CHAMBERS

Global Practice Guides

FinTech

Law & Practice – Poland

Contributed by

Soltysinski Kawecki & Szlezak

2018

CHAMBERS® AND PARTNERS

POLAND

The 'Law & Practice' sections provide easily accessible information on navigating the legal system when conducting business in the jurisdiction. Leading lawyers explain local law and practice at key transactional stages and for crucial aspects of doing business.

Contributed by Soltysinski Kawecki & Szlezak ***Authors:*** Dr Marcin Olechowski, Agata Szeliga, Dr Wojciech Iwański, Katarzyna Paziewska

Law and Practice

Contributed by Soltysinski Kawecki & Szlezak

CONTENTS

POLAND LAW AND PRACTICE

Contributed by Soltysinski Kawecki & Szlezak ***Authors:*** Dr Marcin Olechowski, Agata Szeliga, Dr Wojciech Iwański, Katarzyna Paziewska

Soltysinski Kawecki & Szlezak (SK&S) is a leading Polish full-service firm established 1991 with a team of over 130 lawyers. FinTech matters are handled by interdisciplinary teams composed of lawyers from the financial regulation, privacy and IP/IT practices. Key practice areas involved in FinTech work are financial regulation/banking and finance, e-commerce and IT, IP, personal data protection (privacy) and corporate and commercial transactions. Recent key projects include ongoing advice on the Payment Services Directive/PSD2 to banks and non-bank service providers, and representing Microsoft in matters related to the offering of cloud services to regulated entities from the financial sector.

Authors

Dr Marcin Olechowski is a partner and the head of financial regulatory/banking and finance practice, who regularly advises financial sector clients and service providers on regulatory and client documentation issues concerning the online and mobile provision of financial services, new product development and other FinTech-related matters, including Bitcoin. Dr Olechowski, who also practises in M&A and international arbitration, is involved in a project aiming to implement distributed ledger technology as a sectoral solution in the Polish banking industry for client documentation. He lectures at the Warsaw University Faculty of Law on banking law, including FinTech, and sits on the supervisory board of Mediacap SA, a publicly listed leading Polish marketing and communications group focused on applying big data, video online and machine learning solutions in marketing and communications.

Agata Szeliga is a partner and head of personal data and privacy law practice, who practises in personal data and privacy law, IP law (including IT and cloud computing) and public aid and public procurement. Ms Szeliga represents clients before Polish and EU authorities, including the General Inspector of Personal Data Protection and the Electronic Communication Office, where she is an arbitrator in the consumer conciliation court, and regularly advises clients on privacy matters and new technologies. Ms Szeliga completed postgraduate studies in copyright, publishing and press law at the Institute of Inventions and Protection of Intellectual Property at the Jagellonian University in Cracow.

Dr Wojciech Iwański, a senior associate, regularly advises financial sector clients and service providers on financial regulatory and client documentation issues related to online and mobile provision of financial services, new product development and other FinTech-relevant matters (including Bitcoin). Dr Iwański, who also practises in securities and capital markets law, is currently involved in a project aiming to implement distributed ledger technology as a sectoral solution in the Polish banking industry for client documentation. His doctoral thesis concerned the impact of the Payment Services Directive on Polish regulation of e-banking services.

Katarzyna Paziewska, an associate, practises in IT, personal data protection and e–commerce. She advises financial sector clients and service providers on personal data protection regulatory and client documentation issues related to personal data processing, as well as on data protection implications for new product development (including blockchain). These include preparing and updating privacy policies for internet services users, as well as notifications, information and draft consents, and declarations concerning data processing; reviewing regulations regarding loyalty programmes; advising on personal data collection and transfers; advising in negotiations of data processing agreements; and assisting on issues related to conducting background checks on employees and subcontractors (a US client from the financial sector).

1. FinTech Market

1.1 The Development of FinTech Products and Services

As a result of leapfrogging in the 1990s/2000s, Poland benefits from a very modern financial services market, in terms of offers to customers, back-office and infrastructure.

Poland is at the forefront of technological advancement in Europe regarding the implementation of such solutions as contactless payments (including both card and HCE mobile payments), bank-branded pay-by-link payments, or sector-wide solutions such as the BLIK mobile payment service. National Bank of Poland data shows consistently increasing popularity for non-cash payments, and contactless payment instruments are currently used in more than half of all non-cash payments. The high popularity of mobile and e-banking (with almost 7 and 14 million active users, respectively) is driven by technological diffusion and customers' openness to innovation, as well as dynamic development of Polish transactional banking systems. Implementations that stand out, in both European and global contexts, include instant (express) transfer systems, "pure online" remote channels of financial product sales, Personal Finance Management (PFM), and remote customer service systems such as video advisory services.

A peculiarity of the Polish market is that significant innovation is implemented in banks; in fact, the most innovative banks tend to define themselves as part of the FinTech sector (or as FinTech banks). Paradoxically, this has somewhat limited the potential for development of other FinTechs, as the majority of Polish banks stand out in comparison to their European counterparts for using and offering very advanced card, online and mobile payment technology. This is helped by a state-of-the-art interbank payment infrastructure (including Europe's second instant payments system – Express Elixir).

1.2 The Market for FinTech Products and Services

Industry reports indicate that, apart from innovative banks, there are at least several dozen non-bank FinTech companies which are active in all main and globally known segments of the Polish market; entrepreneurs specialising in e-payments and financial platforms are the most numerous and mature group. Other strengths include data analysis, cognitive algorithms (machine learning), and sales channels development. Several distinct companies operate in social financing. There are also projects relating to the application of distributed ledger technology in financial services.

Key areas of the Polish FinTech market include:

- mobile payments – developed both by banks and by established payment organisations such as MasterCard and VISA;
- trading platforms, in particular offering access to the Forex market, with the involvement of predominantly non-Polish investment firms acting in Poland on a cross-border basis, but with the support of Polish-based IT companies;
- online currency exchange platforms, which enable "simple" foreign exchange transactions at limited costs. Their popularity is bolstered by a relatively high number of customers with foreign currency denominated /indexed mortgage loans and relatively high numbers of transfers by Poles working abroad; and
- short-term lending platforms – non-bank lenders (particularly those targeting consumers) have been aggressively growing their activities, including through the use of online lending platforms that offer short-term high interest ("pay-day") loans.

1.3 The Key Market Participants in the Specified Activities

Banks remain key innovators in Poland, implementing significant innovation both in the start-up model ("FinTech banks") by creating new banks or banking concepts from scratch (Alior Bank, FM Bank, Idea Bank), and within large, well-established multichannel banks that generate innovation on their own (such as mBank, PKO Bank Polski, ING Bank Śląski and Millennium Bank).

In particular, traditional financial service providers remain the key market participants in the payments industry. For example, a local mobile payment system operated by an inter-bank initiative is currently used by more than 2 million Polish customers. Banks also develop their own currency exchange platforms, enabling swift currency exchange and transfers, and at least some of them operate Forex platforms and/or closely co-operate with non-bank external Forex trading platforms. In those areas, new FinTech technologies/companies have not yet begun to displace traditional financial service providers.

Despite bank prevalence, industry reports indicate that Poland has at least several dozen non-bank FinTech companies in a variety of segments, from payments to data analysis. Most of these companies operate in a start-up/entrepreneurial model. Entrepreneurs specialising in e-payments and financial platforms are the most numerous and mature group. Polish FinTechs are largely geared towards collaboration with banks because, even though the former target directly the consumer market, they recognise the need for co-operation and mutual benefits resulting from it.

1.4 FinTech Technologies/Companies

Traditional financial service providers (mainly banks) generally continue to dominate the market, but are gradually being displaced in two areas.

One such area is online currency exchange, where the largest players are non-bank FinTech companies. One of the largest platforms, Cinckiarz.pl, has a volume of business in excess of PLN14 billion. In fact, the success of Cinckiarz.pl and similar enterprises has prompted some banks (Alior Bank, Raiffeisen Polbank, mBank, BZWBK) to develop their own currency exchange platforms to compete with them.

Another area is consumer lending, where non-bank lenders successfully compete with banks in offering consumer credit through online lending platforms (usually for short-term, high-interest loans). Again, this has prompted some banks to try developing similar online lending channels, but banks are generally hobbled in this area by a restrictive regulatory and prudential network, whereas non-bank lenders operate in a flexible regulatory environment, subject only to consumer credit and data protection regulations.

Non-bank providers are also active in payments services, where they usually operate as licensed payments institutions. Their growth in Poland is slightly less visible than in other markets, however, because Polish banks offer efficient payments infrastructure, thus reducing available "white space".

1.5 Partnerships Between Traditional Institutions and FinTech Companies

Traditional financial institutions (principally banks) have a history of partnering with FinTech companies, and quite a lot of innovative solutions have been implemented by banks in close co-operation with FinTech enterprises that were still start-ups during their first banking implementations. This is made easier by cultural similarities between the most technologically advanced banks and FinTechs ("FinTech banks" or "FinTech in banks"). A variety of models are present, from incubators/accelerators (such a programme is run, for instance, by the largest Polish bank – PKO BP) to acquisitions (for instance, PKO BP recently acquired ZenCard, a FinTech company operating in the innovative mobile payments market).

Most frequently, however, banks work with FinTechs based on outsourcing schemes, with FinTech companies acting as specialised service providers (subcontractors). Still, a significant number of innovations are also created by development, IT, and remote channel management departments in major Polish banks and well-established payment sector companies. Some banks have also recently started to invest directly in IT companies.

1.6 Approach to FinTech Innovation

Although Poland currently lacks special incentives targeted at FinTech development, the overall sentiment is clearly positive. Principal market players are open to innovation, financial services customers are tech-savvy, and Poland counts among the countries with the best software developers in the world. On the back of this, official government policy is geared towards encouraging innovation, with prominent government representatives expecting Poland to be in the "eye of the IT development cyclone".

1.7 Laws or Policy to Encourage Innovation

Although specific regulatory or legislative action has yet to be implemented, several important government initiatives are aimed at development of the FinTech area.

In June 2016, the government launched its #StartInPoland programme, an umbrella brand that encompasses the most important tools for supporting start-ups in Poland. The programme provides investment in start-ups by the Polish Development Fund and an expansion of accelerator programmes under the aegis of the Polish Agency for Developing Entrepreneurship. The government estimates that Poland has the potential to become a place in which 1,500 companies will emerge and thrive in the next seven years, creating high-quality innovative technologies capable of competing in foreign markets.

The Minister of Development and Economy is also spearheading a "Paperless, cashless Poland" initiative, a large-scale digitalisation project expected to affect many areas of administration operation. One of the core elements is to enable citizens to use their banking ID and password to log on to the social insurance board or local government sites to deal with administrative matters.

Finally, a dedicated FinTech working group has been jointly established by financial market authorities and stakeholders to review the legal framework and regulatory guidelines from the perspective of FinTech development. The group includes representatives from the Ministry of Development, the Financial Supervision Commission (KNF), the National Bank of Poland and the Polish Banks Association. To date, the FinTech Working Group has identified a number of regulatory barriers for further assessment.

2. Regulation

2.1 Regulatory Regimes for Specified Activities or FinTech Companies

Currently, there are no laws or regulations designed specifically for FinTech companies, but they are likely to be adopted in the near future. In particular, the FinTech Working Group is expected to propose legislative changes intended to lift

barriers to the development of FinTech in Poland. For the time being, particular areas of FinTech operation remain subject to sectoral regulatory regimes and/or general legislation related to consumer protection, among other matters.

Payments
Activity in the field of payments may be subject to a variety of regulatory regimes, depending on the nature of the operations. In particular, providing payment services – including acquiring and issuing payment instruments (including payment cards and payment devices) – is subject to the Polish implementation of the EU Payment Services Directive 2007/64/EC (PSD) (namely the 2011 Payment Services Act – PSA), and, as a rule, requires a payment services licence granted by KNF.

At the same time, mere payments processing is considered a non-regulated activity, subject only to certain regulated outsourcing regulations if the processing service is provided to banks. Processors carrying out standard processing activities on behalf of the acquirer do not require a payment services licence, as they benefit from the technical service providers exemption under the PSD/PSA.

Trading platforms
Operation of trading platforms usually involves brokerage services in respect of various types of financial instruments, such as access to Forex products. Such brokerage services, including intermediation in trading in financial instruments or providing individualised advice is subject to Polish legislation on trading in securities. The main regulation in the area of investment services is the 2005 Act on Trading in Financial Instruments (ATFI), which implements the EU's Markets in Financial Instruments Directive 2004/39/EC (MiFID).

Providing brokerage services requires a KNF licence, although a number of trading platforms operate in Poland based on an "EU passport" (discussed below).

Non-Bank Lending
As a rule, lending per se is not regulated in Poland, provided it is not financed from a deposit-taking activity. The prevailing view in Poland is that, in order to avoid the qualification of conducting a banking business without the requisite licence, the lending activities of non-banks should, in principle, be financed out of their own funds (and not from deposits of any kind).

If the loans constitute "consumer credits" within the meaning of the 2011 Consumer Credit Act (CCA), implementing Directive 2008/48/EC on credit agreements for consumers, non-banking creditors are qualified as "lending institutions" under the CCA, triggering certain limited regulatory obligations (registration with the KNF).

Mortgage Loans
Offering mortgage credits – including the operation of mortgage credit intermediators – recently became subject to a dedicated regulation under the 2017 Mortgage Credit Act, which implements the EU's Mortgage Credit Directive. As a result, mortgage loan intermediation – including the operation of online intermediation services – became a regulated activity requiring registration and subject to KNF supervision.

Insurance Mediation
Insurance mediation is a supervised activity under the 2003 Insurance Mediation Act (implementing the EU's Insurance Mediation Directive), with registration requirements for agents and licensing obligations for insurance brokers. The upcoming implementation of the Insurance Distribution Directive is expected to expand the scope of regulation in this area.

However, several areas remain unregulated, creating a sort of gray area that affects FinTechs' ability to operate. This particularly pertains to cryptocurrencies, crowdfunding and peer-to-peer banking.

Cryptocurrencies
Cryptocurrency (bitcoins, to be exact) has so far only been the object of tax interpretations (which instruct to treat cryptocurrency as economic rights, implying an obligation to report income only at the time of their exchange to a "traditional" currency) and warnings from supervisory authorities about the uncertainty of cryptocurrencies and their potential use for illicit activities (eg, warnings issued by the KNF in 2017 and by the National Supervisory Authority and General Inspector of Financial Information in 2014 and 2017). Thereby, out of caution, many entities in the cryptocurrency sector move their operations outside Poland in order to limit the risk of their activity becoming illegal or subject to regulations imposing excessive requirements.

Crowdfunding
Crowdfunding remains a regulatory grey area, insofar as the typical activities of a crowdfunding platform (accepting, storage and transfer of funds) meet the definition of payment services under the Payment Services Act and requires a KNF licence. Due to the burdensome nature of the process to obtain such a licence and relatively heavy prudential requirements, in practice crowdfunding platforms rely on a range of solutions to allow them to pursue their activity without having to secure a full payment institution licence (acting as a service bureau or a crowdfunding agent). However, these actions do not guarantee full certainty as to their "legality".

Peer-to-Peer Banking
Similar to crowdfunding platforms, peer-to-peer banking platforms operate on the fringe of regulated payment ac-

tivity and, in some cases, may be considered para-banking institutions. Therefore, the operation of such p2p platforms carries a high degree of legal risk, which significantly hinders their development.

2.2 Regulatory or Governmental Agencies for Specified Activities or FinTech Companies

The main regulatory bodies relevant for FinTech companies and the Specified Activities are the Financial Supervision Commission (*Komisja Nadzoru Finansowego* – KNF), the Office of Competition and Consumer Protection (*Urząd Ochrony Konkurencji i Konsumentów* – UOKiK), the Financial Ombudsman (*Rzecznik Finansowy*), and the General Inspector for Personal Data Protection (*Generalny Inspektor Ochrony Danych Osobowych* – GIODO).

KNF

KNF is the main financial markets regulatory authority and supervises traditional financial market participants (such as banks, investment firms, insurers and payment institutions, as well as certain financial services intermediaries), and their compliance with regulated outsourcing rules.

In particular, KNF issues prudential recommendations and guidelines affecting operation of established market participants in the FinTech market and their co-operation with FinTech companies. These include detailed recommendations concerning management of areas of Information Technology and security of the teleinformatic environment in banks, insurance companies and investment firms, as well as recommendations regarding the operation of OTC trading platforms.

Enforcement vis-à-vis licensed entities is essentially conducted by KNF, which has a range of regulatory instruments at its disposal (including fines and recommendations). Enforcement vis-à-vis unlicensed entities is usually initiated by KNF but conducted through law enforcement authorities.

KNF also maintains a public warnings list that identifies entities suspected or convicted of conducting regulated activities without the requisite licence.

UOKiK

The Office of Competition and Consumer Protection (UOKiK) is very active in the area of consumer rights enforcement. It takes action in respect of licensed market participants (especially banks and insurance companies), as well as non-regulated entities, such as non-bank lenders. Enforcement is conducted by UOKiK directly.

Financial Ombudsman

Since late 2015, the Financial Ombudsman is the new financial market customer protection authority. The Financial Ombudsman takes part in out-of-court dispute resolution between financial market entities and customers who are natural persons (whether acting as consumers or not).

GIODO

The General Inspector for Personal Data Protection (GIODO) is the main regulatory agency in charge of personal data protection issues. GIODO plays an important role through issuing position papers (no-action letters). Its enforcement powers include inspections and fines. GIODO's powers and importance are expected to increase significantly with the implementation of the EU's General Data Protection Regulation.

2.3 Capital and Liquidity Requirements

There are no general capital and liquidity requirements, affiliate transaction limitations or other regulatory requirements for FinTech companies as such, unless they engage in a regulated activity.

Typical regulatory requirements such as capital requirements, affiliate transaction limitations and risk management rules apply to banks, investment firms and insurance companies. In that respect, the Polish regulatory regime is harmonised with EU legislation applicable to particular types of regulated entities.

Payment institutions are subject to regulatory requirements resulting from PSD / PSA. In principle, the performance of such activity requires a KNF licence issued after a complex administrative procedure, provided that specific requirements, including capital ones, are met (tier 3 capital; the full payment activity may be provided by an entity with share capital of EUR125,000).

Non-bank lending institutions are currently subject to very limited requirements, including a minimum share capital of PLN200,000, paid in cash and which cannot result from loans or credits.

If a FinTech company co-operates with regulated entities as an unregulated service provider (insourcer), it is not subject to any specific capital and liquidity requirements or affiliate transaction limitations. However, reliability of the FinTech company (including its financial stability) would be subject to assessment and constant monitoring by the regulated entity.

2.4 "Sandbox" or Other Regulatory "Neutral Zones"

There are currently no "sandboxes" or regulatory "neutral zones" established in Poland. It is not possible to offer a product that would be marked in a special way and that met only limited legal requirements (organisational, capital, personnel or informational ones).

Establishment of such "sandboxes" is currently subject to evaluation by the FinTech Working Group. However, KNF representatives have previously expressed skepticism about regulatory "sandboxes" on policy grounds (risk for consumers). In addition, KNF is generally considered a conservative regulator and its strategic institutional goals do not include support for the creation and promotion of innovative solutions (these goals include, above all, ensuring stability, security and transparency on the market, creating market trust and protecting the interests of market participants).

2.5 Change of Control Approval Requirements

Change of control requirements apply in respect of typical regulated entities, such as banks, investment firms and insurance companies. The acquisition of qualifying holdings in such entities requires regulatory clearance from KNF. During the process, KNF reviews the new direct and/or indirect shareholders and their potential influence on the regulated entity in question.

Payment institutions have only limited reporting requirements in respect of changes in shareholding (and no established approach of the KNF).

Change of control over non-regulated FinTech companies does not require any special approval. However, outsourcing contracts under which such companies provide services to regulated entities may contain specific change-of-control clauses. Regulated entities' outsourcing policies may also require periodical reassessment of service providers and their ownership (other than antitrust approvals, where applicable).

2.6 Recent Developments or Notable Proposed/ Forthcoming Regulatory Changes

Substantial changes in the FinTech regulatory landscape are expected in coming months. Apart from the results of the FinTech Working Group (the direction of which is not yet certain), a number of legislative changes are expected to enter into force.

In particular, Poland should implement the Second Payment Services Directive (EU Directive 2015/2366 or PSD2) by mid-January 2018, fostering operation of payment services third party providers (TPP) and requiring account servicing payment service providers to allow TPPs' access to customers' accounts through a dedicated interface. Work on the implementation is pending.

Trading platforms will be affected by the future implementation of EU Directive 2014/65/EU (MiFID 2). Only the first draft of the bill of legislative changes has been published to date, but the new provisions are expected to affect financial instrument distributors (including operators of trading platforms) – particularly by imposing additional information requirements (eg, on remuneration and incentives received from investment firms). KNF is also proposing to adopt certain caps for the remuneration of distributors, but this issue has not yet been decided.

Still prior to the implementation of MiFID2, KNF spearheaded legislative work aimed at tightening supervision over the provision of investment services (investment advice in particular) to Polish customers, also by EU investment firms operating on a cross-border basis. Since the end of April 2017, the ability to provide marketing services (including various types of business introduction) in respect of investment services has been limited to investment firms themselves or their tied agents. The new law is targeted at business introducers of Forex platforms.

Moreover, the new Mortgage Credit Act (discussed above) will introduce extensive new requirements for mortgage credit distributors, and also those acting through the web.

2.7 Burden of Regulatory Framework and Protection of Customers

The regulatory burden of operation is relatively high for established market participants such as banks, investment companies and insurance companies, as well as their external service providers (insourcers). At the same time, a wide range of FinTech companies are still outside of any regulatory regime.

2.8 Regulatory Impediments to FinTech Innovation at Traditional Financial Institutions

Regulated Outsourcing

Legal provisions regulating the issue of outsourcing – and having a material impact on various types of FinTech services – have gradually been introduced in Poland in relation to different types of financial institutions, from banks through to investment firms, investment fund management companies (*towarzystwa funduszy inwestycyjnych* – TFI), alternative fund managers, insurance and reinsurance companies, and domestic payment institutions. Differences in these regulations have created a fragmented and non-uniform regime. A common point is that they are fairly restrictive, and that KNF takes a formalistic approach to their application.

The outsourcing-related provisions of the Banking Law are the most developed, as they identify two categories of activities that are subject to applicable outsourcing regulations.

The first category covers activities related to intermediation (understood very broadly) in the performance of banking activities, eg, concluding bank account agreements, credit agreements or loan agreements with natural persons. The catalogue of such activities is not exhaustive, but performance of intermediary activities other than those expressly mentioned therein requires a permit from KNF.

The second category of activities covers so-called "factual operations" related to banking activity. These operations are directly connected with banking activity and can usually be performed only with access to sensitive banking information (eg, client information, including information covered by banking secrecy) or operations ensuring continuous and uninterrupted functioning of the bank and performance of banking activities (eg, the functioning of IT systems used directly to perform banking activities).

Discussion is currently ongoing between Polish banks and KNF on whether the rules on banking outsourcing apply to standard IT services based on cloud computing solutions. KNF supports such qualification, claiming that the service provider of cloud services could potentially have access to processed data, including banking secrets.

As regards other regulations under Polish law, the following services are generally excluded from the regulated outsourcing rigors:

- services that do not fall within an exhaustive catalogue of activities that might be the subject of regulated outsourcing; or
- services that are classified as so-called "standardised services" (eg, services for the provision of market data or information on listings of financial instruments), and are therefore excluded from the regulated outsourcing rigours.

If services are classified as regulated outsourcing, the service provider will face various legal repercussions, notably including the following:

- the agreement for providing services would have to include certain provisions (including representations and warranties) usually required by regulated entities;
- the service provider would be subject to statutory restrictions related to exclusion of the insourcer's liability; and
- the regulated entity would be required to notify KNF of the conclusion of the outsourcing agreement or, in some cases, to obtain KNF's prior consent to conclude such an agreement.

The regulated entity has the regulatory duty to ensure compliance with the applicable provisions on regulated outsourcing, rather than the service provider. The potential classification of IT services as a regulated outsourcing service would depend to a great degree on the approach of individual regulated entities. In practice, some regulated entities (especially banks) tend to read the provisions on regulated outsourcing more broadly than the exact wording of these provisions implies.

AML

Regulated entities are usually subject to anti-money laundering rules under the Act on counteracting money laundering and terrorism financing (AMLA). This also applies to lending institutions (formally classified as "financial institutions") and EU credit institutions/investment firms acting through branch offices in Poland.

Such institutions are obliged to appoint one of their management board members as the person responsible for compliance with its AML obligations, and to apply so-called "financial safety measures" while entering into the agreement (eg, executing the account agreement), including proper identification of the customer and its beneficial owner. The law also requires that such financial safety measures are applied on an ad hoc basis if the transaction is in any way suspicious.

Unless qualified into any particular category of obliged institutions, non-regulated FinTech companies are not usually subject to AML obligations.

2.9 Regulatory Regime's Approach to Consumers and Small Business Customers

A relevant peculiarity of the Polish legal system is that, while consumer protection measures are aligned on the generally applicable EU framework, the practice of Polish consumer protection authorities and courts in this area is relatively restrictive. This is particularly true regarding general terms and conditions and other standard documentation used by regulated entities, in which case client documentation is monitored by both KNF and UOKiK.

A different approach is taken vis-a-vis non-consumer clients, including small businesses. UOKiK is not involved in their protection (unless the issue of unfair competition comes up). As discussed above, only the Financial Ombudsman is competent to protect the rights of entrepreneurs who are natural persons, but its authority is considerably limited.

2.10 Outreach by Regulators or Government Authorities to Engage with FinTech Innovators

The Polish financial market supervisory authority is actively involved in the evolution of the FinTech market in Poland. In late 2016, KNF became the co-ordinator of the FinTech Working Group, discussed above.

Also, despite its generally conservative outlook, KNF has so far been open to discussing innovative ideas with regulated entities, as well as compliance in terms of co-operation with non-regulated FinTech companies. Such discussions typically involve legal issues as well as technical ones.

2.11 Unregulated Specified Activities

Despite overregulation in particular areas of the financial market in Poland, certain FinTech fields remain unregulated.

Online currency exchange
The operation of online currency exchange providers is deemed to be out of the scope of supervision by both the National Bank of Poland (granting authorisations to "brick and mortar" exchange offices) and KNF, unless the exchange service is combined with maintaining payment accounts and/or enabling the clients to originate external transfers.

Crowdfunding
There is no dedicated legal regulation for crowdfunding. In the past, there was some dispute as to what extent laws applicable to public collections apply to crowdfunding, but the current position of the authorities is that those provisions apply only to cash collections (wire transfers or other forms of electronic payments are exempted). Depending on how it is structured, crowdfunding may trigger regulatory requirements under either the Payment Services Act or securities trading legislation (if it involves the offering of financial instruments, such as stock in companies).

Blockchain
There are also no specific regulations applicable to digital currency or blockchain payments, unless they could be qualified as issuing e-money under harmonised EU legislation, providing payment services and/or organising a payment scheme.

Consumer Lending
As discussed above, generally, consumer lending is still largely a non-regulated activity. However, this is likely to change in the foreseeable future.

2.12 Foreign FinTech Companies

General Rules
As a rule, European Economic Area (EEA) companies benefit from freedom to provide services (ie, to act on a cross-border basis) and freedom of establishment (ie, to act through a local branch office).

EU Passporting
EEA regulated entities (such as banks, investment firms and payment institutions) may exercise those freedoms upon completion of a standard "EU passporting" procedure. In principle, a foreign regulated entity licensed in another EU/EEA Member State may offer licensed services in Poland without a local permit from KNF within the scope of its "home" licence. Such activities may be conducted in the territory of Poland through a local branch ("an organisational unit without legal personality separated within the organisational structure of an investment firm") or on a cross-border basis, without establishing a branch. In both cases, the regulated entity notifies its home member state of the intention to commence such operation. The notification is subsequently passed to KNF.

Non-EEA Outsourcing
In co-operation between a Polish regulated entity and a non-EEA FinTech service provider, if such co-operation is qualified as regulated outsourcing, particular sector provisions (eg, banking ones) could require prior express consent from KNF for entering into the agreement. The authorisation proceeding is document-heavy and usually lengthy. Also, to some extent, the proceedings involve discretionary risk assessment by KNF based on the location of the insourcer, among other matters. As a rule, KNF is very cautious in respect of certain locations (such as India or China).

Non-EEA Entities
In principle, foreign entities with their seats outside of the EEA are not entitled to provide cross-border services on a regular basis. Generally, the more the centre of gravity of the particular cross-border relationship shifts toward Poland, the more likely the activity will qualify as being pursued on a regular basis, and it could be subject to a challenge under the local regulations, particularly the Banking Law or ATFI. This is assessed on a case-by-case basis and there is no clear guidance in this area (whether in legislation, case-law or regulatory practice) that would allow the dividing line to be drawn with precision. The distinction between "regular basis" and "temporary and occasional nature" (as discussed above) is based on the intensity of the operation rather than the type of activities (eg, referrals v sale of specified products). It means that non-EU entities cannot pursue regular operation in the territory of the EU without setting up a permanent establishment.

If the service is directly provided to the clients by the non-EEA entity on a cross-border basis, it may be disputable whether the non-EEA entity is actively acting vis-à-vis Polish clients or whether such activity falls within "passive" freedom to provide services under applicable EU law principles. Once again, each setup should be assessed individually.

2.13 Regulatory Enforcement Actions Against FinTech Companies

Protection of Forex Clients
For a number of years, KNF has been making efforts to strengthen the protection of consumers trading on Forex markets, especially through trading platforms offered by EU investment firms acting on a cross-border basis. Apart from entering several business introducers and other local and foreign entities involved in the operation of Forex platforms into its public warnings list, KNF supports legislative changes requiring more comprehensive information for consumers about risks connected with that type of investment.

TPP
In the past, KNF has issued warnings against the use of certain TPP services, particularly account information aggregators and payment initiation services. Regulatory action in

such cases is rarely undertaken directly against the FinTech company. Instead, KNF exercises pressure on regulated institutions (banks) to stop facilitating a given service.

Cryptocurrencies
KNF has issued several warnings regarding cryptocurrencies (most recently in mid-2017), emphasising risks related to their volatility and their use in potentially illicit activities.

2.14 "Shadow Banking"

Anti-Usury Legislation
The CCA provides very restrictive provisions on caps for non-interest costs of credit applicable to all kind of lenders, including non-bank online lenders. The Ministry of Justice announced in 2016 that they are taking steps to prepare legislative changes intended to lower that cap and introduce severe criminal sanctions for its breach. If adopted, such changes would materially affect the operations of online lenders.

Public Warnings List
KNF maintains a public warnings list where it communicates information to the public about filing a notification with the prosecutor regarding suspicion of committing a crime of pursuing regulated activity without a licence. Deletion from the list requires a final decision from the prosecutor and/or the court handling the case, which could take up to several years. The current KNF practice in that respect is very strict; the number of entities currently entered into the list is considerable, and includes various Forex market entities.

Theoretically, being entered into the public warning list does not trigger any particular public or civil law consequences; it is much more a reputational issue. However, in practice, entities entered into the list suffer from various sanctions – eg, regulated entities terminate co-operation with prescribed contractors. Consequently, non-regulated entities acting in the FinTech field should be very cautious about entering into any regulatory "grey area" to avoid being entered into the list.

3. Form of Legal Entity

3.1 Potential Forms of Charter

Local regulated service providers, such as banks, investment firms and insurance companies, are legally required to be established and operate in the form of joint-stock companies (*spółka akcyjna*), being the most complex form of commercial company under Polish law.

Entities from other EEA states operating in other legal forms (eg, limited companies) are free to provide banking, investment or insurance services upon completion of the EEA passporting requirements, as discussed above. If the non-Polish entity intends to act in the form of a branch office, such branch must be separately registered in a Polish commercial register but qualified as an organisational unit of the foreign entity without any separate legal personality.

Under the PSA, there are no specific requirements regarding the legal form in which a payment institution operates. The law does require, however, that the payment institution has separate legal personality, which in fact requires the establishment of a limited liability company (*spółka z ograniczoną odpowiedzialnością*) or a joint-stock company.

Operation in one of those legal forms is expressly required in the case of lending institutions, and also those operating solely through the web.

There are no specific legal requirements regarding the legal form in which other FinTech entities operate.

3.2 Key Differences in Form

The most commonly used form of non-regulated FinTech company is a limited liability company (*spółka z ograniczoną odpowiedzialnością*). It is relatively simple to establish, with a low minimal share capital (PLN5,000 – approx. USD1,350), and offers relative flexibility in shaping its corporate governance.

However, if the entrepreneur plans an IPO in the near future and is not willing to go through a transformation procedure, the FinTech company may be established as a Polish joint stock company (*spółka akcyjna*). However, this type of a corporation is less flexible than a limited liability company and requires a larger investment (the minimal statutory capital is PLN100,000 – approx. USD27,000). On the other hand, shares in joint stock companies constitute transferable securities within the meaning of MiFID.

Under the Polish Commercial Companies Code, both a limited liability company and a joint stock company may be established for any legitimate purpose by one or more persons (some limitations pertain to establishing a limited liability company solely by another one-shareholder limited liability company, in which case a second shareholder has to be involved, at least during the foundation stage).

The establishment procedure encompasses, inter alia, the following:

- executing the Articles of Association/Statutes;
- subscribing for and making cash or in-kind contributions to cover the shares;
- appointing the Subsidiary's governing bodies (ie, the management board members and the supervisory board members; the supervisory board is mandatory in a joint stock company only);

- submitting the registration application to the pertinent registration court; and
- registering the company in the commercial registry.

A supervisory board is a mandatory body in a joint stock company and in large limited liability companies (ie, if there are more than 25 shareholders, and the share capital exceeds PLN500,000). In a "standard" size limited liability company, the supervisory board is not required but may be established.

3.3 Recent Legal Changes

Under Polish law, it is also possible to establish a limited liability company via the Internet (a so-called "24h company"). This should be less time-consuming than the standard establishment described above. However, it is still necessary to visit a public notary in order to modify the company's Articles of Association.

Legislative work is underway to introduce a new type of simplified corporation that would be suitable for technological start-ups and venture capital investors.

4. Legal Infrastructure (Non-regulatory)

4.1 Desirable Changes to Facilitate Specified Activities

"Simple" Joint Stock Company

As part of the Paperless Cashless Poland project, the working groups are considering introducing a so-called "simple" joint stock company that could be established through the Internet (as in the case of a "24h company", discussed above), with minimum share capital (even PLN1) and flexible corporate governance rules.

The "simple" joint companies are intended for start-ups, including those in the FinTech area, but legislative work is, at a very preliminary stage.

Documentary Form

In order to simplify e-commerce and limit practical problems connected with the requirement for the written form of particular agreements (a handwritten signature is required), the Polish civil code has been amended by introducing a so-called "documentary form". The intention was to introduce a flexible form of contracting to be commonly used in e-commerce and any other kind of electronic communication. Wwithin the meaning of those new provisions, the "document" refers to any carrier of information, such as SMS or e-mail.

However, the new provisions ended up being very ambiguous and their practical impact on the market practice has been marginal.

4.2 Access to Real-Time Gross Settlement Systems

Access to real time gross settlement systems (or similar infrastructure) is limited to regulated entities, such as banks, investment firms and payment institutions. Non-regulated entities may access such systems only indirectly, ie, through regulated entities.

However, particular FinTech service providers try to establish independent settlement systems, eg, dedicated to settlements for purchases in a given chain of stores, but the range of such dedicated systems is, by definition, limited.

4.3 Special Insolvency Regimes

There is no special insolvency regime dedicated to non-regulated FinTech companies – they are subject to the general insolvency/reorganisation regimes under Polish law.

4.4 Electronic Signatures

Qualified Electronic Signature

The Polish civil code provides special provisions on treating electronic signatures as equivalent to "wet" signatures. However, this rule applies only to qualified and certified electronic signatures. In practice, the solution is not commonly used due to the relatively high costs of the necessary devices and subscriptions.

Banking E-signatures

The Banking Law provides separate provisions on electronic communication between banks and their customers. Pursuant to these provisions, parties may agree that any declarations related to banking operations between them may be made in electronic form, which is equal to a "wet" signature. The bank is legally obliged to store electronic declaration exchanges with customers properly.

Durable Medium

A number of provisions implementing EU legislation (including on payment services and consumer credits) require that communication between the service provider and its customer or potential customer is provided on a durable medium, as defined under respective legislation.

However, there are certain situations where it is hard to clearly qualify the particular means of communication as a durable medium or not. Currently, a dispute is pending between UOKiK and several Polish banks as to whether e-banking platforms can be qualified as a durable medium, eg, for the purpose of communication related to changes in agreements. UOKiK questions such qualification, arguing that the service provider may interrupt with the wording of communication already provided to the customer. The dispute could have a material influence on FinTech operations in the future.

4.5 Standards for Proving Identity in Electronic Transactions

Currently, there is no common standard for proving identity in electronic transactions. The only such standard applies to communications with public authorities that accept a public identity key (ePuap).

In practice, financial service providers use authorisation transfers from accounts opened with established regulated entities (banks), proving identity of the customer acting online. Such authentication is usually acknowledged by courts, eg, in disputes related to online short-term loans.

At the same time, Polish banks and FinTech companies are pursuing work on new authentication tools based on new technologies, such as behavioural or biometric solutions.

5. Data Privacy and Cybersecurity

5.1 Data Privacy and Cybersecurity Regulatory Regimes

The basic rules on the processing of personal data are currently set forth in the 1997 Personal Data Protection Act ("PDPA"), which is harmonised with EU personal data protection legislation. This regime will be significantly affected by the entry into force of the General Data Protection Regulation ("GDPR") (EU Regulation 2016/679), in May 2018. New legislation on personal data protection will have to be introduced locally to implement certain provisions of the GDPR. Works are pending on the new legislation, but they are at a very early stage.

Poland does not have a comprehensive regulation on cybersecurity, but certain statutes address this issue; for instance, an extraordinary threat to the state, the security of the people or the public order arising from a cyber-attackmay justify the imposition of a state of emergency in part or in the entire territory of Poland. Moreover, the Criminal Code identifies a class of "cybercrimes", ie, offences against the security of information, such as illegal access to a system (hacking/cracking), violation of communication secrecy (sniffing), violation of data integrity (viruses, malware, trojans, etc), violation of system integrity (DDoS attacks, Ping flood), etc.

Published draft policy documents propose the protection of significant sectors in cyberspace, eg, banking services. A Government Centre for Security (NC Cyber) has been established under the authority of Ministry of Digital Affairs to play the leading role in Polish cyber-security, eg by issuing guidelines and recommendations, and auditing various companies and public bodies where elements of critical infrastructure are located. NC Cyber is an early warning and quick reaction centre that co-ordinates activities and serves as an information exchange platform in the case of potential attacks. It also monitors network-related threats, and manages the exchange of related information. Several banks and companies from the energy sector have declared that they are willing to co-operate with NC Cyber, and have a representative at the NC Cyber office. These representatives have access to the most recent solutions and hardware, as well as data on cyber-attacks all over the world.

In regulated financial sectors, data privacy and cybersecurity are a focal point of interest for KNF, which requires regulated entities to have adequate solutions. Protection of personal data is also a critical point of review in most outsourcing arrangements.

5.2 Recent and Significant Data Privacy Breaches

Cybersecurity is also increasingly important to the financial sector, but there have been no reported significant data privacy breaches involving FinTech companies. Paradoxically, the most significant recent breach of cybersecurity involved a so-called "watering hole attack" exploiting the infrastructure and website of KNF itself. The infected KNF website used malfunctioning Flash and Silverlight plug-ins that allowed the attackers to inject and remotely execute certain pieces of code and capture numerous batches of account-related data from banks using said website. The attackers used unique malware, but the attack itself resembled one of the recent attacks against Mexican banks. Investigation by Polish authorities is currently underway, with multiple possible suspects including hacker groups from North Korea, but no specific information is available to date. KNF updated its systems and conducted an internal investigation. Pursuant to the publicly available information, no financial funds were lost as a consequence of the security breach in question, but the leaked data might be used by hackers in future attacks.

There have also been a number of smaller incidents, not necessarily associated with deliberate attacks on the IT infrastructure but mostly related to inadequate security measures applied by banks (eg, it was possible to view the personal and account data of other clients merely by altering the client ID in an internet browser – no encryption or randomisation were used). In 2015, one of the banks had its data stolen by a group of hackers. After a series of attempted blackmails, some members of the group were identified and arrested by the enforcement authorities. Related criminal proceedings are currently underway.

5.3 Companies Utilising Public Key Infrastructures or Other Encryption Systems

The basic statute regulating the rules governing IT infrastructure security is a 2004 Decree issued by the Minister for Internal Affairs and Administration on personal data processing documentation and technical and organisational conditions that should be fulfilled by devices and computer systems used for personal data processing. The Decree was

issued on the basis of the PDPA and particularly specifies length of passwords for a user's account, frequency of password changes, main requirements for authorisation methods and storing backup copies. Security requirements specified in the Decree seem to be insufficient in the light of current cybersecurity threats. The Decree will cease to be binding after the GDPR enter into force.

Use of third-party IT infrastructure by FinTech companies is subject to general outsourcing regulations applicable to FinTech companies acting as service providers to regulated entities. A number of special rules apply when such IT services are classified as regulated outsourcing, such as providing a right for the regulator to audit the service provider or the right to terminate the outsourcing contract if requested by the regulator.

Key guidelines on cybersecurity are also included in KNF's 2013 Recommendation D regarding management of IT and information environment security fields ("Recommendation D"). Recommendation D regulates, among other matters, data management (including data quality management), rules governing co-operation between business and technology and security fields, management information systems for IT and IT security, cloud computing, implementation of new technologies and modification of existing IT solutions, co-operation with external service providers, and IT security risk management. Recommendation D applies to banks, but similar guidelines were also issued for investment firms and insurance companies.

5.4 Biometric Data

The use of biometric data for client identification remains quite limited in Poland, with no specific regulation of use and processing of biometric data as such by FinTech companies. This kind of data is treated as personal data, subject to a heightened protection regime under the PDPA. Additionally, if such data is used in banking to assist the performance of banking activities (eg, fingerprint identification of the client using an ATM), it falls within the scope of information protected under bank secrecy. Some identification methods may relate to processing of health data, eg those involving palm veins, hand geometry or iris recognition. Under the PDPA, health data is considered as "sensitive data". Sensitive data may be collected and processed only in cases specified in the provisions of law. There are currently no provisions that would allow FinTech companies to process such data for security reasons, so the use of such data would require the client's written consent. The Polish Bank Association (*Związek Banków Polskich*) is constantly monitoring the development of biometrics in banking practice and might propose more detailed regulation in the future.

6. Intellectual Property

6.1 Intellectual Property Protection Regime

The framework for IP protection in Poland is set out in the 1994 Copyrights Act and the 2000 Industrial Property Law Act ("IPLA").

Polish copyright law protects any individual human creativity recognised as a "work", established in any form, irrespective of its value, purpose or form of expression. An author's rights to use and dispose of the work ("author's economic rights") are transferrable. Non-economic rights such as the right to sign the work with the author's name ("author's moral rights") are not transferrable.

Industrial property can be protected by the following instruments:

- patents granted in respect of inventions;
- protection rights for utility models;
- registration right for industrial designs;
- protection right for trade marks; and
- registration right for geographical indications.

A company's know-how can also be protected; for instance, the provisions on patent licence contracts apply *mutatis mutandis* to contracts for the exploitation of an invention for which protection has not been applied but which is the company's know-how. Copyright law does not protect ideas and know-how as such, but an idea or know-how can be protected, eg, if it is recognised as an invention under the IPLA or if it constitutes a company secret (trade secret).

Databases may also be protected under general copyright law or the 2001 Database Protection Act ("DPA"). A database is protected by the DPA if its compilation, verification or presentation of content required investment described as substantial in regard to its quality or quantity. A database is protected by the Copyrights Act if it manifests individual human creativity.

6.2 Trade Secret Regime

In Poland, a "trade secret" is treated as commercial confidential information (company information of commercial value, not revealed to the public) and is part of the so-called "company secret" – technical, technological or organisational information about the specific activity of a company. Company secrets (including trade secrets) are protected by the 1993 Act on Combating Unfair Competition, as well as labour law regulations. Specific regulations on company secret protection are implemented in the banking sector, the insurance sector, for investment funds, etc. For instance, a "banking secret" encompasses all information concerning banking operations that is obtained during negotiations, or the conclusion and performance of an agreement under which

the bank performs such operations, including the personal data of customers or potential customers. In principle, the obligation to maintain a banking secret lies with the bank, its employees and persons involved in the performance of banking operations. Pursuant to insurance law, an insurance company and its employees or persons and entities through which it performs insurance-related activities, including insurance agents and brokers, are required to maintain secrets concerning particular insurance contracts. According to jurisprudence, an insurance secret encompasses data on particular insurance contracts.

6.3 Copyrights, Patents, Trade Marks

In principle, FinTech technology (ie, software) is copyrightable, and trademarks related to FinTech technology are trademarkable. The protection of software under copyright law mainly covers the source code, but it does not protect the functionality of a given software, or methods applied in it. Software is not subject to patent protection under Polish law.

6.4 Protection of Intellectual Property or Trade Secrets

Crucial issues related to the problems regarding the protection of intellectual property rights and trade secrets belonging to FinTech companies include the confidentiality of know-how (and its protection from disclosure to third parties), and the acquisition of IP rights to the work products of employees and contractors.

The first issue is readily dealt with by appropriate non-disclosure agreements, as well as managing access to information in-house.

As regards the creation of works, inventions, etc, inside the company, eg by employees, and their acquisition by the company, it is necessary to make sure that relevant employment agreements specify the scope of employee duties, and that the creation of works or inventions is within said scope. Furthermore, employment agreements with employees who participate in work creation for the employer should include appropriate clauses providing that all intellectual property rights will belong to or will be acquired by that FinTech company (eg, pursuant to the Copyrights Act and the IPLA, the employer acquires full rights to software and inventions created by the employee by virtue of law). Without such clauses, employees may seek to question the transfer of IP rights to the employer, or may demand additional compensation for using the software that they created. In practice, this is a frequent practical problem as FinTech companies (and specifically start-ups) often do not have the necessary documentation in place.

6.5 Joint Development of Intellectual Property

In the joint development of intellectual property rights, all co-developers have certain rights specified in statutory provisions of law. As a rule, particular statutes – such as the Copyrights Act or the IPLA – provide for specific regulation of the co-ownership of works, inventions, etc. For works protected under the Copyrights Act, performance of rights for the entire work requires the consent of all co-owners, while each individual owner is entitled to pursue claims arising from copyright infringement and claim compensation in accordance with their share in the right. Under the IPLA, the co-developers of an invention hold a joint right to apply for patent protection. A co-developer is able to pursue claims arising from patent infringement, without the consent of other co-developers. The co-developers might adopt different regulation of the use of their jointly held property right in an individual agreement, which might also regulate the division of profits among co-developers.

The Copyrights Act provides the possibility to develop a so-called related work, eg modification of an earlier work developed by another author. The author of the derivative work holds copyright for that derivative work (the so-called related rights), but is only entitled to use it with the consent of the author of the original work. This issue should also be regulated in the employment agreement if the work is created by an employee.

6.6 Intellectual Property Litigation

At this moment, intellectual property is not a significant source of litigation for FinTech companies in Poland.

6.7 Open Source Code

Source code is treated as a work within the meaning of the Copyrights Act, and use of software requires at least a non-exclusive licence. The Copyrights Act does not include any regulation regarding the use of open source code. Consequently, the current practice is that the scope of permissible use of open source software and its possible development/modification should be compliant with published licence terms for the relevant open source software. Some licences for open source software provide that the use of open source code in development of other software, or by combining it with other software, causes that other software to adopt the provisions of the relevant open source licence.

7. Tax Matters

7.1 Special Tax Issues, Benefits or Detriments

FinTech companies are subject to the general rules of taxation under Polish law.

The provision of particular financial services could be subject to VAT exemptions, as could financial intermediation.

Banks, insurance companies and lending institutions are subject to a special banking tax, introduced in 2016.

Currently, there is no special treatment of startups, save for temporary benefits under the social security regime. While a number of incentives are under consideration, no firm proposal is yet available.

A number of tax interpretations exist in respect of bitcoin. The prevailing position under those interpretations is that cryptocurrencies should be treated as economic rights, which implies an obligation to report income only at the time of their exchange to "traditional" currency, either national or foreign.

Soltysinski Kawecki & Szlezak
ul. Jasna 26
Warsaw
Masovian
Poland
00-054

Tel: +48 22 608 7000
Fax: +48 22 608 7070
Email: office@skslegal.pl
Web: http://www.skslegal.pl/

8. Issues Specific to the Specified Activities

8.1 Additional Legal Issues

Lending platforms are subject to the same restrictions as bank lenders in terms of limits on interest (Poland has a maximum interest regulation that caps interest at 4 times the National Bank of Poland's lombard rate) and non-interest costs (capped at a maximum of 100% of the loan amount, depending on the duration of the loan).

Virtual currencies are not treated as money (the only "official" qualifications – ie, tax rulings – suggest a qualification as property rights rather than money). As a result, holding a virtual currency is not considered as either deposit taking or money transmission.