Paweł Pelc*

The COVID-19 pandemic and the functioning of financial institutions in Poland. Cybersecurity issues

Abstract

The COVID-19 pandemic has significantly influenced the functioning and organisation of financial institutions in Poland and the cybersecurity mechanisms associated with it, due to the change in the model of functioning of these institutions. Changes to the way institutions function have been introduced under the influence of evolving restrictions and regulations, often in a manner which went beyond previously planned scenarios of action. The experience gained in this way should be included in the business continuity plans and procedures of financial institutions. It is also worth considering what changes should be permanently implemented by financial institutions, and what adaptations in the field of cybersecurity will be required. These adjustments should take place in interaction with the Polish Financial Supervision Authority, to maintain an appropriate level of security and quality of services rendered.

Key words: cybersecurity, financial institutions, COVID-19, financial-market supervision

* Paweł Pelc, The War Studies University in Warsaw, Security Research Centre, Centre for Cybersecurity Studies, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

The COVID-19 pandemic has significantly influenced the functioning of financial institutions in Poland. Regulations related to the state of the epidemic emergency, and then to the state of the epidemic itself, made it impossible to operate as before. The restrictions introduced precluded or hindered the use of services in fixed-base institutions, and also made it impossible to provide, or hindered the providing of, work on the premises of these institutions[1]. Both customers and the staff of the bodies of financial institutions, and their supervision[2], had to switch to the use of remote devices. Restrictions also applied to infrastructure institutions and the legal environment, such as administrative bodies[3] and courts. In addition, the legislators made frequent changes to the legal regulations[4], often of an irregular nature, by introducing

1 M. Dekrewicz, W. Boczoń, M. Kisiel, *7 zmian w bankach, które przyszły z koronawirusem*, „Złoty Bankier" 2020, https://www.bankier.pl/wiadomosc/7-zmian-w-bankach-ktore-przyszly-z-koronawirusem-Zloty-Bankier-2020-7908308.html.

2 *Zmiany w organizacji pracy w Urzędzie Komisji Nadzoru Finansowego*, https://www.knf.gov.pl/komunikacja/komunikaty?articleId=69285&p_id=18.

3 W. Ziomek, *KNF wznawia zamrożone postępowania*, https://www.money.pl/gospodarka/knf-wznawia-zamrozone-postepowania-6512217261491841a.html.

4 In particular: Ustawa z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19; rozporządzenie Ministra Finansów z dnia 22 maja 2020 r. w sprawie określenia innego terminu podjęcia przez walne zgromadzenie spółki uchwały w sprawie polityki wynagrodzeń członków zarządu i rady nadzorczej; ustawa z dnia 14 maja 2020 r. o zmianie niektórych ustaw w zakresie działań osłonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2; rozporządzenie Ministra Finansów z dnia 16 kwietnia 2020 r. zmieniające rozporządzenie w sprawie zasad tworzenia rezerw na ryzyko związane z działalnością banków; ustawa z dnia 16 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-CoV-2; rozporządzenie Ministra Finansów z dnia 7 kwietnia 2020 r. w sprawie określenia innych terminów wykonania niektórych obowiązków sprawozdawczych i informacyjnych; ustawa z dnia 31 marca 2020 r. o zmianie ustawy o systemie instytucji rozwoju; ustawa z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw; ustawa z dnia 31 marca 2020 r. o zmianie niektórych ustaw w zakresie systemu ochrony zdrowia związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19; rozporządzenie Ministra Finansów z dnia 31 marca 2020 r. w sprawie przedłużenia terminów do sporządzenia i przesłania niektórych informacji podatkowych; rozporządzenie Ministra Finansów z dnia 31 marca 2020 r. w sprawie określenia innych terminów wypełniania obowiązków w zakresie ewidencji oraz w zakresie sporządzenia, zatwierdzenia, udostępnienia i przekazania do właściwego rejestru, jednostki lub organu sprawozdań lub informacji; rozporządzenie Ministra Finansów z dnia 18 marca 2020 r. uchylające rozporządzenie w sprawie bufora ryzyka systemowego; rozporządzenie Ministra Finansów z dnia 16 marca 2020 r. zmieniające rozporządzenie w sprawie udzielania przez Bank Gospodarstwa Krajowego pomocy *de minimis* w formie gwarancji spłaty kredytów.

further anti-crisis shields. Restrictions on the functioning of the economy related to the pandemic also affected the ability of bank customers to meet their liabilities, and the special regulations introduced in this regard involved both payment holidays[5] and changes to the principles of creating provisions and write-downs by credit institutions[6].

Out of necessity, a substantial proportion of activities moved to cyberspace[7]. This involved both customer contact[8] and supervision, as well as channels for acquiring new customers[9]. In this situation, financial institutions are particularly vulnerable to cyber attacks[10]. According to WMvare data, from the beginning of February to the end of April 2020, the number of cyber attacks against financial institutions increased by 238%[11]. Santander Consumer Bank conducted a survey which showed that, because of the COVID-19 threat, as

5 *BIK: odroczenie spłaty rat bez negatywnych skutków*, https://www.gb.pl/bik-odroczenie-splaty-rat-bez-negatywnych-skutkow-pnews-2951.html; *Wakacje kredytowe w Banku Pocztowym*, https://www.gb.pl/wakacje-kredytowe-w-banku-pocztowym-pnews-2940.html.

6 Rozporządzenie Ministra Finansów z dnia 16 kwietnia 2020 r. zmieniające rozporządzenie w sprawie zasad tworzenia rezerw na ryzyko związane z działalnością banków, Dz.U. 2020, poz. 687. Cf. Stanowisko Urzędu Komisji Nadzoru Finansowego w ramach Pakietu Impulsów Nadzorczych ws. finansowania przez banki klientów korporacyjnych w obliczu pandemii koronawirusa, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_finansowania_przez_banki_klientow_korporacyjnych_69405.pdf.

7 *Jak będzie wyglądać nowa rzeczywistość w biurach?*, https://www.gb.pl/jak-bedzie-wygladac-nowa-rzeczywistosc-w-biurach-pnews-3119.html.

8 *PZU pomaga klientom w czasie epidemii*, https://www.gb.pl/pzu-pomaga-klientom-w-czasie-epidemii-pnews-2997.html; *Zdalne podpisywanie umów dla klientów firmowych Banku Pekao*, https://www.gb.pl/zdalne-podpisywanie-umow-dla-klientow-firmowych-banku-pekao-pnews-2978.html.

9 *W ING otwarcie konta za pomocą wideoweryfikacji*, https://www.gb.pl/w-ing-otwarcie-konta-za-pomoca-wideoweryfikacji-pnews-3005.html.

10 *Uwaga na oszukańcze ogłoszenia związane z epidemią koronawirusa*, https://zbp.pl/Aktualnosci/Wydarzenia/Uwaga-na-oszukancze-ogloszenia-zwiazane-z-epidemia-koronawirusa; *Praca zdalna: najważniejsze zasady cyberbezpieczeństwa dla pracujących z domu z powodu koronawirusa*, https://alebank.pl/praca-zdalna-najwazniejsze-zasady-cyberbezpieczenstwa-dla-pracujacych-z-domu-z-powodu-koronawirusa/; M. Marszycki. *Wykorzystując pandemię koronawirusa, hakerzy próbują wyłudzić dane od posiadaczy kont w PKO BP*, https://itwiz.pl/wykorzystujac-pandemie-koronawirusa-hakerzy-probuja-wyludzic-dane-od-posiadaczy-kont-pko-bp/; *„Rz": rośnie liczba cyberataków w związku z pandemią koronawirusa*, https://www.polskieradio24.pl/5/1222/Artykul/2491227,Rz-rosnie-liczba-cyberatakow-w-zwiazku-z-pandemia-koronawirusa; *Podczas pandemii wzrosła liczba cyberataków. Hakerzy celują w infrastrukturę krytyczną i luki w zabezpieczeniach podczas pracy zdalnej*, https://innowacje.newseria.pl/news/podczas-pandemii-wzrosla,p836654848.

11 M. Klimkowski, *Hakerzy pokochali pandemię. Pozwala im na dużo więcej ataków na banki*, https://biznes.wprost.pl/technologie/10329480/hakerzy-pokochali-pandemie-pozwala-im-na-duzo-wiecej-atakow-na-banki.html.

many as 38% of respondents started paying more often with a card, of which almost 70% was for purchases in traditional stores[12].

It should be stressed that part of the banking infrastructure can be considered to be associated with the provision of critical services, within the meaning of the regulations on the national cybersecurity system[13]. Since 1 April 2017, FinCERT.pl – the Bank Cybersecurity Centre of the Polish Bank Association – has been conducting permanent operational activities related to detecting, analysing, preventing, and combating cybercrimes committed against banks and their customers[14]. The activities of FinCERT.pl might be an important factor limiting the temptation which might arise, for fear of losing customer confidence, to conceal cyber security incidents[15].

Notwithstanding the above, confidence is particularly important in the functioning of financial institutions, and an element of confidence-building is, *inter alia*, the guaranteeing of the security of customers' funds and data, including in situations in which the majority of operations have moved to cyberspace due to the COVID-19 threat. This applies to the security of the systems of financial institutions in a situation where some of their employees work remotely, and where their customers use remote-access channels. COVID-19 has become a particular "stress test", due to a significant extension of the range of services provided remotely, but also a significant expansion in the circle of people who have to use cyberspace both to work for financial institutions and to use their services. Consequently, people with less experience and skills in this field who had previously worked directly or used services in financial institutions were also obliged to use digital mechanisms. As a result, the key risk – associated with the human factor – significantly increased in this situation. It seems that financial institutions in Poland have managed to cope with the threats they have faced, and there has been no loss of confidence in them, or as a result of the outbreak of related scandals, and they have succeeded in adapting to the new reality without losing customer confidence, and without significant cybersecurity incidents. Existing tools such as corporate VPNs have facilitated

12 *Epidemia zmienia nawyki płatnicze Polaków*, https://www.gb.pl/epidemia-zmienia-nawyki-platnicze-polakow-pnews-3122.html.

13 For further details, see P. Pelc, *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, nr 2, s. 160–161.

14 *Cyberbezpieczeństwo*, https://zbp.pl/dla-bankow/Cyberbezpieczenstwo.

15 R. Pitera, *Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej*, „Przegląd Nauk o Obronności" 2017, nr 1, s. 187–188.

the movement towards remote working. Also, innovative projects related to the remote identification of customers[16], implemented even before the introduction of restrictions related to COVID-19, facilitated the easier acquisition of customers, including during the period of restrictions on direct contact for sanitary reasons. The banks have also taken steps to educate their customers about cybersecurity[17].

The changes related to COVID-19 were undertaken on an *ad hoc* basis, due to the dynamically changing situation and regulatory changes pertaining to legal regulations and supervisory recommendations by the Polish Financial Supervision Authority (KNF) and the European supervisory authorities for individual financial market segments[18]. A significant part of these adaptations

16 *Biometria w Banku Pekao*, https://www.gb.pl/biometria-w-banku-pekao-pnews-2784.html.

17 *Uwaga na oszustów wykorzystujących epidemię koronawirusa*, https://www.bnpparibas.pl/repozytorium/komunikaty/Koronawirus-zagrozeniem-nie-tylko-dla-Twojego-zdrowia; *Związek Banków Polskich. Raport ZBP Cyberbezpieczny portfel. Edycja III, styczeń 2020 r.*, https://zbp.pl/getmedia/156b5c44-bfcc-46cb-a5d1-bd0d141e9ed0/ZBP_CyberbezpiecznyPortfel2020; *Przegląd działań i akcji edukacyjnych banków w obszarze cyberbezpieczeństwa*, https://bezpieczny.blog/przeglad-dzialan-i-akcji-edukacyjnych/.

18 *Komunikaty Instytucji Europejskich*, https://www.knf.gov.pl/dla_rynku/Koronawirus_informacje_dla_podmiotow_nadzorowanych.

ESMA: *Stanowisko ESMA ws. wpływu epidemii COVID-19 na półroczne raporty finansowe*; *Stanowisko ESMA ws. ochrony klienta detalicznego korzystającego z usług uregulowanych w MIFID II Q&A dot. wytycznych ESMA ws. APMs*, uaktualnienie w związku z COVID-19; *Komunikat UKNF w sprawie zmiany terminów publikacji sprawozdań finansowych funduszy inwestycyjnych w związku ze stanowiskiem ESMA*; *Stanowisko ESMA dot. publikacji obliczeń dla instrumentów nieudziałowych innych niż obligacje*; *Stanowisko ESMA ws. audytu zewnętrznego wymaganego przez BMR*; *Komunikat UKNF ws. raportowania SFT*; *Komunikat UKNF dotyczący Stanowiska ESMA – obowiązki sprawozdawcze w zakresie wykonywania zleceń (best execution)*; *Komunikat UKNF dot. sprawozdawczości emitentów w związku ze stanowiskiem ESMA*; *Stanowisko ESMA ws. wpływu epidemii COVID-19 na kalkulację oczekiwanych strat kredytowych wg MSSF 9*; *Stanowisko ESMA w sprawie wdrożenia przez podmioty systematycznie internalizujące transakcje wymogów w zakresie minimalnego kroku kwotowań*; *Stanowisko ESMA w sprawie nagrywania rozmów z klientami*; *ESMA zaleca uczestnikom rynków finansowych podjęcie działań w zakresie skutków koronawirusa COVID-19*.

EIOPA: *Oświadczenie EIOPA w sprawie zasad wypłaty dywidend i zmiennych części wynagrodzeń w kontekście COVID-19*; *Oświadczenie EIOPA w sprawie działań podejmowanych przez ubezpieczycieli i pośredników na rzecz złagodzenia wpływu koronawirusa na konsumentów*; *Komunikat dot. sprawozdawczości SII w związku ze stanowiskiem EIOPA*; *Oświadczenie EIOPA w sprawie działań na rzecz ograniczenia wpływu koronawirusa/COVID-19 na sektor ubezpieczeniowy w Unii Europejskiej*.

EBA: *Stanowisko EBA z 22 kwietnia dotyczące dodatkowych działań nadzorczych w obliczu pandemii COVID-19*; *Wytyczne EBA dotyczące ustawowych i pozaustawowych moratoriów na spłaty kredytów, stosowanych w obliczu kryzysu spowodowanego przez COVID-19 – tłumaczenie*; *Stanowisko i wytyczne EBA związane z moratoriami na spłatę kredytów przyznanymi wz. z COVID-19*; *Stanowiska EBA związane z łagodzeniem wpływu COVID-19 na europejski sektor*

had not previously been foreseen in crisis scenarios prepared by individual financial institutions, and often required substantial improvisation on the part of financial institutions and their IT services, as well as security and compliance. A particular challenge was also to provide employees who were directed to work remotely with the appropriate equipment, to enable them to perform such work in a safe manner. Moving a significant proportion of activities to cyberspace could not weaken the protection of professional secrecy (including banking secrecy) and personal data protection.

The attempts by financial institutions to use a public or hybrid cloud were also particularly challenging. As early as just after the outbreak of the pandemic, the Polish Financial Supervision Authority recognised that the measures it was propounding could be excessively restrictive during the pandemic, and it decided to delay the entry into force of its proposed solutions[19].

The lockdown of part of the economy meant that various services normally paid for with a card (such as flights, hotels, other transport and tourism services, etc.) were not provided. Where they had already been paid for with a payment card, and the card acceptor did not reimburse the payment for the service it had been unable to supply, payment card holders could complain about such transactions with their payment card issuers. In practice, it turned out that the regulation on handling complaints did not work in such a situation, as the payment card issuer's deadline for handling complaints expired before the deadline for the card acceptor to respond to it. As a result, in order to avoid the consequences of exceeding the deadline for handling complaints (the tacit acceptance of complaints), payment card issuers rejected complaints until the deadline for the acceptor to respond to the complaint had expired. At the same time, payment card issuers' systems had to enable the increased number of complaints from their customers to be received remotely and processed in a timely manner, and also to generate responses for their customers remotely.

bankowy; *Oświadczenie EUNB w sprawie działań na rzecz ograniczenia wpływu koronawirusa COVID-19 na sektor bankowy w Unii Europejskiej*.

19 *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf; *Zmiany postanowień zawartych w Komunikatu UKNF z 23 stycznia 2020 r. dotyczącym przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*, https://www.knf.gov.pl/knf/pl/komponenty/img/Zmiany_postanowien_zawartych_w_Komunikatu_UKNF_z_23_stycznia_2020.pdf.

After the first period in which changes had to be made quickly, on the one hand, the technical and organisational activities of financial institutions were stabilised. On the other hand, the gradual easing of the restrictions associated with the state of the epidemic allowed a partial return to forms of activity which had existed before the restrictions were introduced. At present, however, it is impossible to predict how long the state of the epidemic emergency will last, or what the further easing of sanitary and epidemiological restrictions will look like, or whether they will be intensified again – throughout the country or locally – in the event of the possible so-called second wave of the pandemic, or significant local pandemic outbreaks. This means that it is not clear when the restrictions on doing business will be completely removed, nor is it clear to what extent changes in consumer and employee behaviour will prove sustainable. Undoubtedly, the COVID-19 pandemic has shown that the business continuity plans of financial institutions must make it possible to ensure the continuity of their operations even if all employees have to switch to remote working. This scenario must be regarded as realistic, given the willingness of central- or local-administration bodies in different countries to even introduce a complete lockdown[20]. This means that it is realistic and feasible to prevent the employees of financial institutions from having physical access to their workplaces, by order of the administrative authorities, for example, in a state of epidemic emergency, or a state of a new epidemic outbreak, without having to introduce constitutional states of emergency, and the existing legal regulations may be used in this way. It is equally feasible to prevent the customers of banking institutions from having access to their facilities, so business continuity plans must provide for the possibility of rendering their services entirely remotely. They should provide not only for remote access to the services rendered by these institutions, but also for the possibility of both parties' entering into new contracts without the need to be physically present in financial institutions. In the case of banks and cooperative savings and credit unions, it is particularly important to ensure that their customers have continuous access to cash, even when it is necessary

20 Cf.: zalecenie ESMA z 11 marca 2020 r.: „Wszyscy uczestnicy rynków finansowych, w tym podmioty obsługujące infrastrukturę rynków, powinni przygotować się za zastosowanie swoich planów awaryjnych, w tym na wdrożenie środków na rzecz utrzymania ciągłości działań, aby zapewnić ciągłość operacyjną zgodnie z obowiązkami określonymi w przepisach prawa" – *ESMA zaleca uczestnikom rynków finansowych podjęcie działań w zakresie skutków koronawirusa COVID-19*, https://www.knf.gov.pl/aktualnosci?articleId=69236&p_id=18; https://www.esma.europa.eu/press-news/esma-news/esma-recommends-action-financial-market-participants-covid-19-impact.

to close all the branches of an institution. This raises not only organisational challenges but also, to a large extent, challenges in terms of the IT structure and security systems, including cybersecurity in particular. Irrespective of the issue of providing services to customers, and teleworking, financial institutions must also be prepared to ensure the full remote operation of their organisations.

Notwithstanding the changes to procedures and business-continuity plans, as well as to the rules governing the bodies of financial institutions which allow them to operate in the event of a lockdown, it is also necessary to build on the experience gained during the first phase of the pandemic, and the related restrictions, in order to use them for further activities, even after the pandemic has ended, and the related restrictions have been fully removed. In particular, it is important for financial institutions to consider the possibility of carrying out remote work on a permanent basis to a significant extent, as well as of limiting the use of traditional facilities for remote access to services. This can be particularly important in the context of low (real negative) interest rates, and economic slowdown, which will adversely affect the revenues of financial institutions. In this situation, savings from remote working and remote access channels can make it easier for financial institutions to adapt to the new conditions. This will involve the permanent implementation of cybersecurity mechanisms, despite possible limitations in operating costs. If the evolution of the financial sector was to have such an effect, it might turn out that cybersecurity issues could become crucial for the survival of financial institutions in the so-called "new normality". In such a situation, educating both employees and customers on cybersecurity, as well as measures to prevent them from becoming dormant and falling into a routine, will be very important. In the case of financial institutions and their relations with customers, too, the weakest link in terms of cybersecurity is usually the human being. It will also be essential to strengthen mechanisms which automatically detect any unusual customer behaviour, and verify whether a breach of cybersecurity has occurred in such a situation.

Another unknown issue is the question of the mechanisms for access to payment accounts between various financial institutions in connection with the implementation of the solutions provided for in the so-called PSD-2 Directive, which, to a large extent, has coincided with the pandemic period. The new solutions might lead to a situation in which the customer of an institution obtains full access to his/her payment account through third parties and the IT tools they provide. As a result, it is possible to consolidate access to payment institutions in the hands of an integrator, who will hold information

on payment accounts with a range of payment service providers. In practice, this can greatly reduce direct interaction between payment institutions and their customers.

In such a scenario, the Polish Financial Supervision Authority should take action to review the modified business continuity plans of financial institutions and the security protocols related to remote working and remote access, and access through third parties. At the same time, the supervisory expectations in this respect must not exceed the real financial capacity of the supervised entities.

Bibliography

Dekrewicz M., Boczoń W., Kisiel M., *7 zmian w bankach, które przyszły z koronawirusem*, „Złoty Bankier" 2020.

Klimkowski M., *Hakerzy pokochali pandemię. Pozwala im na dużo więcej ataków na banki*, https://biznes.wprost.pl/technologie/10329480/hakerzy-pokochali-pandemie-pozwala-im-na-duzo-wiecej-atakow-na-banki.html.

Pelc P., *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, nr 2.

Pitera R., *Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej*, „Przegląd Nauk o Obronności" 2017, nr 1.

Rozporządzenie Ministra Finansów z dnia 16 kwietnia 2020 r. zmieniające rozporządzenie w sprawie zasad tworzenia rezerw na ryzyko związane z działalnością banków, Dz.U. 2020, poz. 687.

Pandemia COVID-19 a funkcjonowanie instytucji finansowych w Polsce. Kwestie cyberbezpieczeństwa

Streszczenie

Pandemia COVID-19 istotnie wpłynęła na sposób funkcjonowania i organizację instytucji finansowych w Polsce oraz na związane z nim mechanizmy cyberbezpieczeństwa w związku ze zmianą modelu funkcjonowania tych instytucji. Zmiany w sposobie funkcjonowania instytucji były wprowadzane pod wpływem zmieniających się ograniczeń i uregulowań, często w sposób wykraczający poza wcześniej przygotowywane scenariusze działania. Zdobyte w ten sposób doświadczenia powinny zostać uwzględnione w planach ciągłości działania instytucji finansowych oraz ich procedurach. Warto też rozważyć, jakie zmiany powinny zostać na stałe wdrożone w instytucjach finansowych i jakich to będzie wymagało dostosowań w zakresie cyberbezpieczeństwa. Dostosowania te powinny odbywać się w interakcji z Komisją Nadzoru Finansowego, by zachować odpowiedni poziom bezpieczeństwa i jakości świadczonych usług.

Słowa kluczowe: cyberbezpieczeństwo, instytucje finansowe, COVID-19, nadzór nad rynkiem finansowym