Komunikat z posiedzenia Rady ds. Systemu Płatniczego w dniu 22 października 2021 r.

W dniu 22 października 2021 r. odbyło się posiedzenie Rady ds. Systemu Płatniczego, organu opiniodawczo-doradczego przy Zarządzie Narodowego Banku Polskiego. Posiedzenie w formie telekonferencji prowadziła Pani Marta Kightley, Przewodnicząca Rady ds. Systemu Płatniczego, Wiceprezes NBP – Pierwszy Zastępca Prezesa NBP.

Rada ds. Systemu Płatniczego zapoznała się z:

- oceną funkcjonowania polskiego systemu płatniczego w I półroczu 2021 r., przygotowaną przez Narodowy Bank Polski, i pozytywnie ją zaopiniowała,
- informacją na temat korzyści i wyzwań związanych z wdrożeniem usług rozliczeniowych KDPW_CCP na rzecz sektora bankowego,
- planami KIR S.A. dotyczącymi uruchomienia rozwiązania dla płatności natychmiastowych w euro (Euro Express Elixir);
- materiałem na temat doświadczeń i wyzwań w walce w transakcjami oszukańczymi w płatnościach detalicznych. Rada przyjęła rekomendacje działań w obszarze prawa, procesów, technologii i edukacji na rzecz ograniczania transakcji oszukańczych w płatnościach detalicznych w Polsce. Rekomendacje Rady zawiera załącznik do komunikatu.

Rada zapoznała się ponadto z następującymi materiałami informacyjnymi, opracowanymi przez Narodowy Bank Polski:

- *Informacją o kartach płatniczych – II kwartał 2021 r.,*
- *Informacją o rozliczeniach i rozrachunkach międzybankowych w II kwartale 2021 r.,*
- *Informacją o transakcjach oszukańczych dokonanych przy użyciu bezgotówkowych instrumentów płatniczych w II kwartale 2021 r.,*
- *Analizą opłat i prowizji związanych z korzystaniem z rachunku płatniczego w Polsce (wg danych na koniec 2020 roku).*

Kolejne posiedzenie Rady ds. Systemu Płatniczego odbędzie się w grudniu 2021 r.

Załącznik:

Rekomendacje Rady ds. Systemu Płatniczego dotyczące działań na rzecz ograniczania transakcji oszukańczych w płatnościach detalicznych w Polsce

I. Rekomendacje w obszarze prawa

1. Rozważenie wprowadzenia rozwiązań prawnych umożliwiających wymianę informacji prawnie chronionych pomiędzy podmiotami z różnych sektorów (bankowego, telekomunikacyjnego, ubezpieczeniowego, niebankowych dostawców usług płatniczych),

2. Rozważenie wprowadzenia rozwiązań prawnych umożliwiających zmianę zasad dostępu przez Policję i Prokuraturę do informacji objętych tajemnicą bankową w szczególnych przypadkach związanych z wykrywaniem i ściganiem przestępczości,

3. Zasygnalizowanie Komisji Europejskiej, w ramach zbliżającego się przeglądu Dyrektywy o usługach płatniczych (PSD2), zapowiedzianego na koniec 2021 r., potrzeby przeprowadzenia analizy zasadności dokonania zmian mających na celu bardziej klarowne uregulowanie kwestii uwierzytelnienia i autoryzacji związanych z transakcją płatniczą i ich skutków prawnych (w tym zakresu odpowiedzialności z tytułu nieautoryzowanych transakcji płatniczych), w szczególności ustalenia dokładnego znaczenia pojęcia „uwierzytelnienia transakcji płatniczej" w rozumieniu art. 72 ust. 1 PSD2, zgodnie z którym dostawca usług płatniczych ma obowiązek udowodnienia, że transakcja była odpowiednio uwierzytelniona (ang. „to prove that the payment transaction was authenticated"), co ma znaczenie w kontekście definicji uwierzytelnienia (art. 4 pkt 29 PSD2), zgodnie z którą uwierzytelnieniu podlega nie transakcja, ale użytkownik (płatnik), albo ważność użycia danego instrumentu płatniczego, jak również bardziej precyzyjne sformułowanie ostatniego zdania art. 72 ust. 2 PSD2, w którym stanowi się, że dostawca usług płatniczych powinien wykazać umyślne działanie płatnika lub jego rażące niedbalstwo (ang „The payment service provider (…) shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user."), w szczególności, czy obowiązkiem dostawcy jest dodatkowo, obok udowodnienia, że transakcja została odpowiednio zarejestrowana (względnie – zależnie od rozumienia tego pojęcia - uwierzytelniona), udowodnić umyślne działanie płatnika, albo jego rażące niedbalstwo,

4. Rozważenie wprowadzenia prawnych ograniczeń możliwości działania grup zajmujących się oszustwami inwestycyjnymi i swobodnego realizowania przez nie operacji związanych z oszukańczym obrotem kryptowalutami lub na rynku forex, w tym wprowadzenia uprawnień dla banków do skutecznego powstrzymywania podejrzanych operacji mogących mieć z tym zjawiskiem związek, w tym możliwości pozyskiwania przez banki na potrzeby analizy antyfraudowej dodatkowych danych, np. danych geolokalizacyjnych czy numerów portów urządzeń z dostępem do Internetu,

5. Rozważenie dokonania w przepisach prawa lub rekomendacjach KNF zmian mających na celu dodatkową ochronę prawną pracowników obszarów zajmujących się bezpieczeństwem z uwagi na fakt, iż jest to praca często angażująca pracownika do współpracy z organami ścigania, niosąca za sobą konieczność składania zeznań i stawiania się na rozprawach sądowych, obciążona silnym stresem związanym z działaniem pod presją czasu, aby zapobiec skutkom kradzieży pieniędzy czy też z konfrontacją na sali rozpraw z oskarżonymi o przestępstwa na

szkodę banków i ich klientów. Taka praca wiąże się z wysokim ryzykiem popełnienia błędu np. pod kątem ryzyka ujawniania tajemnicy zawodowej, bankowej czy złamania zasad RODO.

6. Stworzenie podstawy prawnej (np. w ustawie o Systemie Informacji Finansowej[1]) dla wprowadzenia rozwiązania umożliwiającego kontrolę zgodności numeru rachunku odbiorcy płatności z jego danymi osobowymi (imieniem i nazwiskiem) przed dokonaniem transakcji. Takie rozwiązanie pomogłoby uniknąć bardzo wielu przypadkowych lub wynikających z manipulacji przestępców błędnie skierowanych płatności do nieodpowiedniego właściciela rachunku i zapewniłoby dodatkową ochronę w walce z oszustami.

II. Rekomendacje w obszarze procesów

1. Utworzenie w ramach Rady ds. Systemu Płatniczego Grupy Roboczej ds. Bezpieczeństwa Płatności o charakterze stałym, której zadaniem byłoby szczegółowe monitorowanie różnych aspektów bezpieczeństwa polskiego systemu płatniczego, w tym w szczególności aspektów bezpieczeństwa w płatnościach detalicznych, współpraca pomiędzy najbardziej zainteresowanymi instytucjami i podmiotami oraz wypracowywanie propozycji rozwiązań mających na celu ograniczanie pojawiających się nowych rodzajów oszustw i zagrożeń,

2. Powszechne wykorzystanie funkcji geoblokowania dla płatności kartowych dokonanych poza UE (np. blokowanie płatności z konkretnych obszarów geograficznych dokonywanych z użyciem paska magnetycznego) i danie możliwości odblokowania takich płatności klientowi, który zgłosi taką potrzebę,

3. Umożliwienie samodzielnego ustawiania limitów dla płatności bez obecności karty (CNP) i udostępnianie ograniczonych limitów ilościowych i kwotowych dla płatności CNP klientom, którzy z takich płatności z dużym prawdopodobieństwem nie będą korzystać.

4. Wprowadzenie na rynku polskim odpowiednika brytyjskiej usługi Confirmation of Payee,

5. Identyfikacja rzeczywistych łańcuchów transakcji przestępczych połączona z blokadą środków i wykrywaniem skompromitowanych rachunków oraz danych osobowych i kontaktowych wykorzystywanych do utylizacji środków pochodzących z przestępstwa,

6. Uwzględnienie w systemach wymiany informacji pomiędzy bankami informacji o transakcjach i zautomatyzowanie ich na tyle, by można było sprawnie blokować wypłaty „na słupa" w innych bankach,

7. Rozwijanie współpracy międzybankowej oraz międzysektorowej z organami ścigania w ramach tworzonych przez finCERT.pl - BCC ZBP grup operacyjnych, w szczególności obejmującej

[1] Projekt tej ustawy jest aktualnie w toku procesu legislacyjnego (UC66): Projekt (rcl.gov.pl) Ustawa ta będzie stanowiła podstawę prawną dla utworzenia centralnej bazy rachunków płatniczych. W projektowanych przepisach określono typ informacji o rachunkach, które mają być przekazywane przez podmioty zobligowane do dostarczania informacji o rachunku do SInF (tzw. instytucje zobowiązane). Zakres przekazywanych informacji o rachunku zawiera między innymi: dane identyfikacyjne (w tym imię i nazwisko oraz obywatelstwo) posiadaczy rachunku, pełnomocników do rachunku, beneficjentów rzeczywistych posiadaczy rachunku oraz datę otwarcia i zamknięcia rachunku

wymianę wrażliwych informacji o konkretnych modus operandi w bezpiecznych kanałach elektronicznych,

8. Szersze współdzielenie najlepszych praktyk w zakresie monitorowania i zapobiegania wyłudzeniom, ukierunkowane na szybką komunikację zidentyfikowanych przypadków do innych uczestników rynku usług płatniczych,

9. Zwiększenie nakładów u dostawców usług płatniczych na podniesienie świadomości użytkownika końcowego - klienta, zwiększenie nakładów na system ochrony i obrony przed zaawansowanymi atakami,

10. Rozpowszechnienie innych niż numer karty płatniczej rozwiązań do płatności w Internecie, np. płatność BLIKiem lub tokenizacja, polegająca na zastąpieniu numeru karty płatniczej unikalnym identyfikatorem cyfrowym,

11. Rozważenie zasadności opracowania dla potrzeb rynku polskiego odpowiednika Fraud Classifier wprowadzonego w USA,

12. Rozważenie wzmocnienia koordynacyjnej roli FinCERT.pl – BCC ZBP jako ISAC w kontekście działań środowiska bankowego i reprezentowania przed UKNF oraz w kontaktach z operatorami telekomunikacyjnymi.

13. Rozważenie możliwości zastosowania w BLIK i innych schematach niekartowych mechanizmów chargeback podobnych jak w schematach kartowych,

14. Rozważenie potrzeby zorganizowania scentralizowanego systemu raportowania transakcji oszukańczych dla metod płatności BLIK oraz przelewów bankowych procesowanych przez operatorów płatności, z dostępem raportujących podmiotów do zagregowanych danych (analogicznie jak zorganizowane to zostało przez Visa TC40 lub Mastercard SAFE),

15. Rozważenie możliwości powstania systemu antyfraudowego na poziomie ogólnokrajowym, w którym mógłby być monitorowany pełen obraz przepływów pieniędzy, informacji i powiązań między obiektami, gdyż nie da się tego zaobserwować na szczeblu poszczególnych banków oraz innych instytucji finansowych.

III. Rekomendacje w obszarze technologii

1. Wprowadzenie zaawansowanej technologii do monitorowania płatności dokonywanych polskimi kartami płatniczymi poza granicami Polski,

2. Stosowanie narzędzi pozwalających wykryć zdalny pulpit wykorzystany w urządzeniu, które inicjuje płatność,

3. Wykorzystanie w procesach, w których dochodzi do inicjowania płatności, technologii pozwalającej na identyfikację urządzenia użytego do płatności (największą synergię zagwarantuje wykorzystanie jednego standardu w ramach sektora bankowego i usług płatniczych przez wiele organizacji),

4. Wprowadzenie uwierzytelnienia wieloskładnikowego wykorzystującego biometrię behawioralną opartą na analizie zachowania użytkownika (biometria behawioralna),

5. Wypracowanie nowych rozwiązań technologicznych umożliwiających szybką i zautomatyzowaną wymianę informacji np. o skompromitowanych: rachunkach bankowych, danych osobowych i kontaktowych, adresach IP ze znacznikami czasu i numerach portów, urządzeń i indeksów biometrii behawioralnej przestępców pomiędzy bankami, przedsiębiorcami z innych sektorów oraz organami ścigania i GIIF,

6. Rozważenie możliwości wdrożenia przez dostawców usług płatniczych mechanizmu uwierzytelniania poczty mailowej DMARC (Domain-based Message Authentication, Reporting and Conformance), mającej na celu zapobieganie fałszowania maili i podszywania się pod domeny tych dostawców (phishing, e-mail spoofing).

IV. Rekomendacje w obszarze edukacji

1. Wydawanie w odniesieniu do klientów ostrzeżeń o różnych zagrożeniach i oszustwach, ogłaszanie dobrych praktyk bezpiecznego postępowania klientów oraz przeprowadzanie kampanii edukacyjnych dedykowanych do różnych grup odbiorców z wykorzystaniem środków przekazu popularnych w danej grupie,

2. Dbanie o świadomość społeczeństwa, poprzez szkolenia oraz kampanie edukacyjne i reklamowe, szczególnie kierowane w stronę osób starszych - w kontekście zagrożeń, rozpowszechnianie informacji i docieranie z nimi do odbiorców na temat metod socjotechnicznych i manipulacji, których używają przestępcy.

3. Rozważenie przeprowadzenia ogólnokrajowej dużej kampanii edukacyjnej ostrzegającej przed różnego rodzaju typami oszustw, np. w ogólnopolskiej telewizji oraz lokalnych i krajowych rozgłośniach radiowych,

4. Przeprowadzanie dla pracowników instytucji finansowych szkoleń potwierdzających kompetencje w obszarze bezpieczeństwa płatności i cyberbezpieczeństwa,

5. Organizowanie dla organów ścigania i wymiaru sprawiedliwości specjalistycznych warsztatów na bazie realnych studiów przypadku,

6. Przygotowanie treści edukacyjnych dotyczących bezpieczeństwa płatności i cyberbezpieczeństwa oraz ich włączenie w programy właściwych studiów podyplomowych i szkoleń branżowych,

7. Rozważenie wprowadzenia aspektów cyberedukacji i zasad bezpieczeństwa związanych z płatnościami w szkolnictwie od najmłodszych lat.

8. Rozważenie przeprowadzenia przez instytucje publiczne, np. przez UKNF lub Ministerstwo Finansów, kampanii informacyjnych mających na celu budowanie świadomości zagrożeń wśród użytkowników bankowości, którzy korzystają z płatności bezgotówkowych.