the markets that would otherwise be excluded.

In fact, the applications of AI and its improved ability to predict trends in financial markets are enormous, and we are currently seeing probably just the tip of the iceberg.

Nonetheless, it is important that this sparkly side of AI and Bigdata does not blind us, and especially not regulators and supervisors. These tools have limitations that are often difficult to foresee, also to the very experts and even their designers.

The first of all current limitations is that we currently do not have Artificial General Intelligence, that is tools that fit and adapt to many different applications. We have instead a rich set of many different tools that are designed to perform in specific environments but cannot be exported in other contexts. This specificity requires that the assessment of these technologies must be performed by experts of the environments at hand, case by case.

Second, AI can be manipulated. Learning is in fact a delicate process that can be manipulated. It has been shown that AI algorithms can be fooled by modifying small apparently innocuous details of the patterns they should recognise.¹¹ This possibility points to the risk of attacks that may destabilize AI tools, with nefarious consequences and repercussions, especially in applications for financial markets.

Third, AI may come with unexpected consequences. As AI/ML are complex tools, sometimes using sophisticated algorithms, not all consequences can be perfectly understood before deploying them in actual applications. For example, it has been shown that AI algorithms designed to decide prices and compete on markets may autonomously learn to coordinate and collude on high prices.¹² AI algorithms may end up showing biases. For example in credit allocation to certain categories of individuals, biases that emerge spontaneously and in some cases also inherited from the data that are used for training algorithms.

Fourth, AI powered algorithms are often difficult to interpret, thus becoming black boxes. The lack of “explainability”, a technical challenge that designers of algorithms are currently trying to address, makes it difficult to fix possible problems that may emerge when deploying algorithms in financial markets.

Although one can never underestimate the impressive efficiency that AI algorithms can bring to markets in general, and financial market specifically, all the previous issues illustrate that we must avoid any hype about AI and its applications. And a significant part of what is absolutely needed for a safe use of AI in financial markets is the ability to monitor and assess the actual behavior and functioning of these algorithms.

We cannot just accept as a fact that a firm relying on AI is certainly better performing and more efficient. On the contrary, under many circumstances, it may be riskier. Unfortunately, this assessment is not simple, tends to be unavailable to market operators as it must be performed by experts. The risks of not effectively assessing the uses and consequences of sophisticated AI algorithms in financial market are significant, from the smoke screen that AI may offer for fraudulent behavior, as probably in the case of Wirecard, to new risks of financial instability. In the case of payments, a relevant area of activity of

¹¹ See Jiawei et al. (2019).

¹² See Calvano et al. (2020).

Wirecard, most of the activities involved in transactions still go through traditional channels and infrastructures. The relevant innovations where AI may have a significant impact are mostly at the very end of the payments ecosystem. We must thus be able to discern this and avoid thinking that any generic application of AI in the payment system can bring about significant gains of efficiency in this, after all traditional, environment. Although, in the case of Wirecard, specific AI-related risks were not reported, at least so far, one could ask what information was available in this respect and who was monitoring the actual functioning of the AI tools that the company was claiming to use for its financial market operations. We do not have first-hand information, but we suspect that nobody was effectively doing this.

Some national authorities are already setting up units for competent assessment of algorithms and technological services in different areas of financial supervision (e.g. the Fintech Sector unit of the Supervision Department of the Bank of Italy, and the Fintech Hub of the Bank of England). Some authorities are introducing requirements and tests for weakness of financial entities relying on AI, checking also possible plans to address critical situations (e.g. the AI principles identified by the Netherlands Bank and the Hong Kong Monetary Authority).¹³ All this is commendable and must become the standard worldwide.

To limit a possible source of substantial systemic risk, it is therefore crucial to gain a full understanding of the role of providers of technological services to financial intermediaries.¹⁴ It is important that financial intermediaries are required to disclose their dependence on external providers of financial services and that they have contingency plans in case of disruptions. In some cases, it may be possible to require that regulation and supervision can be extended to some specific activities provided by external technological providers.

3.3.2. Technology for Regulation and Supervision: RegTech and SupTech

Interestingly, not only can Fintech rely on innovation and digital technologies, but regulation and supervision can also profit from and adapt to using some of these tools. This possibility has been referred as Regtech and Suptech. Broeders and Prenio (2018) use the terms to define the use of innovative technology, in particular AI and big data analytics, for the regulation of automated and standardised activities and for agencies to support financial supervision.

In particular, regulations can contemplate and impose the use of technologies for compliance of financial entities. A typical application is in reporting to financial authorities, which can be standardised and then automated thus substituting ad-hoc templates and manual activities. This process also has the benefit that standardised data transmission allows for automated data analytics on the side of the supervisors and facilitates information sharing and cooperation of supervisors across the world. Relying on automated and standardised financial reporting, financial entities may also be requested to perform data analytics to recognise internal fraudulent activities.

Suptech could use technologies themselves in performing supervision of financial entities. Among the most promising applications of Suptech, there is the use of AI/ML to detect anomalous patterns, possibly associated with misconduct and heightened risks. Algorithms can be trained to monitor financial transactions and activities and detect these behaviors. These tools (often termed “screens”) promise a more systematic scan of financial markets and a better balance between false positive and false negative than human experts’ judgment. So far, supervision has been based on the idea that

¹³ See Netherlands Bank (2019) and Hong Kong Monetary Authority (2019).

¹⁴ On the risk related to third-party activities in financial services see FSB (2020), European Commission (2020a).

supervised entities had to provide information by means of reports. Suptech may change this paradigm. For example, specified APIs may allow supervisors to directly access data and explore supervised entities for relevant information. This is what happens, for example, at the Netherlands Bank, where automated analysis of orders and executions is used to identify funds transferred to the same recipients via different routes in high-risk jurisdictions.¹⁵

Although Regtech and Suptech will certainly complement the activity of regulation and supervision of financial markets, they will not completely substitute more traditional approaches. Currently, they are only experimental in nature or at a development stage, with very few already being operational. Because they use tools that rely on AI/ML, as we have illustrated, they are also prone to the risk of manipulation and adversarial attacks. These systems must thus be carefully designed to guarantee cyber-resilience and will always require competent human interaction and supervision.

However, what is probably the most significant risk for Regtech and Suptech is that they develop as spontaneous but uncoordinated activities. In fact, they are already growing in numbers and span in many countries worldwide (see BIS, 2020). The risk is that the outcome will be a very fragmented set of tools, wasting a unique opportunity of international collaboration and cooperation. We cannot stress enough that cases like Wirecard developed to such a scale also because of the global reach of this company's activities and the lack of information sharing across authorities.

At least within its boundaries, as we will discuss extensively below, Europe must take action and coordinate the developments of Regtech and Suptech leading to integrated and interoperable systems across the member states. This, in our view, does not mean that Europe requires special entities dealing with Fintech and their innovative activities, rather than existing regulatory bodies must be better prepared to monitor and tame the new technological developments in the industry, within a coordinated European framework. At minimum, coordination must rely on harmonized definitions (this may seem a detail but in a fast growing and changing industry, precise and shared definitions are necessary for any development) and shared knowledge of techniques and approaches. It would be important then to have a common standard for machine readable information which is a necessary step for further coordination which might take place initially with specific working groups of national competent authorities.

3.4. “Know the business model”

Unfortunately, knowing the technology and its application by Fintech players is not enough and we need to understand, also, why firms adopt it. We can reasonably expect that, at least in market economies, technology adoption is ultimately motivated by profit maximisation, over some relevant time horizon. As obvious as this observation may seem, it is relevant here because increased profitability is almost systematically associated with additional risk, especially in financial markets. This does not mean that profit-increasing technologies should be opposed because of higher risks. As with traditional regulation and supervision of financial markets, the problem is when risks of financial activities are not completely accounted for and determine external negative effects, on investors, customers and financial stability. Indeed, limited profitability can be itself a source of risk and instability in financial markets. For example, increased competition among traditional banks may increase the risk of banks default (see Berger, 2009) and we may expect that this is also the case when banks face even more intense competition with new Fintech players. Hence, assessing firms' profitability is key for proper and detailed risk assessment. However, understanding the source of profits and risks, especially with innovative tech firms, is not an easy task. For example, some Fintech firms operate with

¹⁵ See Ehrentraud et al. (2020) for a cross-country overview of Regtech and Suptech initiatives.

technologies that feature large fix setup costs, and negligible per-client costs (this is the case for example with data intensive technologies). Intense competition in markets with this cost structure may become unsustainable, unless firms are able to charge different prices to different customers. Credit platforms may decide to charge their customers (on the side of the borrowers and of the lenders) with fixed fees, in which case they have all the incentives to increase participation, possibly sacrificing the screening of the credit records of participants. The credit card payments system, as another example, involves many operators (credit card companies, card issuers, acquirers, third party acquirers, technology firms executing the payments and providing communications, see Figure 1), that are related by contracts involving many different types of agreements (such as per transaction fees, value-related prices, explicit or implicit credit agreements).

In such a complex environment, it is necessary that the supervisor not only understands the relevant technology of a Fintech player but also knows the efficiency and profit gains it brings about, the cost structure of the firms, and the contractual terms with different operators. In a word, supervisors must know the “business models” of Fintech players.¹⁶

This is not going to be an easy task for supervisors. We have seen that Fintech players are diversified, and they rely on different and often novel and creative business models that evolve over time. In fact, the business model is the core of profitability of innovations and as such it is difficult to track and, even more, to predict.

In the case of Wirecard, knowing the efficiency enhancing technology, the source of profitability, and the company’s actual business model would have been important in identifying possible sources of risks. Piercing the veil of ignorance that was surrounding the real activities and efficiency gain of this company would have avoided the hype surrounding the company, certainly more effectively and quickly than what we have observed. The discussion of the Wirecard case in the previous pages also shows that the perimeter of business models should expand in the case of holding companies, because slicing supervision by activities only gives a partial and insufficient view. Failing to adopt a holistic approach in the evaluation of the full business model of a complex entity, like a holding company, makes a fertile environment for frauds to go unnoticed.¹⁷

Practically, supervisors should be able at least to classify business models of Fintech players into categories and/or Fintech firms in turn should be asked to self-select into a specific category of business models. One possibility could be to adopt a regulation like the Prospectus Directive, but where the lean documentation prepared by companies about their business models is addressed, confidentially, to the supervisors. Since this business models may evolve over time, it would be important to have in machine-readable form so that supervisors can regularly and effectively monitor changes.¹⁸ Clearly, this cannot be the only tool for supervision, and will not be the solution to all problems mentioned above. This relatively simple exercise at least would allow for more transparency that would benefit supervisors, auditors, and ultimately markets.

¹⁶ The importance of business model also resonates with the opinion of the European Commission’s Expert Group on Regulatory Obstacles to Financial Innovation discussed in its Thirty Recommendations on Regulation, Innovation and Finance report (ROFIEG, 2019).

¹⁷ Consistent with this idea, the Commission in its Communication on the Digital Finance Strategy is investigating if the supervision of groups in financial service legislation is still effective in regards of technological innovation in financial markets (European Commission 2020c).

¹⁸ Machine-readable reporting to supervisors is proposed and sustained in European Commission (2020c).

3.4.1. Regulatory Sandboxes

A useful tool that authorities are quickly adopting across the world is that of “Regulatory Sandboxes” (see Ehrentraud et al. 2020). The idea is to offer Fintech players a controlled environment for testing innovations, in terms of technologies and or business model, directly interacting with supervisors and in some cases also having access to temporary regulatory forbearance. In some jurisdictions and for specific applications (e.g. in the case of electronic money, in several countries), the sandbox is also part of the authoritative and licensing procedure. By testing Fintech innovations before market deployment, authorities may gain better access to the business model that Fintech players contemplate, still guaranteeing legally protected discretion. At the same time, Fintech companies can assess the view of supervisors on their business models and potential source of future conflict. Furthermore, better predictability of the regulatory approach can foster more and faster innovations in the financial markets.

These are all good reasons to be very positive with the approach of regulatory sandboxes. At the same time, we cannot underestimate some possible issues. The fact that a Fintech operator is or has gone through a regulatory sandbox may be perceived by markets and by not-experts as a sign of quality or supervision’s approval, which is not necessarily the case. Furthermore, as explained above, business models evolve over time also in response of changed competitive conditions. This requires finding a way to keep track with these evolutions, for example by asking Fintech players to remain in contact with the innovation hub that runs the sandbox. Although an open dialogue between supervisors is certainly desirable, for the reasons explained above, it is still generally better to avoid too close and repeated interactions between supervisors and supervisees. The risk of capture is undeniable, and it can materialise in subtle ways, such as a too-light-touch, forbearance and blindness in favor of courted national champions, as we further elaborate in the next section. Taming this risk of capture is important and can be addressed clearly separating the activities and teams of sandboxes and innovation hubs from supervisory teams.

3.5. “Know the global picture: International cooperation”

Fintech players, especially those unbundling and specialising in narrow segments, have shown a natural tendency to cross border activities. This is expected, as with specialisation firms need to tap new markets rather than new businesses.

At the same time, we have discussed the many ongoing and future regulatory and supervisory reactions to Fintech expansion that are pursued in countries across the globe, like for example Regtech and Suptech and the regulatory sandboxes (see sections 3.3.2 and 3.4.1).

These regulatory experiments risk of favouring an uncoordinated and fragmented oversight of the Fintech industry. And of offering yet another dimension for regulatory arbitrage, that across boundaries. This situation is reminiscent, but to some extent worse, of the status of regulation and supervision of cross-border banks before the Banking Union. It is worse because, large and systemic banks were few and easy to identify, with clear and significant incentives for national authorities to sit down and design a coordinated regulatory and supervisory environment. With Fintech, actors are many, agile, small startup companies, that enter and exit markets quickly, being mostly based on digital intermediation.

In addition, an issue in common with the regulation and supervision of large cross-border banks is the risk of capture by promising national champions. This risk in fact compounds with the lack of international coordination and of common standards. Notably, capture of the supervisor does not necessarily take place with the extreme form of corruption and explicit wrongdoing. In a fast-growing

sector with Fintech, significant unchartered risks can quickly pile up by means of simple forbearance towards national champions that benefit of an allure of efficient and fast-growing firms.

The case of Wirecard highlights how crucial these issues are. The global reach of the company was significant, with the obvious problem that in the payment systems we lack unified supervision and different national standards apply on, for example, interoperability of enabling technologies. When a Fintech player in this business outsources part of its activities to a third-party, national supervisors normally have access to information about these external operators only if they are located within national boundaries. As soon as these activities take place cross-border they become almost impossible to scrutinise in a unified way.

As usual, solutions to the issue of lack of coordination and harmonised standards are not easy to fix. The history of the European Union is rich in this dimension. The effort that is normally required is significant, but not impossible especially in situations of crisis, as the case of Banking Union has shown. We see this process of harmonisation and coordination, in the case of Europe, as a necessary ingredient of the Capital Market Union. The recent Digital Finance Package (European Commission 2020a-c) in fact emphasises the role of cross-border coordination of supervision of innovative financial services, such as with the many national initiatives of regulatory sandboxes and the European Forum of Innovation Facilitators.

A European authority supervising Fintech independently of their corporate structure, e.g. being them financial or technological companies, may offer the unified big picture needed to address issues of customer protection and financial stability like those emerged in Wirecard. But we do not think that Fintech players and the Wirecard case provide a compelling justification for such a new European Authority. As discussed in the previous pages, the potential issues generated by Fintech players should be addressed in the area of regulation and supervision of financial intermediaries, with the objective of customer protection and financial system stability. In the case of investor protection, in our view there are no crucial differences between Fintech and other corporations with complex business models. In each of these areas, customer protection and financial stability, the European Banking Authority (EBA) and ESMA may be put in the position of guaranteeing harmonised and coordinated actions across Europe, which will then be exercised by national competent authorities.

We rather think that supervisors and regulators, both European and national ones, should be endowed with new and harmonised powers and instruments, as argued in the previous pages. After all, Fintech companies emerge out of innovations and, in many cases, they start operating at a small scale. We think that a fully integrated European oversight may stifle innovation of Fintech startups, as European compliance may easily become burdensome for emerging and innovative companies. Furthermore, some regulatory competition across national jurisdictions may be itself beneficial, pushing regulators and supervisors to explore new and unchartered territories.

In this proposed environment with acting national competent authorities and European agencies providing the appropriate frame, it is clearly key that harmonisation takes place. As mentioned above, a key starting point would be to adopt a common and simple set of definitions: although this may seem a detail, a uniform classification of the many different types of Fintech players, business models and innovative services in Europe is becoming an urgent necessity that should reflect into a coherent legal terminology. Also, uniformity of treatment should be guaranteed across all operators: similar Fintech as well as traditional players offering the same services. Coordination to guarantee this uniformity is necessary not only for a single market perspective, but also to allow European Fintech players to scale up in the European domestic market, often a precondition for further expansion. This uniformity of treatment for similar players is also the key for shared access to critical information of Fintech players

operating at the European level. Currently, for example, a Fintech player offering payment services with outsourced activities to third parties may be requested by national authorities to clarify the nature and extent of the outsourced activities, but only within national boundaries. As soon as these activities are performed in a different country, then the powers of inquiry of competent national authorities are very much diminished. This can be addressed extending this power of inquiry in the European area, for example by means of cooperation agreements for supervisory investigations, standardisation of information reporting for Fintech players and information sharing between national competent authorities, independently of the country of incorporation. Although this activity of coordination of national competent authorities is not going to be a simple endeavor and requires a careful and detailed design, we think the EU institutions (EBA, ESMA and possibly the Joint Committee of European Supervisory Authorities) can deliver the appropriate framework for coordination and cooperation.

CONCLUSION

According to currently available information, Wirecard's case is a classical accounting fraud. While it severely hindered investors, it left customers nearly unscathed. But its scrutiny has uncovered many loopholes, not only in the realm of investor protection, but also in the broader issue of regulation and supervision of Fintech companies.

While it is important to avoid stifling the efficiency gains that technological innovation can bring in the financial industry, regulation and supervision must remain effective in guaranteeing investor and customer protection.

With respect to investors, Wirecard's case calls for stronger national authorities, increased international harmonisation, coordination and cooperation, and direct and sound supervision of auditing firms. In fact, this is necessary not only in the case of Fintech companies, but more in general for all listed firms.

With respect to customers' protection, effective regulation and supervision of Fintechs is only possible with a thorough understanding of their business model and of the technologies that they use, to identify where the risks inherent in their activities lie. Attention must be paid to the role of operators that perform key technology-based activities for financial markets, which we have called *enhancers*, that are often unregulated, or subject to very light regulation.

Regulatory arbitrage must be avoided to ensure a level playing field between Fintech companies and traditional businesses, requiring that entities carrying the same activity follow the same sets of rules, however they carry them out. But this needs at the same time to be combined with the oversight of entities, and holdings in case of complex companies. Indeed, the Wirecard lesson is that a partial oversight of an entity – i.e. Wirecard Bank AG and Wirecard Card UK – has allowed to contain the impact on customers but has left open substantial regulatory loopholes. Given the ample span of cross-border activities carried on by Fintech firms, harmonisation, coordination and cooperation are essential, but we see no need for a new regulatory agency at the European level: oversight can be guaranteed empowering existing authorities.

REFERENCES

- Barba Navaretti, G., Calzolari, G., Mansilla-Fernandez, J. M., and Pozzolo, A. F. (2017). Fintech and Banking. Friends or Foes? *European Economy – Banks, Regulation and the Real Sector* 2, 9-39.
- Barth, J. R., Caprio, G., and Levine, R. (2008). *Rethinking bank regulation: Till angels govern*. Cambridge University Press.
- Berger A.N., L.F. Klapper, R. Turk Ariss, (2009), "Bank competition and financial stability," *Journal of Financial Service Research*, 35(2), 99-118.
- Boot, A. W. (2017). The Future of Banking: From Scale & Scope Economies to Fintech 29. *European Economy*, (2), 77-95.
- Broeders, D., and Prenio, J. (2018). Innovative Technology in Financial Supervision (suptech) – The Experience of Early Users. Financial Stability Institute (FSI) Insights on policy implementation. Available online at: <https://www.bis.org/fsi/publ/insights9.pdf>
- Bundesministerium der Finanzen. (2020). Aufzeichnung für den Finanzausschuss des Deutschen Bundestags; Sachstandsbericht und Chronologie Wirecard. Berlin: Bundesministerium der Finanzen (Federal Ministry of Finance, Germany).
- Calomiris, C. W., and Gorton, G. (1991). The origins of banking panics: models, facts, and bank regulation. In *Financial markets and financial crises*, 109-174. University of Chicago Press.
- Calvano, E., Calzolari, G., Denicolo, V., and Pastorello, S. (2020). "Artificial Intelligence, Algorithmic Pricing and Collusion," *American Economic Review* (forthcoming).
- Castro, R., Clementi, G. L., and MacDonald, G. (2004). Investor protection, optimal incentives, and economic growth. *The Quarterly Journal of Economics*, 119(3), 1131-1175.
- Demirgüç-Kunt, A., Kane, E., and Laeven, L. (2014). Deposit insurance database. The World Bank.
- Dermine, J. (2017). Digital disruption and bank lending. *European Economy*, (2), 63-76.
- DeYoung, R., Evanoff, D. D., and Molyneux, P. (2009). Mergers and acquisitions of financial institutions: A review of the post-2000 literature. *Journal of Financial services research*, 36(2-3), 87-110.
- di Castri S., Hohl, S., Kulenkampff, A. and Prenio, J. (2019), The suptech generations, BIS working paper.
- Diamond, D. W., and Dybvig, P. H. (1983). Bank runs, deposit insurance, and liquidity. *Journal of political economy*, 91(3), 401-419.
- Ehrentraud J., Ocampo, D.G., Garzoni, L., Piccolo, M. (2020). Policy responses to Fintech: a cross-country overview, BIS Report.
- ESMA (2019) Opinion on a proposed emergency measure by BaFin under Section 1 of Chapter V of Regulation (EU) No 236/2012, 70-146-19, 18/02/2019
- European Commission (2020a), Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, September 24th, 2020, and Accompanying documentation.

- European Commission (2020b), Commission staff working document - Impact assessment report accompanying the document "Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014", September 24th, 2020.
- European Commission, (2020c), Communication on a Digital Finance Strategy for the EU, 24.9.2020, COM(2020) 591 final.
- European Parliament (2020), Resolution on emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, A9-0161/2020.
- Farruggio, C. and Uhde, A. (2015). Determinants of loan securitization in European banking. *Journal of Banking and Finance* 56, 12-27.
- Ferrarini, G. (2017). "Regulating Fintech: Crowdfunding and Beyond", *European Economy*, (2), 121-142.
- FSB (2019). Assesses Fintech developments and potential financial stability implications, report 14 February 2019.
- FSB (2020). Effective Practices for Cyber Incident Response and Recovery: Consultative document.
- Goodhart, Charles (1975). Problems of Monetary Management: The U.K. Experience. *Papers in Monetary Economics*. Reserve Bank of Australia.
- Hong Kong Monetary Authority (2019), High-level principles on artificial intelligence.
- KPMG (2020). "Report concerning the independent special investigation, Wirecard AG", Munich, April 2020
- Krahn, J.P. and Langenbucher, K. (2020). The Wirecard lessons: A reform proposal for the supervision of securities markets in Europe, SAFE Policy Letter, No. 88, Leibniz Institute for Financial Research SAFE.
- Mc Crum, D. and Storbeck, O. (2020). "Wirecard Deceit went Beyond its Fraudulent Asian Operations", *Financial Times*, September 23, 2020.
- Mc Crum, D. (2015). "The House of Wirecard", *Financial Times*, April 27, 2015
- Mc Crum, D. (2020). "Wirecard and me", *Financial Times*, September 3, 2020
- Netherlands Bank (2019). General principles for the use of Artificial Intelligence in the financial sector.
- OECD (2006). "Online Payment Systems for E-commerce", *OECD Digital Economy Papers*, No. 117.
- Panetta, F., and Pozzolo, A. F. (2018). Why do banks securitise their assets? Bank-level evidence from over one hundred countries in the pre-crisis period. *Bank-Level Evidence from Over One Hundred Countries in the Pre-Crisis Period*. Bank of Italy Temi di Discussione (Working Paper) No. 1183.
- Piotroski, J. D., and Srinivasan, S. (2008). Regulation and bonding: The Sarbanes-Oxley Act and the flow of international listings. *Journal of Accounting Research*, 46(2), 383-425.
- Pozzolo, A. F. (2009). Bank cross-border mergers and acquisitions: causes, consequences, and recent trends. In *The Changing Geography of Banking and Finance* (pp. 155-183). Springer, Boston, MA.
- Rajan, R. (1998). The Past and Future of Commercial Banking Viewed Through an Incomplete Contract Lens. *Journal of Money, Credit and Banking*, 30(3), 524-550. doi:10.2307/2601255ab.

- ROFIEG, 30 Recommendations on Regulation, Innovation and Finance – Final Report to the European Commission (December 13, 2019). Available at: https://ec.europa.eu/info/files/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.
- Salway, J. (2020). "Wirecard Collapse Exposes Gap in Payment Regulation", Financial Times, September 20, 2020.
- Strathern, M. (1997). 'Improving ratings': audit in the British University system. *European review*, 5(3), 305-321.
- Veron, N. (2020). The Wirecard debacle calls for a rethink of EU, not just German, financial reporting supervision. Accessed on October 12th, 2020 at: <https://www.bruegel.org/2020/06/the-wirecard-debacle-calls-for-a-rethink-of-eu-not-just-german-financial-reporting-supervision/>.
- Zeranski, S. and Sancak, I.E. (2020), The Wirecard Scandal: The High-speed Rise and Fall of a Fintech Company and Its Implications for Developed and Developing Economies, Oxford Blog of Law and Business.

Beginning with a discussion of the Wirecard case, this study highlights several lessons for the regulation and supervision of Fintech companies. Innovation in the financial industry brings both efficiency gains and new risks. To balance these two elements, regulators need a deep understanding of Fintech's technologies and business models. Because Fintechs can be very complex companies, there is a need for an approach combining the oversight of both entities and activities. The global scope of Fintech's activities also calls for convergence and coordination of rules and supervisory practices at the European level and beyond.

This document was provided by the Economic Governance Support Unit at the request of the ECON Committee).

PE 651.384

IP/A/ECON-BU/IC/2020-114

Print ISBN 978-92-846-7338-4 | doi: 10.2861/638448 | QA-04-20-613-EN-C

PDF ISBN 978-92-846-7339-1 | doi: 10.2861/011222 | QA-04-20-613-EN-N