POLICY INSIGHTS
Thinking ahead for Europe

No 2018/12, October 2018

Cyber finance challenges demand a unified response

Karel Lannoo

The biggest opportunities and threats in finance these days come from the cyber-sphere. Fintech firms (fintechs) have made big inroads in financial intermediation, and some new companies are valued more than large banks. Blockchain and robo-advice are expected to revolutionise the ways banks interact with their clients and structure operations internally. The use of cryptocurrency has created a big controversy in central banking circles about the creation of a new form of money outside the classic institutions.

But more cyber could also create more threats for operational failures of systems, or huge thefts of data. Fintech is depriving banks of important sources of revenue and raising questions about the adequacy and sustainability of bank business models and their legacy systems. Blockchains may in theory be very secure, but the technology is still immature and they are very energy intensive. Cryptocurrencies facilitate money laundering and reduce financial inclusion, or may be simply Ponzi schemes. Robots store large amounts of private information, but how the data are used and the reasons why certain products are recommended to clients may be very opaque.

Innovation in the financial sector should be welcomed, but the policy response is not uniform, either at the global or European levels. Ten years ago, the G-20 managed a coordinated response to the challenges posed by the financial crisis. This led to a series of rules, which were well implemented, both in the EU and globally. This time is different. Cryptocurrencies are seen

Karel Lannoo is the Chief Executive Officer at CEPS. This article benefitted from discussions at a Roundtable organised by Tortoise with Ana Botin, Chairman of Santander in Brussels on 6 June, and at a workshop of the Institute for Finance and Governance, Beyrouth. It builds upon a presentation for BoNYMellon in London on 2 October. Research assistance by Inna Oliinyk is gratefully acknowledged.

978-94-6138-702-8

Available for free downloading from the CEPS website (www.ceps.eu)

as an opportunity for small or rogue countries to escape from the dominance of the big reserve currencies. Some countries have adopted rules to facilitate ICOs, and have high volumes of issuance, while others are resisting. Approaches also differ for regulating fintechs: some are registered as banks, others under a much lighter scheme, or following the practice of a regulatory sandbox. Cybersecurity problems require global or at least regional responses, but some G-20 members seem to openly or secretly use it as a 'weapon of mass destruction'. Only the US has managed to achieve a coordinated response by its regulatory authorities, but this is not much use in today's geopolitical context.

This Policy Insight assesses the impact of innovation in the cyber-sphere on finance, addressing the central question of whether the policy response is adequate. It starts by discussing broader fintech developments, followed by blockchain and cybersecurity issues.

What's new about fintech?

What is different in the current wave of technology adoption in the financial sector? The banking sector has been going through different phases of technological change since the 70s, from the introduction of large mainframe computers to the internet and digitalisation from 2000 onwards, to mobile banking and the use of artificial intelligence (AI) today for marketing and robo-advice. So is it more the real threat of new entrants and consequent disruption of traditional bank business models that has made the debate more acute now than before?

Fintech refers to the use of technology and innovation to provide financial products and services. It covers payments, loans, capital markets advisory and back office operations. So far, the shift seems to be most pronounced, and threatening to banks, in the retail payments sector, as indicated for example by the Adyen IPO. But even within the payments sector, newcomers compete with incumbents such as credit card providers and first phase start-ups. Overall, the market cap data indicate that, even for the traditional players, markets value payments providers more than banks, even in the US. This possibly indicates that markets fear non-transparent loan portfolios, legacy costs or unclear business models more than just utility functions. Paypal, one of the first wave newcomers and a spin-off of E-Bay, has a market value comparable to that of Goldman Sachs, for example. At its IPO, Adyen surpassed the market value of some leading European banks, and remains highly valued (see Annex). In addition to the specialised payment providers, there are also the Big Tech companies: Apple, Google, Facebook, Amazon have entered the retail finance space, and are a threat to the banks, but no separate data are available.

Table 1. Payment Services Providers, some key data (September 2018)

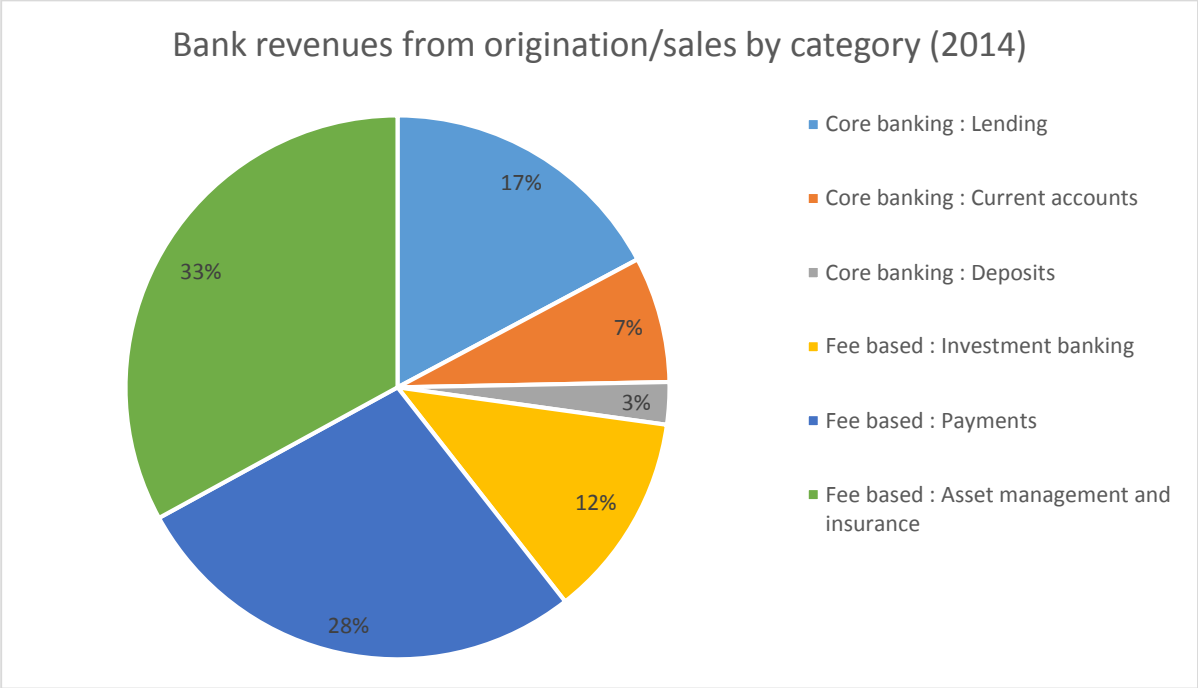
Company	EU licence	Gross revenue in 2017 (in € bn)	Revenue per employee in 2017 (€ m)	Market capitalisation (€ bn)[1]
VISA	Credit card network	15.24	1.11	278.67
MasterCard	Credit card network	10.38	0.86	188.84
Amex	Payment services provider	27.78	0.60	79.27
Paypal	Banking licence	10.86	0.65	91.59
Alipay	Payment services provider	10.59	0.17	127.50
Worldpay	Payment services provider	4.87	3.29	26.17
Wire Card	Banking licence	1.49	0.33	21.84
Adyen	Banking licence	0.95	1.47	15.62
Transferwise	E-money institution	0.78	0.56	1.38
Western Union	PSP and bank licence	4.58	0.41	7.25

Source: MarketWatch, company websites.

These newcomers have eaten a substantial (but seemingly unattractive) share of bank's revenues. Payments and transactions represent the second largest share of revenue for global banks, behind asset management and insurance fees, but well ahead of loan origination and interest income (Figure 1). Between 10 to 40 percent of bank revenues (depending on the business model) could be at risk by 2025, it is estimated (Dietz, Khanna, Olanrewaju, & Rajgopal, 2015). Fintech start-ups are likely to cause lower prices and cause further margin compression. They are not hampered by the cost of physical distribution networks, and, in addition, they have the capacity to exploit the data analytics of their users, to possibly move into lending, the core banking activity. The expectation is that payments markets will grow further, given healthy underlying fundamentals, including electronic-transaction and digital-commerce growth, and increasing cross-border activity.

[1] Market cap figures as of early September 2018

Figure 1. Bank revenues by category



Source: "Cutting through the FinTech noise", McKinsey, 2015.

Other segments of the fintech market are not yet so fully developed. E-lending and crowdlending are still in their infancy, or are advancing more within banks rather than as separate entities (and in Europe have not grown as rapidly). The same applies for capital markets advisory functions, such as robo-advice, which are being developed both within incumbent capital market players often in cooperation with large consulting firms and also at start-ups. On the back-office side, blockchain could become a powerful technology to facilitate the processing of transactions in, for example, clearing and settlement or for intra-group transactions. This is discussed more in detail below.

What's new is that never before has there been such an effect on the traditional bank business model of vertical integration of processing and horizontal breadth of supply of a whole variety of financial products. It seems that technology now is making possible what was not possible before. Banks will need to come to terms with the fact that this diversity of supply is no longer competitive, and that they will need to question the effectiveness of the combination of their different business lines.

EU regulation in the sector has followed the different waves of technology, from the e-money directive in 2000 to the payment services directive, and its update in 2017, and there is more to come. But horizontal directives also come into play, such as GDPR, because of privacy protection, and electronic signatures (eIDAS). The different licences used by payment services providers (see Table 1) indicate that there is no real consistency, or that differing business models lead to different licences and different forms of regulation. This diversity of approaches, and the impact on cross-border activity, is the main reason why the Commission submitted its proposal on crowdfunding providers in March 2018 (European Commission , 2018). But this

only tackles one very small segment of the fintech scene, and this reasoning has not yet been followed by the Commission for others.

The diversity of regulatory approaches also has significant implications for supervision. Banks are much more tightly supervised than a payment services provider under PSD or an e-money institution following the e-money directive. On the other hand, several European payment providers operate with a banking licence, as can be seen in Table 1, and are thus subject to the same regulation as a bank. But again, as they do not have a loan portfolio or do not take deposits, the supervisory approach will be much lighter.

Table 2. Main pieces of regulation in the fintech sphere

Legislation	Scope	Impact
E-Money Directive II (2009/110/EC), repealing Directive 2000/46/EC	Banks, e-money institutions, national banks and the ECB.	• Emergence of new market participants; • Increased competition; • Easier market access and enhanced consumer security.
Payment Services Directive II (2015/2366/EU), repealing Directive 2007/64/EC	Payment Initiation Services. Account Information Services, banks.	• Better integrated EU payments market; • Enhanced consumer security; • Increased competition.
Directive on distance marketing of financial services (2002/65/EC)	All financial services providers	• Increased transparency; • Proper legal redress; • Strengthened Digital Single Market and increased number of cross-border operations.
Regulation on traceability of money transfers (2015/847/EU)	Transfers of funds sent or received by payment service providers or their intermediaries	• Preventing, detecting and investigating money laundering and terrorism financing; • Increased transparency of operations.
Prevention of use of financial system for money laundering and terrorism-financing purposes (2015/849/EU)	All financial sector participants	• Enhanced customer due diligence; • Stricter risk assessments; • Limitations on e-money.
Proposal on European Crowdfunding Service Providers (draft)	Investment-based or lending-based crowdfunding services	• One-stop-shop access to EU market; • Enhanced consumer protection; • More investment/funding opportunities.

Source: European Commission.

There is further regulatory divergence with the PSD2 and other Directives. The Commission has recently revised the Payment Services Directive, aiming to spur innovation in the payments sector. The revision mandates more secure ways of connection to payment accounts while opening up the market to third-party providers (i.e. fintechs). Screen scraping of payment

accounts will be banned starting from September 2019.[2] Instead, fintechs will have to use a dedicated interface (Application Programming Interface) or secured customer interface (screen scraping+) provided by banks to connect.

While such a move is of obvious benefit for consumer privacy, its impact on banks and fintechs is still unclear. Fintechs claim that banning screen scraping would grant banks a gatekeeper role. Controlling the data flows could constrain the activities of fintechs and access to the data needed. Implementing provisions are currently being developed by the European Banking Authority (EBA). Nevertheless, the absence of common EU technical standards for dedicated interfaces remains an issue, as the EBA did not clarify technical specification for APIs. Hence, banks will develop their own APIs, which may create operational complications for third parties. With more than 8,000 banks, fintechs will struggle to configure each connection separately (Oliinyk & Echikson , 2018).

Banks on the other hand are threatened by the increased competition from the newcomers. Ana Botin, chairman of Santander, said that PSD2 gives an unfair advantage to big tech firms in terms of funding costs and customer base. While big tech firms can obtain customer data from banks, they are not obliged to share the data in return, which puts traditional banks in an unfavourable position (Financial Times, 2018). Furthermore, big tech firms have sufficient market clout for fair competition rules to also come into play.

Additional complications stem from overlaps and incoherence between the rules. PSD2 overlaps with and/or contradicts many other important Directives and Regulations. For example, the Commission acknowledges a large crossover between PSD2 and EMD2 (European Commission, 2018), while the European Data Protection Board has confirmed the overlap between PSD2 and GDPR (The European Data Protection Board, 2018). This further supports the call for more coherent and harmonised digital regulation in the EU.

Blockchain and cryptocurrencies

Blockchain is the subject of much hype today, but it is still an immature technology. It allows for decentralised record-keeping in distributed ledgers, or databases, shared across public or private computing networks. Every piece of information is validated as a new “block” in the chain of historical records. This decentralised structure promotes competition, but entails inefficiencies. There are public blockchains and permissioned private blockchains. Consultants estimate that blockchain is still three to five years away from feasibility at a broader level, primarily because of the difficulty of resolving the “co-opetition” paradox to establish common standards (Carson, Romanelli, Walsh, & Zhumaev, 2018). Some have compared it to the emergence of the World Wide Web in the early 90s, which also required some fundamental governance issues to be resolved before it could take off.

[2] Screen scraping is a way for third party providers to access consumer bank account data. They enter, store and re-use consumer credentials to access the data needed to provide the service.

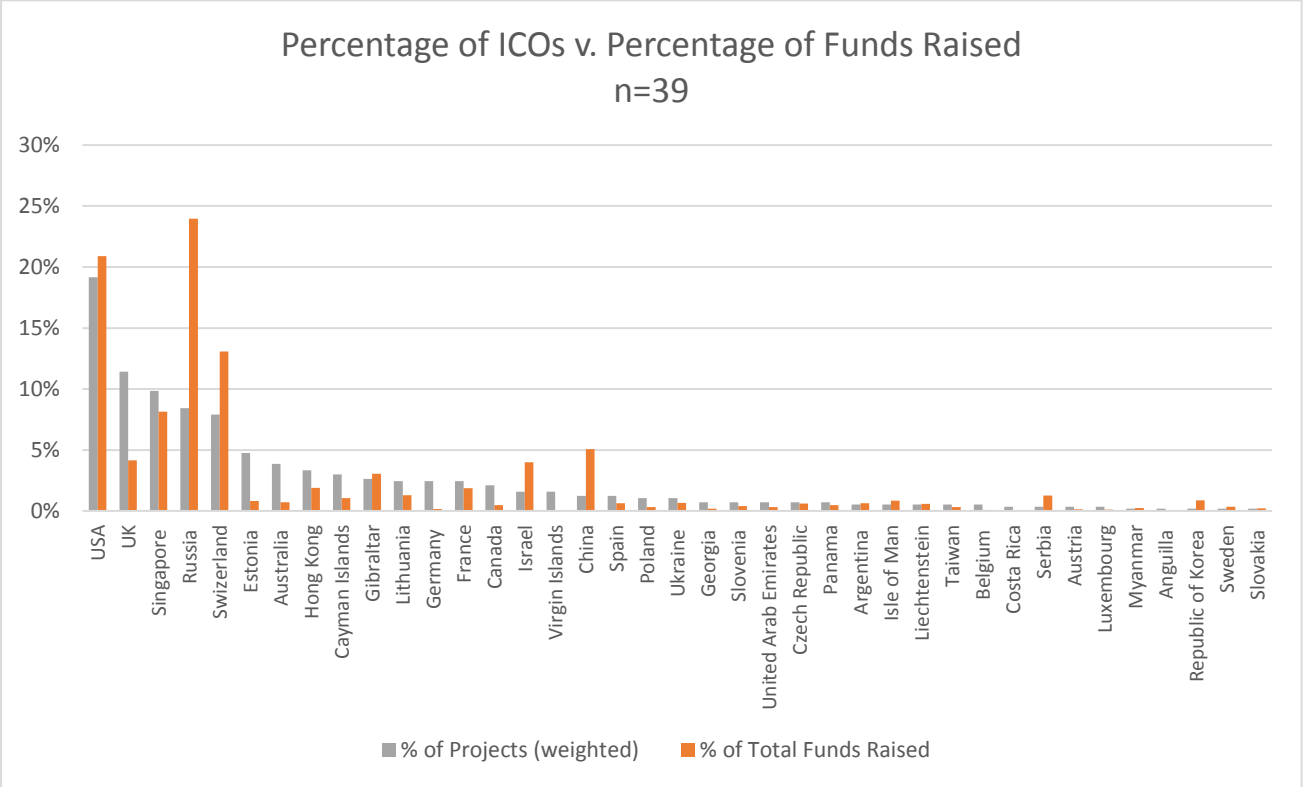
At the micro level, private blockchains are already used, in private computing networks, with controlled access and editing rights. Permissioned blockchains allow for optimising network openness and scalability. Private blockchains are expected to have a high potential for managing and integrating back offices in the financial sector, in, for example, reducing the costs of cross-border payments, in the clearing and settlement of securities transactions, in the reporting of transactions for regulatory purposes, or for managing risk in the insurance sector. However, difficulties remain, as a widely announced network for equities clearing to reduce back-office reconciliation work for its member-brokers was recently put on hold by the Australian Securities Exchange.

EU rules have already created the context for blockchain to be effective in securities processing through the requirement for interoperability among operators. This applies in the regulation for central securities depositories (CSDR) and the market infrastructures regulation (EMIR). Hence, because of the obligation to offer access to these service providers at different stages in the value chain, blockchain networks could exploit system inefficiencies and create more competition to securities markets infrastructures, which largely remain vertically integrated.

Even more hyped today are cryptocurrencies based on blockchain technology. Cryptocurrencies have created a deep controversy among central bankers whether they could be considered currencies. They have stated that cryptocurrencies are not, and cannot be a storage of value or a unit of account, although the fervour of their positions indicates that they are unsure. They specify that cryptocurrencies lack the scalability and finality of payments. During the BIS general meeting in June 2018, several speakers, starting with the BIS General Manager, Agustin Carstens, highlighted the shortcomings of cryptocurrencies. They called for "global coordination to prevent abuses and to strictly limit interconnections with regulated financial institutions. (…) Cryptocurrencies cannot undermine the role of central banks" (BIS, 2018).

Markets and regulators have not waited, however. Certain countries, including some G-20 member countries, accept Initial Currency Offerings (ICOs) as securities or commodities offerings. In the US, securities laws apply for SEC, commodities for CFTC, and the platforms where they are traded are like regulated trading infrastructures. Regulated guidance by authorities has increased considerably recently (NERA, 2018). In Europe, a variety of approaches prevails, with a very lenient attitude by some authorities, most clearly in Switzerland, for a total value of offerings in Europe that is much higher relative to the number of ICOs launched (Figure 2). Earlier this year, new legislation came into force in France to allow for distributed-ledger technology for the issuance of securities as long as those securities are neither listed on a regulated market or a trading facility organised under MiFID, nor admitted to the operations of a CSD (The DLT order). In the Middle East, several countries with weak currencies have adopted very lenient attitudes towards cryptocurrencies as a way to break the dominance of the large reserve currencies. They plan to develop a blockchain economy (i.e. Dubai, Estonia, Tunesia, Cyprus, Lebanon). But by far the highest value of funds raised is in the US, with over $1 billion so far. The total value of bitcoins outstanding is estimated at $210 billion today (source: coinmarketcap.com).

Figure 2. Percent of ICOs v. Percent of Funds raised, October 2018



Source: ICOWatchList.

Cybersecurity in finance

Cybersecurity issues lie beneath all these different developments, but they are not new either. The main concerns today are related to dependence on IT, the leakage and hacking of systems and the related operational or even financial stability risks. But systems have evolved enormously in the domain of data storage and protection. Silent facilities, which were a big issue after 9/11, have become obsolete with the emergence of cloud technology. Global securities trading systems have faced quite some stress moments during the financial and sovereign crisis, but have resisted. Derivatives markets have become more interconnected through mandatory clearing by central counterparties (CCPs), and thus more critical.

It is clear that cybersecurity can best be dealt with at EU or global level, but the initiatives needed have barely started. Data privacy is regulated at EU level, as are financial market infrastructures and operators, but the implementation is largely in the hands of the EU member states. Sometimes the requirements vary across different rules, and there is no European authority really in charge of supervision. The ECB has stepped up its activity in this domain, with the announcement of an initiative to test and simulate cyberattacks (in TIBER-EU), and the European Banking Authority has issued guidelines. From its side, ENISA (EU Agency for Network and Information Security) is in charge of the IT dimension, but it is clear that this is a cross-cutting issue that requires a much more coordinated approach. Following President Juncker's 2017 State of the Union initiative, ENISA was to be given a more central role, but the proposal

has been watered down in EU Council and Parliament. Personnel-wise, it will only translate into a staff increase of 40 for ENISA, with an increased advisory role for the EU but a very limited operational capacity.

In recent reports, (CEPS, 2018a) (CEPS, 2018b) we called for:

- A harmonised taxonomy of cybersecurity and cyber-incidents;
- A common EU approach to software vulnerability disclosure and incidents;
- The alignment of reporting requirements in EU directives and regulations, and harmonisation of templates for reporting where possible;
- The sharing of data amongst supervisory authorities, and between supervisors and banks;
- Reliable EU-wide statistics;
- A European cyber-certification scheme;
- Reinforcing cross-border cooperation and an improved process of attribution and criminalisation;
- A crisis management structure and the need for remedies in case of attacks.

This list alone indicates that much remains to be done. Without taxonomy, there are no common statistics and no comparable reporting, making it difficult to launch EU-wide cooperation. In addition, how can international cyber-attacks be dealt with if supervisory and judicial frameworks are mostly national?

The recent cases of large-scale money laundering through the European banking system have indicated that the EU is also not ready for cyber-threats to the system. Digitalisation and other technological advances have facilitated and accelerated money transfers, but also created possibilities for abusing the system. The response so far is the greater cooperation between member states included in the fifth money laundering directive, and an enhanced role for the EBA, though with very limited means. It is however clear that this will not be sufficient, even more so because of the cross-sectoral nature of the problem. In an editorial on 5 September, the Financial Times called for a separate AML agency (Financial Times, 2018).

The same applies for cybersecurity. Relying on cooperation between a variety of national supervisory authorities will not work if rogue states are trying to crack holes in the system. A European data shield will be needed, as Commissioner Katainen has called for, EU-wide surveillance and an EU-wide response. Any less will be far from sufficient.

Conclusion

The challenges and threats to the financial system, 10 years after the financial crisis, have changed radically. European banks are in a much better shape: they have deleveraged and their core capital (CET1) levels have doubled. The perception of the markets is different, however. European banks are facing challenges from fintechs, from blockchain technology and on the cyber-security front, which are fundamentally threatening their business model.

10 years ago, the response to the financial crisis from world leaders in the G-20, with its first meeting in Washington in November 2008, and the ensuing meetings in London and Pittsburg was unified. The current response at global and European levels to new threats to the financial system is not. Payment system providers are affecting profitability at banks, but they are regulated and supervised in different ways at the EU and global levels, or they are part of big tech firms that have huge market clout and thereby generate deep level-playing-field issues. Blockchain technology is advancing, and may become a fundamental challenge for the way in which banks and infrastructures process transactions. The technology is used for crypto currency offerings, which have seen a significant take-off in some countries. The response from regulators is very diverse, however, and there is certainly not a common European approach. Much also remains to be done on the cybersecurity front, and the massive recent money laundering cases have demonstrated how porous European surveillance can be.

If the EU, and the world at large wants to meet the challenges raised by cyber finance, a far more unified response is urgently required.

Bibliography

BIS (2018, June 25), *Speech by Agustín Carstens at the AGM.* Retrieved from BIS: https://www.bis.org/speeches/sp180704a.htm

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018, June), *Blockchain beyond the hype: What is the strategic business value?* Retrieved from Digital McKinsey : https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

CEPS (2018a), *Cybersecurity in Finance.*

CEPS (2018b), *Software vulnerability disclosure in Europe, Technology, Policies and Legal Challenges.*

Dietz, M., Khanna, S., Olanrewaju, T., & Rajgopal, K. (2015), *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks.* McKinsey & Company.

ESMA, EBA, & EIOPA (2018, September 5), Joint Committee Report . *The results of the monitoring exercise on 'automation in financial advice'*.

European Commission (2018, March 8), FinTech Action plan: For a more competitive and innovative European financial sector. Brussels.

European Commission (2018, March 8), Proposal on European Crowdfunding Service Providers (ECSP) for Business. Brussels.

European Commission (2018), *Report on the implementation and impact of Directive 2009/110/EC in particular on the application of prudential requirements for electronic money institutions.* Brussels: European Commission.

Financial Times (2018, September 5), *Europe needs a central anti-money laundering body*. Retrieved from https://www.ft.com/content/0b2476e4-b02b-11e8-99ca-68cf89602132

Financial Times (2018, April 17), *Santander chair calls EU rules on payments unfair*. Retrieved from Financial Times: https://www.ft.com/content/d9f819f2-3f39-11e8-b7e0-52972418fec4

NERA (2018), *Recent Trends in Virtual Currency Regulation, Econforcement and Regulation.*

Oliinyk , I., & Echikson , W. (2018), *Europe's Payments Revolution: Stimulating Payments Innovation while Protecting Consumer Privacy.* Brussels: Centre for European Policy Studies .

The European Data Protection Board (2018, July 5), Letter. *Regarding the revised Payments Services Directive*. Brussels: EDPB.

Annex

Source: Market Watch.