ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2018/389

z dnia 27 listopada 2017 r.

uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającą dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającą dyrektywę 2007/64/WE ([1]), w szczególności jej art. 98 ust. 4 akapit drugi,

a także mając na uwadze, co następuje:

(1) Usługi płatnicze oferowane drogą elektroniczną powinny być wykonywane w sposób bezpieczny, z użyciem technologii będących w stanie zagwarantować bezpieczne uwierzytelnianie użytkownika i w jak największym stopniu ograniczyć ryzyko oszustw. Procedura uwierzytelniania zasadniczo powinna obejmować mechanizmy monitorowania transakcji w celu wykrywania prób wykorzystania utraconych, skradzionych lub przywłaszczonych indywidualnych danych uwierzytelniających użytkownika usług płatniczych, a także powinna zapewniać, aby użytkownik usług płatniczych był użytkownikiem uprawnionym, a zatem wyraża zgodę na transfer środków pieniężnych i dostęp do informacji o swoim rachunku w ramach zwykłego stosowania indywidualnych danych uwierzytelniających. Ponadto konieczne jest określenie wymogów dotyczących silnego uwierzytelniania klienta, które należy stosować każdorazowo wówczas, gdy płatnik uzyskuje dostęp do swojego rachunku płatniczego w trybie online, inicjuje elektroniczną transakcję płatniczą lub przeprowadza czynność za pomocą kanału zdalnego, która może wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć, poprzez wprowadzenie wymogu generowania kodu uwierzytelniającego odpornego na ryzyko sfałszowania w całości lub na skutek ujawnienia dowolnych elementów, z których kod został wygenerowany.

(2) Mając na względzie, że metody dokonywania oszustw stale ewoluują, w ramach wymogów dotyczących silnego uwierzytelniania klienta należy dopuścić możliwość innowacji w zakresie rozwiązań technicznych, stanowiących odpowiedź na pojawianie się nowych zagrożeń dla bezpieczeństwa płatności elektronicznych. W celu zapewnienia nieprzerwanego skutecznego wdrażania wymogów, które zostaną sformułowane, należy również wymagać, aby środki bezpieczeństwa w zakresie stosowania silnego uwierzytelniania klienta i wyłączeń w tym zakresie, środki służące ochronie poufności i integralności indywidualnych danych uwierzytelniających oraz środki ustanawiające wspólne i bezpieczne otwarte standardy komunikacji były dokumentowane, okresowo badane, poddawane ocenie i audytowi przez audytorów posiadających wiedzę ekspercką w zakresie bezpieczeństwa informatycznego i płatności elektronicznych, którzy działają niezależnie. Aby właściwe organy mogły monitorować jakość przeglądu takich środków, przeglądy te należy udostępniać organom na ich żądanie.

(3) Zważywszy na fakt, że elektroniczne zdalne transakcje płatnicze obarczone są większym ryzykiem oszustwa, należy wprowadzić dodatkowe wymogi dotyczące silnego uwierzytelniania klienta w przypadku tych transakcji, zapewniające, aby elementy objęte uwierzytelnieniem dynamicznie łączyły transakcję z kwotą i odbiorcą określonymi przez płatnika w momencie zainicjowania transakcji.

(4) Dynamiczne łączenie można uzyskać poprzez generowanie kodów uwierzytelniających, które podlega zestawowi restrykcyjnych wymogów bezpieczeństwa. Aby zapewnić neutralność pod względem technologicznym, nie należy wymagać stosowania konkretnej technologii do celów wdrożenia kodów uwierzytelniających. Kody uwierzytelniające powinny zatem opierać się na takich rozwiązaniach, jak: generowanie i walidacja jednorazowych haseł, podpisy cyfrowe lub innego rodzaju metody stwierdzania ważności oparte na mechanizmach kryptograficznych z zastosowaniem kluczy lub materiału kryptograficznego przechowywanego w elementach uwierzytelnienia, z zastrzeżeniem spełnienia wymogów bezpieczeństwa.

([1]) Dz.U. L 337 z 23.12.2015, s. 35.

(5) Należy określić szczegółowe wymogi dotyczące sytuacji, w której w momencie zainicjowania elektronicznej zdalnej transakcji płatniczej przez płatnika ostateczna kwota transakcji nie jest znana, w celu zapewnienia, aby silne uwierzytelnianie klienta dotyczyło konkretnie maksymalnej kwoty, na jaką płatnik wyraził zgodę, jak określono w dyrektywie (UE) 2015/2366.

(6) Aby zagwarantować stosowanie silnego uwierzytelniania klienta, konieczny jest również wymóg zapewnienia odpowiednich zabezpieczeń w przypadku elementów silnego uwierzytelniania klienta, którymi to zabezpieczeniami mogą być: w przypadku elementów należących do kategorii „wiedza" (coś, co wie wyłącznie użytkownik) – długość lub złożoność; w przypadku elementów należących do kategorii „posiadanie" (coś, co posiada wyłącznie użytkownik) – specyfikacja algorytmu, długość klucza i entropia informacyjna; oraz w przypadku urządzeń i oprogramowania do odczytu elementów należących do kategorii „cechy klienta" (coś, czym jest użytkownik) – specyfikacja algorytmu, zabezpieczenia czytnika i wzorca biometrycznego, przy czym zabezpieczenia te są szczególnie istotne w celu ograniczenia ryzyka, że elementy te zostaną odkryte przez osoby niepowołane, ujawnione takim osobom lub przez nie wykorzystane. Konieczne jest również określenie wymogów w celu zapewnienia, aby elementy te były niezależne, tak aby naruszenie jednego z nich nie osłabiało wiarygodności pozostałych, w szczególności jeżeli którykolwiek z tych elementów jest stosowany w urządzeniu wielofunkcyjnym, czyli w urządzaniu takim jak tablet lub telefon komórkowy, które można wykorzystać zarówno do wydania dyspozycji płatności, jak i w procesie uwierzytelniania.

(7) Wymogi dotyczące silnego uwierzytelniania klienta mają zastosowanie do płatności zainicjowanych przez płatnika, niezależnie od tego, czy płatnik jest osobą fizyczną czy osobą prawną.

(8) Płatności dokonywane za pomocą instrumentów płatniczych używanych anonimowo ze względu na swój charakter nie podlegają obowiązkowi silnego uwierzytelniania klienta. Jeżeli na podstawie postanowień umowy lub przepisów prawa możliwość anonimowego używania takich instrumentów zostanie zniesiona, wówczas płatności podlegają wymogom bezpieczeństwa wynikającym z dyrektywy (UE) 2015/2366 i z przedmiotowego regulacyjnego standardu technicznego.

(9) Zgodnie z dyrektywą (UE) 2015/2366 wyłączenia z obowiązku stosowania zasady silnego uwierzytelniania klienta określono na podstawie poziomu ryzyka związanego z transakcją płatniczą, kwoty transakcji, powtarzalnego charakteru transakcji i kanału płatności używanego do wykonania transakcji płatniczej.

(10) Czynności, które wiążą się z dostępem do salda rachunku płatniczego i ostatnich transakcji na rachunku płatniczym bez ujawniania szczególnie chronionych danych dotyczących płatności, powtarzającymi się płatnościami na rzecz tych samych odbiorców, które zostały uprzednio ustanowione lub potwierdzone przez płatnika z zastosowaniem silnego uwierzytelnienia klienta, a także płatnościami dokonywanymi na rzecz tej samej osoby fizycznej lub prawnej posiadającej rachunek u tego samego dostawcy usług płatniczych oraz płatnościami dokonywanymi przez taką osobę, charakteryzują się niskim poziomem ryzyka, w związku z czym dostawcy usług płatniczych nie muszą stosować silnego uwierzytelniania klienta. Niezależnie do powyższego, zgodnie z art. 65, 66 i 67 dyrektywy (UE) 2015/2366 dostawcy świadczący usługę inicjowania płatności, dostawcy usług płatniczych wydający instrumenty płatnicze oparte na karcie i dostawcy świadczący usługę dostępu do informacji o rachunku powinni występować do dostawcy usług płatniczych prowadzącego rachunek o niezbędne i istotne informacje na potrzeby świadczenia danej usługi płatniczej i je od niego uzyskiwać wyłącznie za zgodą użytkownika usług płatniczych. Taka zgoda może zostać udzielona indywidualnie w odniesieniu do poszczególnych wniosków o udzielenie informacji lub inicjowanych płatności lub, w przypadku dostawców świadczących usługę dostępu do informacji o rachunku, jako upoważnienie w odniesieniu do wyznaczonego rachunku płatniczego i powiązanych transakcji płatniczych określonych w ramach uzgodnienia umownego z użytkownikiem usług płatniczych.

(11) Należy przewidzieć wyłączenia dotyczące niskokwotowych płatności zbliżeniowych w punktach sprzedaży, uwzględniające również maksymalną liczbę następujących po sobie transakcji lub pewną ustaloną maksymalną wartość następujących po sobie transakcji, które nie wymagają stosowania silnego uwierzytelniania klienta, gdyż takie wyłączenia pozwalają na rozwój usług płatniczych przyjaznych użytkownikowi i obarczonych niskim ryzykiem. Należy również wprowadzić wyłączenie dotyczące elektronicznych transakcji płatniczych inicjowanych za pomocą terminali samoobsługowych w sytuacjach, w których zastosowanie silnego uwierzytelnienia klienta może nie zawsze być łatwe ze względów operacyjnych (np. w celu uniknięcia kolejek i ewentualnych wypadków w bramkach poboru opłat za przejazd lub ze względu na innego rodzaju ryzyko w zakresie bezpieczeństwa lub ochrony).

(12) Podobnie jak w przypadku wyłączenia dotyczącego niskokwotowych płatności zbliżeniowych w punkcie sprzedaży należy osiągnąć właściwą równowagę między koniecznością osiągnięcia większego bezpieczeństwa zdalnych transakcji płatniczych a potrzebą zapewnienia, aby płatności w obszarze handlu elektronicznego były przyjazne użytkownikowi i łatwo dostępne. W myśl tych zasad progi, poniżej których nie trzeba stosować żadnego silnego uwierzytelniania klienta, należy określać w sposób ostrożny, tak aby uwzględnić wyłącznie zakupy przez internet o niskiej wartości. Progi w odniesieniu do zakupów przez internet należy określać w sposób bardziej ostrożny, ponieważ brak fizycznej obecności danej osoby przy dokonywaniu zakupu stwarza nieznacznie większe ryzyko dla bezpieczeństwa.

(13) Wymogi dotyczące silnego uwierzytelniania klienta mają zastosowanie do płatności zainicjowanych przez płatnika, niezależnie od tego, czy płatnik jest osobą fizyczną czy osobą prawną. Wiele płatności korporacyjnych jest inicjowanych za pomocą specjalnych procesów lub protokołów gwarantujących wysokie poziomy bezpieczeństwa płatności, które dyrektywa (UE) 2015/2366 ma na celu osiągnąć za pomocą silnego uwierzytelniania klienta. Jeżeli właściwe organy ustalą, że takie procesy lub protokoły płatności – dostępne wyłącznie dla płatników, którzy nie są konsumentami – zapewniają osiągnięcie celów w zakresie bezpieczeństwa określonych w dyrektywie (UE) 2015/2366, dostawcy usług płatniczych mogą, w odniesieniu do takich procesów lub protokołów, zostać zwolnieni z wymogu stosowania silnego uwierzytelniania klienta.

(14) Jeżeli w ramach analizy ryzyka transakcji w czasie rzeczywistym dana transakcja płatnicza zostaje uznana za transakcję niskiego ryzyka, wówczas również stosowne jest wprowadzenie wyłączenia wobec dostawcy usług płatniczych, który nie zamierza stosować silnego uwierzytelniania klienta, przyjmując zamiast tego skuteczne wymogi oparte na analizie ryzyka, które gwarantują bezpieczeństwo środków pieniężnych i danych osobowych użytkownika usług płatniczych. Takie wymogi oparte na analizie ryzyka powinny uwzględniać wyniki analizy ryzyka – potwierdzające, że nie odnotowano żadnego nadzwyczajnego schematu wydatków ani wzorca zachowań ze strony płatnika, z uwzględnieniem innych czynników ryzyka, w tym informacji na temat lokalizacji płatnika i odbiorcy – w połączeniu z progami kwotowymi opartymi na wskaźnikach oszustw obliczonych dla zdalnych transakcji płatniczych. Jeżeli – na podstawie analizy ryzyka transakcji w czasie rzeczywistym – danej płatności nie można uznać za płatność charakteryzującą się niskim poziomem ryzyka, dostawca usług płatniczych powinien powrócić do stosowania silnego uwierzytelniania klienta. Maksymalną wartość, której może dotyczyć tego rodzaju wyłączenie na podstawie analizy ryzyka, należy określić w sposób zapewniający bardzo niski odnośny wskaźnik oszustw, również w porównaniu ze wskaźnikami oszustw dla wszystkich transakcji płatniczych realizowanych przez danego dostawcę usług płatniczych, w tym transakcji uwierzytelnionych z zastosowaniem silnego uwierzytelnienia klienta, w określonym przedziale czasowym i w ujęciu kroczącym.

(15) Do celów zapewnienia skutecznego egzekwowania wyłączeń dostawcy usług płatniczych, którzy pragną korzystać z wyłączeń z obowiązku stosowania silnego uwierzytelniania klienta, powinni regularnie monitorować i udostępniać właściwym organom i Europejskiemu Urzędowi Nadzoru Bankowego (EUNB), na ich żądanie i w odniesieniu do każdego rodzaju transakcji płatniczych, wartość nielegalnych lub nieautoryzowanych transakcji płatniczych i odnotowane wskaźniki oszustw w odniesieniu do wszystkich realizowanych przez nich transakcji płatniczych, zarówno tych uwierzytelnionych z zastosowaniem silnego uwierzytelniania klienta, jak i tych realizowanych w oparciu o stosowne wyłączenie.

(16) Gromadzenie tych nowych danych historycznych dotyczących wskaźników oszustw w przypadku elektronicznych transakcji płatniczych przyczyni się również do skutecznego przeglądu progów dokonywanego przez EUNB na potrzeby wyłączenia z obowiązku stosowania silnego uwierzytelniania klienta na podstawie analizy ryzyka transakcji w czasie rzeczywistym. EUNB powinien dokonywać przeglądu przedmiotowych regulacyjnych standardów technicznych i, w stosownych przypadkach, przedłożyć Komisji wniosek dotyczący ich aktualizacji, przedstawiając projekty nowych progów i stosownych wskaźników oszustw w celu zwiększenia bezpieczeństwa zdalnych płatności elektronicznych zgodnie z art. 98 ust. 5 dyrektywy (UE) 2015/2366 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 ([1]).

(17) Dostawcy usług płatniczych korzystający z przewidzianych wyłączeń powinni w każdej chwili mieć możliwość podjęcia decyzji o stosowaniu silnego uwierzytelniania klienta w odniesieniu do czynności i transakcji płatniczych, o których mowa w tych przepisach.

(18) Środki służące ochronie poufności i integralności indywidualnych danych uwierzytelniających, jak również urządzenia i oprogramowanie uwierzytelniające powinny ograniczać ryzyko związane z oszustwami popełnianymi w ramach nieuprawnionego lub nielegalnego użycia instrumentów płatniczych oraz nieuprawnionego dostępu do rachunków płatniczych. W tym celu konieczne jest wprowadzenie wymogów dotyczących bezpiecznego tworzenia oraz dostarczania indywidualnych danych uwierzytelniających i ich powiązania z użytkownikiem usług płatniczych, a także określenie warunków odnowienia i dezaktywacji takich danych uwierzytelniających.

(19) Aby zapewnić skuteczną i bezpieczną komunikację między odpowiednimi podmiotami w kontekście usług dostępu do informacji o rachunku, usług inicjowania płatności i potwierdzania dostępności środków pieniężnych, konieczne jest określenie wymogów w zakresie wspólnych i bezpiecznych otwartych standardów komunikacji, których muszą przestrzegać wszyscy odpowiedni dostawcy usług płatniczych. W dyrektywie (UE) 2015/2366 przewidziano dostęp dostawców świadczących usługę dostępu do informacji o rachunku do informacji o rachunku płatniczym i korzystanie przez nich z takich informacji. Niniejsze rozporządzenie nie zmienia zatem zasad dotyczących dostępu do rachunków innych niż rachunki płatnicze.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

(20) Każdy dostawca usług płatniczych prowadzący rachunek, który obsługuje rachunki płatnicze dostępne za pośrednictwem internetu, powinien zapewnić co najmniej jeden interfejs dostępu umożliwiający bezpieczną komunikację z dostawcami świadczącymi usługę dostępu do informacji o rachunku, dostawcami świadczącymi usługę inicjowania płatności i dostawcami usług płatniczych wydającymi instrumenty płatnicze oparte na karcie. Taki interfejs powinien zapewniać dostawcom świadczącym usługę dostępu do informacji o rachunku, dostawcom świadczącym usługę inicjowania płatności i dostawcom usług płatniczych wydającym instrumenty płatnicze oparte na karcie możliwość identyfikacji siebie wobec dostawcy usług płatniczych prowadzącego rachunek. Taki interfejs powinien również umożliwiać dostawcom świadczącym usługę dostępu do informacji o rachunku i dostawcom świadczącym usługę inicjowania płatności poleganie na procedurach uwierzytelniania zapewnianych użytkownikowi usług płatniczych przez dostawcę usług płatniczych prowadzącego rachunek. Aby zapewnić neutralność technologii i modelu biznesowego, dostawcy usług płatniczych prowadzący rachunek powinni mieć możliwość dokonania wyboru, czy zapewnią osobny interfejs przeznaczony do komunikacji z dostawcami świadczącymi usługę dostępu do informacji o rachunku, dostawcami świadczącymi usługę inicjowania płatności i dostawcami usług płatniczych wydającymi instrumenty płatnicze oparte na karcie, czy też dopuszczą, do celów takiej komunikacji, stosowanie interfejsu służącego do identyfikacji użytkowników usług płatniczych dostawców usług płatniczych prowadzących rachunek i do komunikacji z takimi użytkownikami.

(21) Specyfikacja techniczna interfejsu powinna być odpowiednio udokumentowana i podana do wiadomości publicznej, aby dostawcy świadczący usługę dostępu do informacji o rachunku, dostawcy świadczący usługę inicjowania płatności i dostawcy usług płatniczych wydający instrumenty płatnicze oparte na karcie mogli opracować swoje rozwiązania techniczne. Ponadto dostawca usług płatniczych prowadzący rachunek powinien zapewnić mechanizm umożliwiający dostawcom usług płatniczych przetestowanie swoich rozwiązań technicznych co najmniej na sześć miesięcy przed datą rozpoczęcia stosowania niniejszych standardów regulacyjnych lub, jeżeli uruchomienie takich rozwiązań następuje po dacie rozpoczęcia stosowania niniejszych standardów, przed datą wprowadzenia interfejsu na rynek. Aby zapewnić interoperacyjność różnych technologicznych rozwiązań komunikacyjnych, interfejs musi opierać się na standardach komunikacji opracowanych przez międzynarodowe lub europejskie organizacje normalizacyjne.

(22) Jakość usług świadczonych przez dostawców świadczących usługę dostępu do informacji o rachunku i dostawców świadczących usługę inicjowania płatności będzie zależeć od prawidłowego działania interfejsów wprowadzonych lub dostosowanych przez dostawców usług płatniczych prowadzących rachunek. Ważne jest zatem, aby w przypadku braku zgodności takich interfejsów z przepisami określonymi w przedmiotowych standardach podejmowano środki gwarantujące ciągłość działania z myślą o użytkownikach przedmiotowych usług. Właściwe organy krajowe odpowiadają za zapewnienie, aby nie dochodziło do blokowania ani zakłócania usług świadczonych przez dostawców świadczących usługę dostępu do informacji o rachunku i dostawców świadczących usługę inicjowania płatności.

(23) Jeżeli dostęp do rachunków płatniczych odbywa się za pośrednictwem specjalnego interfejsu, aby zapewnić użytkownikom usług płatniczych prawo do korzystania z usług dostawców świadczących usługę inicjowania płatności i z usług umożliwiających dostęp do informacji o rachunku, jak przewidziano w dyrektywie (UE) 2015/2366, konieczne jest określenie wymogu, zgodnie z którym poziom dostępności i efektywności specjalnych interfejsów musi odpowiadać poziomowi dostępności i efektywności interfejsu dostępnego dla użytkownika usług płatniczych. Dostawcy usług płatniczych prowadzący rachunek powinni również określić przejrzyste kluczowe wskaźniki efektywności i cele w zakresie gwarantowanego poziomu usług w odniesieniu do dostępności i efektywności specjalnych interfejsów, które to wskaźniki i cele powinny być przynajmniej w równym stopniu rygorystyczne co wskaźniki i cele wykorzystywane w odniesieniu do interfejsu stosowanego na potrzeby ich użytkowników usług płatniczych. Takie interfejsy powinny być testowane przez dostawców usług płatniczych, którzy będą z nich korzystać, i powinny podlegać testom warunków skrajnych i monitorowaniu prowadzonym przez właściwe organy.

(24) W celu zagwarantowania, aby dostawcy usług płatniczych świadczący usługi w oparciu o specjalny interfejs mogli nadal świadczyć swoje usługi w przypadku wystąpienia problemów związanych z dostępnością lub nieprawidłowym działaniem tego interfejsu, konieczne jest zapewnienie, z zastrzeżeniem rygorystycznych warunków, mechanizmu rezerwowego umożliwiającego takim dostawcom korzystanie z interfejsu utrzymywanego przez dostawcę usług płatniczych prowadzącego rachunek do celów identyfikacji swoich własnych użytkowników usług płatniczych i komunikacji z nimi. Niektórzy dostawcy usług płatniczych prowadzący rachunek zostaną wyłączeni z obowiązku zapewnienia takiego mechanizmu rezerwowego za pośrednictwem stosowanego przez nich interfejsu widocznego dla klienta, jeżeli właściwe organy, którym podlegają, stwierdzą, że specjalne interfejsy spełniają szczegółowe warunki zapewniające niezakłóconą konkurencję. Jeżeli specjalne interfejsy objęte wyłączeniem nie spełniają koniecznych warunków, odpowiednie właściwe organy cofają udzielone wyłączenia.

(25) Aby właściwe organy mogły skutecznie nadzorować i monitorować wdrażanie interfejsów komunikacyjnych i zarządzanie nimi, dostawcy usług płatniczych prowadzący rachunek powinni udostępniać na swojej stronie internetowej podsumowanie odpowiedniej dokumentacji i udostępniać właściwym organom na żądanie dokumentację rozwiązań na wypadek wystąpienia sytuacji nadzwyczajnych. Dostawcy usług płatniczych prowadzący rachunek powinni również podawać do wiadomości publicznej dane statystyczne dotyczące dostępności i efektywności interfejsu.

(26) Aby zagwarantować poufność i integralność danych, konieczne jest zapewnienie bezpieczeństwa sesji komunikacyjnych między dostawcami usług płatniczych prowadzącymi rachunek, dostawcami świadczącymi usługę

dostępu do informacji o rachunku, dostawcami świadczącymi usługę inicjowania płatności i dostawcami usług płatniczych wydającymi instrumenty płatnicze oparte na karcie. Należy w szczególności wprowadzić wymóg, by stosowano bezpieczne szyfrowanie podczas wymiany danych między dostawcami świadczącymi usługę dostępu do informacji o rachunku, dostawcami świadczącymi usługę inicjowania płatności i dostawcami usług płatniczych wydającymi instrumenty płatnicze oparte na karcie a dostawcami usług płatniczych prowadzącymi rachunek.

(27) Aby zwiększyć zaufanie użytkowników i zapewnić silne uwierzytelnianie klienta, należy uwzględnić stosowanie środków identyfikacji elektronicznej i usług zaufania określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([1]), w szczególności w odniesieniu do notyfikowanych systemów identyfikacji elektronicznej.

(28) W celu zapewnienia jednolitych dat rozpoczęcia stosowania niniejsze rozporządzenie powinno mieć zastosowanie od tego samego dnia, od którego państwa członkowskie muszą zapewnić stosowanie środków bezpieczeństwa, o których mowa w art. 65, 66, 67 i 97 dyrektywy (UE) 2015/2366.

(29) Podstawę niniejszego rozporządzenia stanowi projekt regulacyjnych standardów technicznych przedłożony Komisji przez Europejski Urząd Nadzoru Bankowego (EUNB).

(30) EUNB przeprowadził otwarte przejrzyste konsultacje publiczne na temat projektu regulacyjnych standardów technicznych, który stanowi podstawę niniejszego rozporządzenia, dokonał analizy potencjalnych powiązanych kosztów i korzyści oraz zwrócił się o opinię do Bankowej Grupy Interesariuszy ustanowionej zgodnie z art. 37 rozporządzenia (UE) nr 1093/2010,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu ustanawia się wymogi, które dostawcy usług płatniczych muszą spełniać w celu wdrożenia środków bezpieczeństwa umożliwiających tym dostawcom:

a) stosowanie procedury silnego uwierzytelniania klienta zgodnie z art. 97 dyrektywy (UE) 2015/2366;

b) skorzystanie z wyłączenia z obowiązku stosowania wymogów bezpieczeństwa dotyczących silnego uwierzytelniania klienta pod warunkiem spełnienia określonych i ograniczonych warunków, które zależą od poziomu ryzyka, kwoty i powtarzalnego charakteru transakcji płatniczej oraz kanału płatności wykorzystanego do jej dokonania;

c) ochrona poufności i integralności indywidualnych danych uwierzytelniających użytkowników usług płatniczych;

d) określenie wspólnych, bezpiecznych i otwartych standardów komunikacji między dostawcami usług płatniczych prowadzącymi rachunek, dostawcami świadczącymi usługę inicjowania płatności, dostawcami świadczącymi usługę dostępu do informacji o rachunku, płatnikami, odbiorcami i innymi dostawcami usług płatniczych w odniesieniu do świadczenia i korzystania z usług płatniczych przy stosowaniu tytułu IV dyrektywy (UE) 2015/2366.

Artykuł 2

Ogólne wymogi dotyczące uwierzytelniania

1. Dostawcy usług płatniczych posiadają mechanizmy monitorowania transakcji, które umożliwiają im wykrywanie nieautoryzowanych lub nielegalnych transakcji płatniczych, w celu wdrożenia środków bezpieczeństwa, o których mowa w art. 1 lit. a) i b).

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 53).

Podstawę tych mechanizmów stanowi analiza transakcji płatniczych z uwzględnieniem elementów, które są typowe dla danego użytkownika usług płatniczych w warunkach zwykłego stosowania indywidualnych danych uwierzytelniających.

2. Dostawcy usług płatniczych zapewniają uwzględnienie w ramach mechanizmów monitorowania transakcji przynajmniej każdego z następujących czynników opartych na analizie ryzyka:

a) wykazów elementów uwierzytelnienia, które użyto w sposób nieuprawniony lub skradziono;

b) kwoty każdej transakcji płatniczej;

c) znanych scenariuszy oszustw w zakresie świadczenia usług płatniczych;

d) sygnałów wskazujących na obecność złośliwego oprogramowania w którejkolwiek sesji procesu uwierzytelniania;

e) w przypadku udostępniania urządzenia lub oprogramowania dostępowego przez dostawcę usług płatniczych – historii stosowania urządzenia lub oprogramowania dostępowego przekazanego użytkownikowi usług płatniczych i niestandardowego korzystania z urządzenia lub oprogramowania dostępowego.

Artykuł 3

Przegląd środków bezpieczeństwa

1. Wdrażanie środków bezpieczeństwa, o których mowa w art. 1, jest dokumentowane, okresowo badane, poddawane ocenie i audytowi zgodnie z mającymi zastosowanie ramami prawnymi właściwymi dla dostawcy usług płatniczych przez audytorów posiadających wiedzę ekspercką w dziedzinie bezpieczeństwa informatycznego i płatności elektronicznych, którzy działają niezależnie w ramach podmiotu będącego dostawcą usług płatniczych lub jako odrębny podmiot.

2. Okres między audytami, o których mowa w ust. 1, określa się z uwzględnieniem istotnych ram księgowania i badań ustawowych mających zastosowanie do dostawcy usług płatniczych.

Dostawcy usług płatniczych korzystający z wyłączenia, o którym mowa w art. 18, podlegają jednak audytowi metodyki, modelu i zgłoszonych wskaźników oszustw przeprowadzanemu co najmniej raz w roku. Audytor prowadzący przedmiotowy audyt musi posiadać wiedzę ekspercką w zakresie bezpieczeństwa informatycznego i płatności elektronicznych oraz działać niezależnie w ramach podmiotu będącego dostawcą usług płatniczych lub jako odrębny podmiot. W trakcie pierwszego roku stosowania wyłączenia na podstawie art. 18, a następnie co najmniej co trzy lata lub – na wniosek właściwego organu – częściej, przedmiotowy audyt przeprowadza niezależny i uprawniony audytor zewnętrzny.

3. W wyniku wspomnianego audytu przedstawia się ocenę i sprawozdanie w zakresie zgodności środków bezpieczeństwa stosowanych przez dostawcę usług płatniczych z wymogami określonymi w niniejszym rozporządzeniu.

Kompletne sprawozdanie udostępnia się właściwym organom na ich wniosek.

ROZDZIAŁ II

ŚRODKI BEZPIECZEŃSTWA PRZY STOSOWANIU SILNEGO UWIERZYTELNIENIA KLIENTA

Artykuł 4

Kod uwierzytelniający

1. W przypadkach gdy dostawcy usług płatniczych stosują silne uwierzytelnianie klienta zgodnie z art. 97 ust. 1 dyrektywy (UE) 2015/2366, uwierzytelnianie opiera się na zastosowaniu co najmniej dwóch elementów należących do kategorii „wiedza", „posiadanie" i „cechy klienta" oraz prowadzi do wygenerowania kodu uwierzytelniającego.

Dostawca usług płatniczych przyjmuje kod uwierzytelniający wyłącznie jeden raz, w przypadku gdy płatnik używa kodu uwierzytelniającego w celu uzyskania dostępu do swojego rachunku płatniczego w trybie online, w celu zainicjowania elektronicznej transakcji płatniczej lub w celu przeprowadzenia jakiejkolwiek czynności za pomocą kanału zdalnego, która może wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć.

2. Do celów ust. 1 dostawcy usług płatniczych przyjmują środki bezpieczeństwa zapewniające spełnienie każdego z określonych poniżej wymogów:

a) z ujawnionego kodu uwierzytelniającego nie można pozyskać żadnych informacji dotyczących elementów, o których mowa w ust. 1;

b) wygenerowanie nowego kodu uwierzytelniającego nie jest możliwe na podstawie znajomości jakiegokolwiek innego kodu uwierzytelniającego wygenerowanego wcześniej;

c) kodu uwierzytelniającego nie można sfałszować.

3. Dostawcy usług płatniczych zapewniają, ab uwierzytelnianie poprzez generowanie kodu uwierzytelniającego obejmowało następujące środki:

a) jeżeli uwierzytelnianie na potrzeby dostępu zdalnego, zdalnych płatności elektronicznych i wszelkich innych czynności przeprowadzanych za pomocą kanału zdalnego, które mogą wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć, nie wygenerowało kodu uwierzytelniającego do celów ust. 1, nie jest możliwe ustalenie, który z elementów, o których mowa w tym ustępie, był błędny;

b) liczba mogących nastąpić po sobie nieudanych prób uwierzytelnienia, po przekroczeniu której wykonanie czynności, o których mowa w art. 97 ust. 1 dyrektywy (UE) 2015/2366, zostaje tymczasowo lub stale zablokowane, nie przekracza pięciu prób w określonym okresie;

c) sesje komunikacyjne są chronione przed przechwyceniem danych uwierzytelniających przekazywanych podczas uwierzytelniania oraz przed manipulacją ze strony osób niepowołanych, zgodnie z wymogami określonymi w rozdziale V;

d) maksymalny czas bezczynności płatnika po jego uwierzytelnieniu na potrzeby dostępu do jego rachunku płatniczego w trybie online nie przekracza pięciu minut.

4. Jeżeli blokada, o której mowa w ust. 3 lit. b), jest tymczasowa, czas trwania tej blokady i liczbę ponownych prób określa się na podstawie cech usługi świadczonej na rzecz płatnika oraz wszelkich istotnych rodzajów ryzyka, uwzględniając – co najmniej – czynniki, o których mowa w art. 2 ust. 2.

Płatnika powiadamia się przed nałożeniem stałej blokady.

W przypadku nałożenia stałej blokady ustanawia się bezpieczną procedurę umożliwiającą płatnikowi odzyskanie dostępu do zablokowanych instrumentów płatności elektronicznej.

Artykuł 5

Dynamiczne połączenia

1. Jeżeli dostawcy usług płatniczych – oprócz wymogów określonych w art. 4 niniejszego rozporządzenia – stosują silne uwierzytelnianie klienta zgodnie z art. 97 ust. 2 dyrektywy (UE) 2015/2366, przyjmują oni również środki bezpieczeństwa spełniające każdy z następujących wymogów:

a) płatnika powiadamia się o kwocie transakcji płatniczej oraz o odbiorcy;

b) wygenerowany kod uwierzytelniający jest przypisany do kwoty transakcji płatniczej oraz do odbiorcy, które płatnik zaakceptował podczas inicjowania transakcji;

c) kod uwierzytelniający przyjęty przez dostawcę usług płatniczych odpowiada pierwotnej konkretnej kwocie transakcji płatniczej oraz tożsamości odbiorcy, które płatnik zaakceptował;

d) wszelkie zmiany kwoty lub odbiorcy skutkują unieważnieniem wygenerowanego kodu uwierzytelniającego.

2. Do celów ust. 1 dostawcy usług płatniczych przyjmują środki bezpieczeństwa zapewniające poufność, autentyczność i integralność każdego z następujących elementów:

a) kwoty transakcji i odbiorcy na wszystkich etapach uwierzytelniania;

b) informacji wyświetlanych płatnikowi na wszystkich etapach uwierzytelniania, w tym podczas generowania, przekazywania i wykorzystania kodu uwierzytelniającego.

3. Do celów ust. 1 lit. b) oraz jeżeli dostawcy usług płatniczych stosują silne uwierzytelnianie klienta zgodnie z art. 97 ust. 2 dyrektywy (UE) 2015/2366, do kodu uwierzytelniającego zastosowanie mają następujące wymogi:

a) w stosunku do transakcji płatniczych realizowanych w oparciu o kartę, w odniesieniu do których płatnik udzielił zgody na zablokowanie konkretnej kwoty środków pieniężnych zgodnie z art. 75 ust. 1 przedmiotowej dyrektywy, kod uwierzytelniający jest przypisany do kwoty, na zablokowanie której płatnik udzielił zgody i na którą przystał podczas inicjowania transakcji;

b) w stosunku do transakcji płatniczych, w odniesieniu do których płatnik udzielił zgody na przeprowadzenie serii zdalnych elektronicznych transakcji płatniczych na rzecz jednego odbiorcy lub wielu odbiorców, kod uwierzytelniający jest przypisany do całkowitej kwoty serii transakcji płatniczych oraz do określonych odbiorców.

Artykuł 6

Wymogi dotyczące elementów należących do kategorii „wiedza"

1. Dostawcy usług płatniczych przyjmują środki łagodzące ryzyko odkrycia przez osoby niepowołane lub ujawnienia osobom niepowołanym elementów silnego uwierzytelniania klienta należących do kategorii „wiedza".

2. Wykorzystanie tych elementów przez płatnika podlega środkom ograniczającym ryzyko w celu zapobieżenia ujawnieniu ich osobom niepowołanym.

Artykuł 7

Wymogi dotyczące elementów należących do kategorii „posiadanie"

1. Dostawcy usług płatniczych przyjmują środki łagodzące ryzyko wykorzystania przez osoby niepowołane elementów silnego uwierzytelniania klienta należących do kategorii „posiadanie".

2. Wykorzystanie tych elementów przez płatnika podlega środkom opracowanym w celu zapobieżenia powielaniu tych elementów.

Artykuł 8

Wymogi dotyczące urządzeń i oprogramowania powiązanych z elementami należącymi do kategorii „cechy klienta"

1. Dostawcy usług płatniczych przyjmują środki łagodzące ryzyko odkrycia przez osoby niepowołane elementów uwierzytelniania należących do kategorii „cechy klienta" i odczytywanych przez udostępnione płatnikowi urządzenia i oprogramowanie dostępowe. Dostawcy usług płatniczych zapewniają przynajmniej bardzo niskie prawdopodobieństwo uwierzytelnienia osób niepowołanych jako płatnika przez przedmiotowe urządzenia i oprogramowanie dostępowe.

2. Wykorzystanie tych elementów przez płatnika podlega środkom zapewniającym odporność przedmiotowych urządzeń i przedmiotowego oprogramowania na nieuprawnione użycie elementów za pośrednictwem dostępu do tych urządzeń i tego oprogramowania.

Artykuł 9

Niezależność elementów

1. Dostawcy usług płatniczych zapewniają, aby wykorzystanie elementów silnego uwierzytelniania klienta, o których mowa w art. 6, 7 i 8, podlegało środkom gwarantującym, że – pod względem technologii, algorytmów i parametrów – naruszenie jednego z elementów nie osłabia wiarygodności pozostałych elementów.

2. W przypadku gdy z któregokolwiek z elementów silnego uwierzytelniania klienta lub z samego kodu uwierzytelniającego korzysta się za pośrednictwem urządzenia wielofunkcyjnego, dostawcy usług płatniczych przyjmują środki bezpieczeństwa, aby zmniejszyć ryzyko wynikające z możliwości użycia tego urządzenia wielofunkcyjnego w sposób nieuprawniony.

3. Do celów ust. 2 środki ograniczające ryzyko zawierają każdy z następujących elementów:

a) stosowanie osobnych bezpiecznych środowisk uruchomieniowych za pośrednictwem oprogramowania zainstalowanego na urządzeniu wielofunkcyjnym;

b) mechanizmy zapewniające, aby płatnik lub osoba trzecia nie dokonali zmian w oprogramowaniu bądź urządzeniu;

c) jeżeli wprowadzono zmiany – mechanizmy łagodzące konsekwencje wprowadzonych zmian.

ROZDZIAŁ III

WYŁĄCZENIA Z OBOWIĄZKU STOSOWANIA SILNEGO UWIERZYTELNIANIA KLIENTA

Artykuł 10

Informacje o rachunku płatniczym

1. Dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta, z zastrzeżeniem spełnienia wymogów określonych w art. 2 i w ust. 2 niniejszego artykułu, w przypadku gdy dostęp użytkownika usług płatniczych ogranicza się do dostępu do jednej z wymienionych niżej pozycji w trybie online lub do obu tych pozycji bez ujawniania szczególnie chronionych danych dotyczących płatności:

a) salda jednego wyznaczonego rachunku płatniczego lub większej liczby wyznaczonych rachunków płatniczych;

b) transakcji płatniczych przeprowadzonych w ciągu ostatnich 90 dni za pośrednictwem jednego wyznaczonego rachunku płatniczego lub większej ich liczby.

2. Do celów ust. 1 dostawcy usług płatniczych nie podlegają wyłączeniu z obowiązku stosowania silnego uwierzytelniania klienta, jeżeli spełniony jest którykolwiek z następujących warunków:

a) użytkownik usług płatniczych uzyskuje dostęp do informacji określonych w ust. 1 w trybie online po raz pierwszy;

b) minęło więcej niż 90 dni odkąd użytkownik usług płatniczych po raz ostatni uzyskał dostęp do informacji określonych w ust. 1 lit. b) w trybie online oraz odkąd ostatni raz zastosowano silne uwierzytelnianie klienta.

Artykuł 11

Płatności zbliżeniowe w punktach sprzedaży

Dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta, z zastrzeżeniem spełnienia wymogów określonych w art. 2, w przypadku gdy płatnik inicjuje zbliżeniową elektroniczną transakcję płatniczą i jeżeli spełnione zostały następujące warunki:

a) pojedyncza kwota zbliżeniowej elektronicznej transakcji płatniczej nie przekracza 50 EUR; oraz

b) łączna kwota poprzednich zbliżeniowych elektronicznych transakcji płatniczych zainicjowanych za pomocą instrumentu płatniczego posiadającego funkcję płatności zbliżeniowej od dnia ostatniego zastosowania silnego uwierzytelnienia klienta nie przekracza 150 EUR; lub

c) liczba następujących po sobie zbliżeniowych elektronicznych transakcji płatniczych zainicjowanych za pomocą instrumentu płatniczego posiadającego funkcję płatności zbliżeniowej od dnia ostatniego zastosowania silnego uwierzytelnienia klienta nie przekracza pięciu.

Artykuł 12

Terminale samoobsługowe służące uiszczaniu opłat za przejazd i opłat za postój

Dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta, z zastrzeżeniem spełnienia wymogów określonych w art. 2, jeżeli płatnik inicjuje elektroniczną transakcję płatniczą w terminale samoobsługowym służącym do regulowania opłat za przejazd lub opłat za postój.

Artykuł 13

Zaufani odbiorcy

1. Dostawcy usług płatniczych stosują silne uwierzytelnianie klienta, w przypadku gdy płatnik tworzy lub zmienia listę zaufanych odbiorców za pośrednictwem swojego dostawcy usług płatniczych prowadzącego rachunek.

2. Dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta, z zastrzeżeniem spełnienia ogólnych wymogów dotyczących uwierzytelniania, jeżeli płatnik inicjuje transakcję płatniczą, a odbiorca znajduje się na liście zaufanych odbiorców utworzonej uprzednio przez płatnika.

Artykuł 14

Transakcje cykliczne

1. Dostawcy usług płatniczych stosują silne uwierzytelnianie klienta w przypadku, gdy płatnik tworzy, zmienia lub po raz pierwszy inicjuje serię transakcji cyklicznych opiewających na tę samą kwotę na rzecz tego samego odbiorcy.

2. Dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta, z zastrzeżeniem spełnienia ogólnych wymogów dotyczących uwierzytelniania, w odniesieniu do inicjowania wszystkich kolejnych transakcji płatniczych należących do serii transakcji płatniczych, o których mowa w ust. 1.

Artykuł 15

Polecenia przelewu miedzy rachunkami będącymi w posiadaniu tej samej osoby fizycznej lub prawnej

Dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta, z zastrzeżeniem spełnienia wymogów określonych w art. 2, jeżeli płatnik inicjuje polecenie przelewu w sytuacji, gdy płatnik i odbiorca są tą samą osobą fizyczną lub prawną i oba rachunki płatnicze są prowadzone przez tego samego dostawcę usług płatniczych prowadzącego rachunek.

Artykuł 16

Transakcje niskokwotowe

Dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta, jeżeli płatnik inicjuje zdalną elektroniczną transakcję płatniczą i jeżeli spełnione zostały następujące warunki:

a) kwota zdalnej elektronicznej transakcji płatniczej nie przekracza 30 EUR; oraz

b) łączna kwota poprzednich zdalnych elektronicznych transakcji płatniczych zainicjowanych przez płatnika od dnia ostatniego zastosowania silnego uwierzytelnienia klienta nie przekracza 100 EUR; lub

c) liczba poprzednio wykonanych zdalnych elektronicznych transakcji płatniczych zainicjowanych przez płatnika od dnia ostatniego zastosowania silnego uwierzytelnienia klienta nie przekracza pięciu następujących po sobie, pojedynczych zdalnych elektronicznych transakcji płatniczych.

Artykuł 17

Procesy i protokoły realizacji bezpiecznych płatności korporacyjnych

Dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta wobec osób prawnych inicjujących elektroniczne transakcje płatnicze za pośrednictwem przeznaczonych do tego procesów lub protokołów, które udostępnia się wyłącznie płatnikom niebędącym konsumentami, jeżeli właściwe organy uznają, że przedmiotowe procesy lub protokoły gwarantują poziom bezpieczeństwa równoważny co najmniej poziomowi przewidzianemu w dyrektywie (UE) 2015/2366.

Artykuł 18

Analiza ryzyka transakcji

1. Dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta, jeżeli płatnik inicjuje zdalną elektroniczną transakcję płatniczą, którą dostawca usług płatniczych uzna za charakteryzującą się niskim poziomem ryzyka zgodnie z mechanizmami monitorowania transakcji, o których mowa w art. 2 oraz w ust. 2 lit. c) niniejszego artykułu.

2. Elektroniczną transakcję płatniczą, o której mowa w ust. 1, uznaje się za charakteryzującą się niskim poziomem ryzyka, jeżeli spełnione są wszystkie następujące warunki:

a) wskaźnik oszustw dla tego rodzaju transakcji, zgłoszony przez dostawcę usług płatniczych i obliczony zgodnie z art. 19, wynosi nie więcej niż referencyjne wskaźniki oszustw określone w tabeli zamieszczonej w załączniku odpowiednio dla „zdalnych płatności elektronicznych realizowanych w oparciu o kartę" i „zdalnych elektronicznych poleceń przelewu";

b) kwota transakcji nie przekracza odpowiedniej wartości progu wyłączenia określonej w tabeli zamieszczonej w załączniku;

c) po przeprowadzeniu analizy ryzyka w czasie rzeczywistym dostawcy usług płatniczych nie stwierdzili występowania żadnego z następujących elementów:

   (i) niestandardowych wydatków lub niestandardowego wzorca zachowań płatnika;

   (ii) nietypowych informacji na temat dostępu do urządzenia/oprogramowania płatnika;

   (iii) wystąpienia złośliwego oprogramowania w którejkolwiek sesji procesu uwierzytelniania;

   (iv) znanego scenariusza oszustwa w świadczeniu usług płatniczych;

   (v) niestandardowej lokalizacji płatnika;

   (vi) lokalizacji odbiorcy wiążącej się z wysokim ryzykiem.

3. Dostawcy usług płatniczych, którzy mają zamiar objąć elektroniczne zdalne transakcje płatnicze wyłączeniem z obowiązku stosowania silnego uwierzytelniania klienta ze względu na to, iż wiąże się z nimi niski poziom ryzyka, uwzględniają przynajmniej następujące czynniki oparte na analizie ryzyka:

a) poprzednie schematy wydatków indywidualnego użytkownika usług płatniczych;

b) historię transakcji płatniczych każdego użytkownika usług płatniczych danego dostawcy usług płatniczych;

c) lokalizację płatnika i odbiorcy podczas transakcji płatniczej, w przypadku gdy urządzenie lub oprogramowanie dostępowe pochodzi od dostawcy usług płatniczych;

d) identyfikację niestandardowych wzorców płatności użytkownika usług płatniczych w stosunku do historii transakcji płatniczych tego użytkownika.

W ramach oceny dokonywanej przez dostawcę usług płatniczych łączy się wszystkie te czynniki oparte na analizie ryzyka, aby uzyskać punktową ocenę ryzyka dla każdej pojedynczej transakcji w celu określenia, czy konkretną płatność można przeprowadzić bez silnego uwierzytelnienia klienta.

Artykuł 19

Obliczanie wskaźników oszustw

1. Dla każdego rodzaju transakcji, o którym mowa w tabeli zamieszczonej w załączniku, dostawca usług płatniczych zapewnia, aby łączne wskaźniki oszustw obejmujące zarówno transakcje płatnicze uwierzytelnione poprzez silne uwierzytelnianie klienta, jak i te przeprowadzone w ramach wyłączeń, o których mowa w art. 13–18, były nie wyższe niż referencyjny wskaźnik oszustw dla tego samego rodzaju transakcji płatniczej wskazany w tabeli zamieszczonej w załączniku.

Całkowity wskaźnik oszustw dla każdego rodzaju transakcji oblicza się jako całkowitą wartość nieautoryzowanych lub nielegalnych transakcji zdalnych – niezależnie od tego, czy środki odzyskano, czy też nie – podzieloną przez całkowitą wartość wszystkich transakcji zdalnych dla tego samego rodzaju transakcji – niezależnie od tego, czy uwierzytelniono je poprzez zastosowanie silnego uwierzytelniania klienta, czy przeprowadzono je w ramach któregokolwiek z wyłączeń, o których mowa w art. 13–18 – w ujęciu kwartalnym w trybie kroczącym (90 dni).

2. Obliczenia wskaźników oszustw i wynikające z nich dane liczbowe ocenia się w ramach audytu, o którym mowa w art. 3 ust. 2, które zapewnia ich kompletność i dokładność.

3. Metodyka i wszelkie modele, z których dostawca usług płatniczych korzysta do obliczenia wskaźnika oszustw – a także same wskaźniki oszustw – są odpowiednio dokumentowane i w pełni udostępniane właściwym organom i EUNB na ich wniosek po wcześniejszym zawiadomieniu odpowiedniego właściwego organu lub odpowiednich właściwych organów.

Artykuł 20

Zaprzestanie stosowania wyłączeń na podstawie analizy ryzyka transakcji

1. Dostawcy usług płatniczych korzystający z wyłączenia, o którym mowa w art. 18, niezwłocznie zawiadamiają właściwe organy, jeżeli jeden z monitorowanych przez nich wskaźników oszustw dla któregokolwiek z rodzajów transakcji płatniczych określonych w tabeli zamieszczonej w załączniku przekracza odnośny referencyjny wskaźnik oszustw, oraz przedstawiają właściwym organom opis środków, które zamierzają wprowadzić, aby przywrócić zgodność monitorowanego przez nich wskaźnika oszustw z odnośnym referencyjnym wskaźnikiem oszustw.

2. Dostawcy usług płatniczych natychmiast zaprzestają stosowania wyłączenia, o którym mowa w art. 18, w odniesieniu do wszelkiego rodzaju transakcji płatniczych wskazanych w tabeli zamieszczonej w załączniku dla konkretnego przedziału progu wyłączenia, jeżeli monitorowany przez nich wskaźnik oszustw przez dwa następujące po sobie kwartały przekracza referencyjny wskaźnik oszustw mający zastosowanie do danego instrumentu płatniczego lub rodzaju transakcji płatniczej w danym przedziale progu wyłączenia.

3. W następstwie zaprzestania stosowania wyłączenia, o którym mowa w art. 18, zgodnie z ust. 2 niniejszego artykułu dostawcy usług płatniczych nie stosują wyłączenia ponownie do momentu, kiedy obliczony przez nich wskaźnik oszustw nie przekracza referencyjnych wskaźników oszustw mających zastosowanie do danego rodzaju transakcji płatniczej w przedziale progu tego wyłączenia przewidzianym przez okres jednego kwartału.

4. Jeżeli dostawcy usług płatniczych zamierzają ponownie zastosować wyłączenie, o którym mowa w art. 18, zawiadamiają o tym właściwe organy w rozsądnym terminie, a przed ponownym zastosowaniem wyłączenia przedstawiają dowody przywrócenia zgodności monitorowanego przez nich wskaźnika oszustw z odnośnym referencyjnym wskaźnikiem oszustw dla przedziału progu tego wyłączenia zgodnie z ust. 3. niniejszego artykułu.

Artykuł 21

Monitorowanie

1. W celu zastosowania wyłączeń określonych w art. 10–18 dostawcy usług płatniczych co najmniej raz na kwartał dokumentują i monitorują wymienione poniżej dane dla każdego rodzaju transakcji płatniczych, z wyszczególnieniem zdalnych i niezdalnych transakcji płatniczych:

a) całkowitą wartość nieautoryzowanych lub nielegalnych transakcji płatniczych zgodnie z art. 64 ust. 2 dyrektywy (UE) 2015/2366, całkowitą wartość wszystkich transakcji płatniczych i wynikający z nich wskaźnik oszustw z wyszczególnieniem transakcji płatniczych zainicjowanych za pośrednictwem silnego uwierzytelniania klienta i w ramach każdego z wyłączeń;

b) średnią wartość transakcji z wyszczególnieniem transakcji płatniczych zainicjowanych za pośrednictwem silnego uwierzytelniania klienta i w ramach każdego z wyłączeń;

c) liczbę transakcji płatniczych, w stosunku do których zastosowano poszczególne wyłączenia, oraz ich udział procentowy w odniesieniu do całkowitej liczby transakcji płatniczych.

2. Na wniosek właściwych organów i EUNB, po wcześniejszym zawiadomieniu odpowiedniego właściwego organu lub odpowiednich właściwych organów, dostawcy usług płatniczych udostępniają właściwym organom i EUNB wyniki monitorowania przeprowadzonego zgodnie z ust. 1.

ROZDZIAŁ IV

POUFNOŚĆ I INTEGRALNOŚĆ INDYWIDUALNYCH DANYCH UWIERZYTELNIAJĄCYCH UŻYTKOWNIKÓW USŁUG PŁATNICZYCH

Artykuł 22

Wymogi ogólne

1. Dostawcy usług płatniczych zapewniają poufność i integralność indywidualnych danych uwierzytelniających użytkowników usług płatniczych, w tym kodów uwierzytelniających, na wszystkich etapach uwierzytelniania.

2. Do celów ust. 1 dostawcy usług płatniczych zapewniają spełnienie każdego z określonych poniżej wymogów:

a) indywidualne dane uwierzytelniające są maskowane podczas ich wyświetlania i nie można ich w pełni odczytać, kiedy użytkownik usług płatniczych wprowadza je podczas uwierzytelnienia;

b) indywidualnych danych uwierzytelniających w formacie danych oraz materiałów kryptograficznych powiązanych z szyfrowaniem indywidualnych danych uwierzytelniających nie przechowuje się jako zwykłego tekstu;

c) tajny materiał kryptograficzny jest chroniony przed nieautoryzowanym ujawnieniem.

3. Dostawcy usług płatniczych w pełni dokumentują proces związany z zarządzaniem materiałem kryptograficznym wykorzystywanym do szyfrowania indywidualnych danych uwierzytelniających lub uniemożliwiania w inny sposób odczytu tych danych.

4. Dostawcy usług płatniczych zapewniają, aby przetwarzanie i routing indywidualnych danych uwierzytelniających oraz kodów uwierzytelniających wygenerowanych zgodnie z rozdziałem II odbywały się w bezpiecznym środowisku, zgodnie z silnymi i powszechnie uznanymi normami branżowymi.

Artykuł 23

Tworzenie i przesyłanie danych uwierzytelniających

Dostawcy usług płatniczych zapewniają tworzenie indywidualnych danych uwierzytelniających w bezpiecznym środowisku.

Ograniczają oni ryzyko nieuprawnionego wykorzystania indywidualnych danych uwierzytelniających oraz urządzeń uwierzytelniających i oprogramowania uwierzytelniającego w następstwie ich utraty, kradzieży lub skopiowania przed ich dostarczeniem do płatnika.

Artykuł 24

Powiązanie z użytkownikiem usług płatniczych

1. Dostawcy usług płatniczych zapewniają, aby wyłącznie użytkownik usług płatniczych był w bezpieczny sposób powiązany z indywidualnymi danymi uwierzytelniającymi, urządzeniami uwierzytelniającymi i oprogramowaniem uwierzytelniającym.

2. Do celów ust. 1 dostawcy usług płatniczych zapewniają spełnienie każdego z określonych poniżej wymogów:

a) do powiązania tożsamości użytkownika usług płatniczych z indywidualnymi danymi uwierzytelniającymi, urządzeniami uwierzytelniającymi i oprogramowaniem uwierzytelniającym dochodzi w bezpiecznym środowisku, za które odpowiedzialność ponosi dostawca usług płatniczych i do którego zaliczają się co najmniej lokale dostawcy usług płatniczych, środowisko internetowe zapewnione przez dostawcę usług płatniczych lub inne podobne bezpieczne strony internetowe wykorzystywane przez dostawcę usług płatniczych oraz jego bankomaty, a także przy uwzględnieniu ryzyka związanego z urządzeniami i podstawowymi elementami wykorzystanymi podczas procesu powiązania, za które dostawca usług płatniczych nie ponosi odpowiedzialności;

b) powiązanie tożsamości użytkownika usług płatniczych z indywidualnymi danymi uwierzytelniającymi, urządzeniami uwierzytelniającymi lub oprogramowaniem uwierzytelniającym za pomocą kanału zdalnego przeprowadza się z zastosowaniem silnego uwierzytelniania klienta.

Artykuł 25

Dostarczenie danych uwierzytelniających, urządzeń uwierzytelniających i oprogramowania uwierzytelniającego

1. Dostawcy usług płatniczych zapewniają, aby dostarczenie użytkownikowi usług płatniczych indywidualnych danych uwierzytelniających, urządzeń uwierzytelniających i oprogramowania uwierzytelniającego przebiegało w sposób bezpieczny w celu zapobieżenia ryzyku związanemu z ich nieuprawnionym użyciem w następstwie ich utraty, kradzieży lub skopiowania.

2. Do celów ust. 1 dostawcy usług płatniczych stosują co najmniej każdy z następujących środków:

a) skuteczne i bezpieczne mechanizmy dostawy zapewniające dostarczenie indywidualnych danych uwierzytelniających, urządzeń uwierzytelniających i oprogramowania uwierzytelniającego uprawnionemu użytkownikowi usług płatniczych;

b) mechanizmy umożliwiające dostawcy usług płatniczych weryfikację autentyczności oprogramowania uwierzytelniającego dostarczonego użytkownikowi usług płatniczych za pośrednictwem internetu;

c) w przypadku gdy dostarczenie indywidualnych danych uwierzytelniających ma miejsce poza lokalem dostawcy usług płatniczych lub za pośrednictwem kanału zdalnego, rozwiązania zapewniające:

   (i) brak możliwości pozyskania przez osobę niepowołaną więcej niż jednego elementu indywidualnych danych uwierzytelniających, urządzeń uwierzytelniających lub oprogramowania uwierzytelniającego, w przypadku ich dostarczenia za pośrednictwem tego samego kanału;

   (ii) konieczność aktywacji dostarczonych indywidualnych danych uwierzytelniających, urządzeń uwierzytelniających lub oprogramowania uwierzytelniającego przed ich użyciem;

d) rozwiązania zapewniające, aby w przypadku gdy indywidualne dane uwierzytelniające, urządzenia uwierzytelniające lub oprogramowanie uwierzytelniające wymagają aktywacji przed ich pierwszym użyciem, aktywacja miała miejsce w bezpiecznym środowisku i odbywała się zgodnie z procedurami powiązania, o których mowa w art. 24.

Artykuł 26

Odnowienie indywidualnych danych uwierzytelniających

Dostawcy usług płatniczych zapewniają, aby odnowienie lub ponowna aktywacja indywidualnych danych uwierzytelniających przebiegały zgodnie z procedurami tworzenia, powiązania i dostarczenia danych uwierzytelniających i urządzeń uwierzytelniających przewidzianymi w art. 23, 24 i 25.

Artykuł 27

Zniszczenie, dezaktywacja i unieważnienie

Dostawcy usług płatniczych zapewniają wdrożenie skutecznych procesów pozwalających na stosowanie każdego z następujących środków bezpieczeństwa:

a) bezpiecznego zniszczenia, dezaktywacji lub unieważnienia indywidualnych danych uwierzytelniających, urządzeń uwierzytelniających i oprogramowania uwierzytelniającego;

b) jeżeli dostawca usług płatniczych udostępnia urządzenia uwierzytelniające i oprogramowanie uwierzytelniające wielokrotnego użytku, urządzenie lub oprogramowanie przywraca się do stanu umożliwiającego jego bezpieczne ponowne wykorzystanie, a proces ten dokumentuje się i realizuje przed udostępnieniem ich innemu użytkownikowi usług płatniczych;

c) dezaktywacji lub unieważnienia informacji związanych z indywidualnymi danymi uwierzytelniającymi przechowywanych w systemach i bazach danych dostawcy usług płatniczych oraz – w stosownych przypadkach – w publicznych repozytoriach.

ROZDZIAŁ V

WSPÓLNE I BEZPIECZNE OTWARTE STANDARDY KOMUNIKACJI

Sekcja 1

Wymogi ogólne dotyczące komunikacji

Artykuł 28

Wymogi dotyczące identyfikacji

1. Dostawcy usług płatniczych zapewniają bezpieczną identyfikację podczas komunikowania się urządzenia płatnika z urządzeniami odbiorcy akceptującymi płatności elektroniczne, w tym również m.in. z terminalami płatniczymi.

2. Dostawcy usług płatniczych zapewniają skuteczne ograniczanie ryzyka niewłaściwego przekierowania komunikacji do osób niepowołanych w ramach aplikacji mobilnych i innych interfejsów użytkownika usług płatniczych, które oferują usługi płatności elektronicznej.

Artykuł 29

Identyfikowalność

1. Dostawcy usług płatniczych posiadają procesy zapewniające identyfikowalność wszystkich transakcji płatniczych i innych interakcji z użytkownikiem usług płatniczych, z innymi dostawcami usług płatniczych oraz z innymi podmiotami, w tym z akceptantami, w kontekście świadczenia usług płatniczych, zapewniając wiedzę *ex post* na temat wszystkich zdarzeń istotnych z punktu widzenia transakcji elektronicznej na wszystkich poszczególnych etapach.

2. Do celów ust. 1 dostawcy usług płatniczych zapewniają, aby wszelkie sesje komunikacyjne ustanawiane z użytkownikiem usług płatniczych, innymi dostawcami usług płatniczych i innymi podmiotami, w tym z akceptantami, opierały się na:

a) niepowtarzalnym identyfikatorze sesji;

b) mechanizmach bezpieczeństwa umożliwiających szczegółowe rejestrowanie transakcji, w tym numeru transakcji, znaczników czasu i wszystkich istotnych danych związanych z transakcją;

c) znacznikach czasu, które opierają się na ujednoliconym systemie odniesienia czasowego i które są synchronizowane zgodnie z oficjalnym sygnałem czasu.

Sekcja 2

Szczególne wymogi dotyczące wspólnych i bezpiecznych otwartych standardów komunikacji

Artykuł 30

Obowiązki ogólne dotyczące interfejsów dostępowych

1. Dostawcy usług płatniczych prowadzący rachunek, którzy oferują płatnikowi rachunek płatniczy dostępny za pośrednictwem internetu, posiadają co najmniej jeden interfejs spełniający każdy z następujących wymogów:

a) dostawcy świadczący usługę dostępu do informacji o rachunku, dostawcy świadczący usługę inicjowania płatności i dostawcy usług płatniczych wydający instrumenty płatnicze oparte na karcie są w stanie zidentyfikować się wobec dostawcy usług płatniczych prowadzącego rachunek;

b) dostawcy świadczący usługę dostępu do informacji o rachunku są w stanie bezpiecznie komunikować się w celu wystąpienia o informacje i uzyskania informacji na temat jednego wyznaczonego rachunku płatniczego lub większej ich liczby i powiązanych transakcji płatniczych;

c) dostawcy świadczący usługę inicjowania płatności są w stanie bezpiecznie komunikować się w celu zainicjowania zlecenia płatniczego z rachunku płatniczego płatnika i uzyskania wszystkich informacji dotyczących zainicjowania transakcji płatniczej oraz wszystkich informacji dotyczących realizacji transakcji płatniczej, do których dostęp mają dostawcy usług płatniczych prowadzący rachunek.

2. Dla celów uwierzytelnienia użytkownika usług płatniczych interfejs, o którym mowa w ust. 1, umożliwia dostawcom świadczącym usługę dostępu do informacji o rachunku i dostawcom świadczącym usługę inicjowania płatności oparcie się na wszelkich procedurach uwierzytelniania zapewnianych użytkownikowi usług płatniczych przez dostawcę usług płatniczych prowadzącego rachunek.

Interfejs ten spełnia co najmniej wszystkie następujące wymogi:

a) dostawca świadczący usługę inicjowania płatności lub dostawca świadczący usługę dostępu do informacji o rachunku jest w stanie zlecić dostawcy usług płatniczych prowadzącemu rachunek rozpoczęcie uwierzytelniania na podstawie zgody wyrażonej przez użytkownika usług płatniczych;

b) sesje komunikacyjne, w których uczestniczą dostawca usług płatniczych prowadzący rachunek, dostawca świadczący usługę dostępu do informacji o rachunku, dostawca świadczący usługę inicjowania płatności i jakikolwiek zainteresowany użytkownik usług płatniczych, ustanawia się i utrzymuje przez cały czas trwania procesu uwierzytelnienia;

c) zapewniona jest integralność i poufność indywidualnych danych uwierzytelniających i kodów uwierzytelniających przekazywanych przez dostawcę świadczącego usługę inicjowania płatności lub dostawcę świadczącego usługę dostępu do informacji o rachunku lub za pośrednictwem tych dostawców.

3. Dostawcy usług płatniczych prowadzący rachunek zapewniają zgodność swoich interfejsów ze standardami komunikacji publikowanymi przez międzynarodowe lub europejskie organy normalizacyjne.

Dostawcy usług płatniczych prowadzący rachunek zapewniają również dokumentację każdego interfejsu określającą zestaw procedur, protokołów i narzędzi, którego dostawcy świadczący usługę inicjowania płatności, dostawcy świadczący usługę dostępu do informacji o rachunku i dostawcy usług płatniczych wydający instrumenty płatnicze oparte na karcie potrzebują, aby umożliwić współdziałanie ich oprogramowania i aplikacji z systemami dostawców usług płatniczych prowadzących rachunek.

Dostawcy usług płatniczych prowadzący rachunek co najmniej udostępniają nieodpłatnie dokumentację na wniosek posiadających zezwolenie dostawców świadczących usługę inicjowania płatności, dostawców świadczących usługę dostępu do informacji o rachunku i dostawców usług płatniczych wydających instrumenty płatnicze oparte na karcie lub dostawców usług płatniczych, którzy złożyli do swoich właściwych organów wniosek o stosowne zezwolenie, nie później niż sześć miesięcy przed datą rozpoczęcia stosowania, o której mowa w art. 38 ust. 2, lub przed datą docelową wprowadzenia na rynek interfejsu dostępowego, jeżeli data wprowadzenia na rynek jest późniejsza niż data, o której mowa w art. 38 ust. 2, oraz publicznie udostępniają streszczenie tej dokumentacji na swojej stronie internetowej.

4. Oprócz przepisów określonych w ust. 3 dostawcy usług płatniczych prowadzący rachunek zapewniają – z wyjątkiem sytuacji nadzwyczajnych – udostępnienie z wyprzedzeniem wszelkich zmian w specyfikacji technicznej ich interfejsu posiadającym zezwolenie dostawcom świadczącym usługę inicjowania płatności, dostawcom świadczącym usługę dostępu do informacji o rachunku i dostawcom usług płatniczych wydającym instrumenty płatnicze oparte na karcie lub dostawcom usług płatniczych, którzy złożyli do swoich właściwych organów wniosek o stosowne zezwolenie, w jak najszybszym terminie i nie później niż 3 miesiące przed wdrożeniem tych zmian.

Dostawcy usług płatniczych dokumentują sytuacje nadzwyczajne, w których wprowadzono zmiany, i udostępniają tę dokumentację właściwym organom na ich wniosek.

5. Dostawcy usług płatniczych prowadzący rachunek udostępniają środowisko testowe (w tym wsparcie) służące do testowania połączenia i funkcjonalności, aby umożliwić posiadającym zezwolenie dostawcom świadczącym usługę inicjowania płatności, dostawcom usług płatniczych wydającym instrumenty płatnicze oparte na karcie i dostawcom świadczącym usługę dostępu do informacji o rachunku lub dostawcom usług płatniczych, którzy złożyli wniosek o stosowne zezwolenie, przetestowanie ich oprogramowania i aplikacji wykorzystywanych do oferowania usług płatniczych użytkownikom. Przedmiotowe środowisko testowe należy udostępnić nie później niż sześć miesięcy przed datą rozpoczęcia stosowania, o której mowa w art. 38 ust. 2, lub przed datą docelową wprowadzenia na rynek interfejsu dostępowego, jeżeli data wprowadzenia na rynek jest późniejsza niż data, o której mowa w art. 38 ust. 2.

Za pośrednictwem środowiska testowego nie prowadzi się jednak wymiany danych szczególnie chronionych.

6. Właściwe organy zapewniają, by dostawcy usług płatniczych prowadzący rachunek stale przestrzegali obowiązków przewidzianych w przedmiotowych standardach w stosunku do wdrożonego interfejsu lub wdrożonych interfejsów. W przypadku gdy dostawca usług płatniczych prowadzący rachunek nie spełnia wymogów dotyczących interfejsów określonych w przedmiotowych standardach, właściwe organy zapewniają, aby nie doszło do powstania przeszkód i zakłóceń w świadczeniu usług inicjowania płatności i usług dostępu do informacji o rachunku, o ile odpowiedni dostawcy tych usług spełniają warunki określone w art. 33 ust. 5.

Artykuł 31

Warianty interfejsu dostępowego

Dostawcy usług płatniczych prowadzący rachunek ustanawiają interfejs lub interfejsy, o których mowa w art. 30, za pośrednictwem specjalnego interfejsu lub poprzez zezwolenie na korzystanie przez dostawców usług płatniczych, o których mowa w art. 30 ust. 1, z interfejsów stosowanych na potrzeby uwierzytelniania użytkowników usług płatniczych dostawcy usług płatniczych prowadzącego rachunek i komunikacji z tymi użytkownikami.

Artykuł 32

Obowiązki dotyczące specjalnego interfejsu

1. Z zastrzeżeniem spełnienia wymogów określonych w art. 30 i 31 dostawcy usług płatniczych prowadzący rachunek, którzy wprowadzili specjalny interfejs, zapewniają, aby specjalny interfejs stale oferował ten sam poziom dostępności i efektywności – w tym wsparcia – co interfejsy udostępnione użytkownikowi usług płatniczych w celu uzyskania bezpośredniego dostępu do jego rachunku płatniczego w trybie online.

2. Dostawcy usług płatniczych prowadzący rachunek, którzy wprowadzili specjalny interfejs, określają przejrzyste kluczowe wskaźniki efektywności i cele w zakresie gwarantowanego poziomu usług, które powinny być przynajmniej w równym stopniu rygorystyczne – zarówno pod względem dostępności, jak i danych przekazywanych zgodnie z art. 36 – co wskaźniki i cele ustalone w odniesieniu do interfejsu stosowanego przez ich użytkowników usług płatniczych. Przedmiotowe interfejsy, wskaźniki i cele podlegają monitorowaniu i testom warunków skrajnych prowadzonym przez właściwe organy.

3. Dostawcy usług płatniczych prowadzący rachunek, którzy wprowadzili specjalny interfejs, zapewniają, aby interfejs ten nie stwarzał przeszkód w świadczeniu usług inicjowania płatności i usług dostępu do informacji o rachunku. Przeszkody takie mogą obejmować m.in. uniemożliwianie dostawcom usług płatniczych, o których mowa w art. 30 ust. 1, wykorzystywania danych uwierzytelniających wydanych przez dostawców usług płatniczych prowadzących rachunek ich klientom, wymuszanie przekierowania do mechanizmu uwierzytelniania lub innych funkcji dostawcy usług płatniczych prowadzącego rachunek, wymóg uzyskania dodatkowych zezwoleń oraz dodatkowych rejestracji oprócz tych przewidzianych w art. 11, 14 i 15 dyrektywy (UE) 2015/2366 lub wymóg dodatkowej weryfikacji zgody udzielonej dostawcom usług inicjowania płatności i usług dostępu do informacji o rachunku przez użytkowników usług płatniczych.

4. Do celów ust. 1 i 2 dostawcy usług płatniczych prowadzący rachunek monitorują dostępność i efektywność specjalnego interfejsu. Dostawcy usług płatniczych prowadzący rachunek publikują na swojej stronie internetowej kwartalne statystyki dotyczące dostępności i efektywności specjalnego interfejsu oraz interfejsu stosowanego przez użytkowników usług płatniczych korzystających z ich usług.

Artykuł 33

Środki awaryjne w zakresie specjalnego interfejsu

1. Dostawcy usług płatniczych prowadzący rachunek uwzględniają w projekcie specjalnego interfejsu strategię i plany w zakresie środków awaryjnych na wypadek, gdyby interfejs nie działał zgodnie z art. 32, bądź na wypadek nieplanowanej niedostępności interfejsu lub awarii systemów. Przyjmuje się, że występuje nieplanowana niedostępność lub awaria systemów, jeżeli na pięć następujących po sobie żądań dostępu do informacji niezbędnych do świadczenia usług inicjowania płatności lub usług dostępu do informacji o rachunku nie zostanie udzielona odpowiedź w ciągu 30 sekund.

2. Środki awaryjne obejmują plany komunikacji służące poinformowaniu dostawców usług płatniczych korzystających ze specjalnego interfejsu o środkach mających na celu przywrócenie systemu oraz opis natychmiast dostępnych wariantów alternatywnych, z których dostawcy usług płatniczych mogą w tym czasie skorzystać.

3. Zarówno dostawca usług płatniczych prowadzący rachunek, jak i dostawcy usług płatniczych, o których mowa w art. 30 ust. 1, bezzwłocznie zgłaszają problemy ze specjalnym interfejsem swoim odpowiednim właściwym organom krajowym, jak opisano w ust. 1.

4. W ramach mechanizmów awaryjnych dostawcom usług płatniczych, o których mowa w art. 30 ust. 1, umożliwia się – do momentu przywrócenia poziomu dostępności i efektywności specjalnego interfejsu do poziomu określonego w art. 32 – korzystanie z interfejsów udostępnionych użytkownikom usług płatniczych na potrzeby uwierzytelnienia i komunikacji z ich dostawcą usług płatniczych prowadzącym rachunek.

5. W tym celu dostawcy usług płatniczych prowadzący rachunek zapewniają możliwość identyfikacji dostawców usług płatniczych, o których mowa w art. 30 ust. 1, oraz poleganie przez nich na procedurach uwierzytelniania zapewnianych użytkownikowi usług płatniczych przez dostawcę usług płatniczych prowadzącego rachunek. Jeżeli dostawcy usług płatniczych, o których mowa w art. 30 ust. 1 korzystają z interfejsu, o którym mowa w ust. 4, to:

a) wprowadzają niezbędne środki w celu zapewnienia, aby nie mieli oni dostępu do danych, nie przechowywali ani nie przetwarzali ich w celach innych niż świadczenie usług zleconych przez użytkownika usług płatniczych;

b) w dalszym ciągu przestrzegają obowiązków wynikających odpowiednio z art. 66 ust. 3 i art. 67 ust. 2 dyrektywy (UE) 2015/2366;

c) rejestrują dane, do których dostęp uzyskano za pośrednictwem interfejsu prowadzonego przez dostawcę usług płatniczych prowadzącego rachunek na potrzeby swoich użytkowników usług płatniczych, i na wniosek bez zbędnej zwłoki przedstawiają pliki rejestrów właściwemu organowi krajowemu;

d) na wniosek i bez zbędnej zwłoki uzasadniają należycie właściwemu organowi krajowemu korzystanie z interfejsu udostępnionego użytkownikom usług płatniczych w celu bezpośredniego dostępu do rachunku płatniczego w trybie online;

e) odpowiednio informują dostawców usług płatniczych prowadzących rachunek.

6. Właściwe organy – po przeprowadzeniu konsultacji z EUNB w celu zapewnienia spójnego stosowania następujących warunków – obejmują wyłączeniem z obowiązku ustanowienia mechanizmów awaryjnych opisanych w ust. 4 tych dostawców usług płatniczych prowadzących rachunek, którzy zdecydowali się na wprowadzenie specjalnego interfejsu, jeżeli specjalny interfejs spełnia wszystkie następujące warunki:

a) spełnia wszystkie obowiązki dotyczące specjalnych interfejsów określone w art. 32;

b) opracowano i przetestowano go zgodnie z art. 30 ust. 5 w sposób zadowalający dostawców usług płatniczych, o których mowa w przytoczonym artykule;

c) od co najmniej trzech miesięcy jest powszechnie stosowany przez dostawców usług płatniczych w celu świadczenia usług dostępu do informacji o rachunku, usług inicjowania płatności i przedstawiania potwierdzenia dostępności środków pieniężnych w przypadku płatności realizowanych w oparciu o kartę;

d) wszelkie problemy związane ze specjalnym interfejsem rozwiązano bez zbędnej zwłoki.

7. Właściwe organy cofają wyłączenie, o którym mowa w ust. 6, jeżeli dostawcy usług płatniczych prowadzący rachunek nie spełniają warunków określonych w lit. a) i d) przez okres dłuższy niż dwa następujące po sobie tygodnie kalendarzowe. Właściwe organy przekazują EUNB informację o cofnięciu wyłączenia i zapewniają, aby dostawca usług płatniczych prowadzący rachunek ustanowił mechanizmy awaryjne, o których mowa w ust. 4, w najkrótszym możliwym terminie, a najpóźniej w ciągu dwóch miesięcy.

Artykuł 34

Certyfikaty

1. Do celów identyfikacji, o której mowa w art. 30 ust. 1 lit. a), dostawcy usług płatniczych polegają na kwalifikowanych certyfikatach pieczęci elektronicznych, o których mowa w art. 3 pkt 30 rozporządzenia (UE) nr 910/2014, lub na kwalifikowanych certyfikatach uwierzytelniania witryn internetowych, o których mowa w art. 3 pkt 39 tego rozporządzenia.

2. De celu niniejszego rozporządzenia numer rejestrowy, o którym mowa w oficjalnym rejestrze, zgodnie z lit. c) załącznika III lub lit. c) załącznika IV do rozporządzenia (UE) nr 910/2014, jest numerem zezwolenia dostawcy usług płatniczych wydającego instrumenty płatnicze oparte na karcie, dostawców świadczących usługę dostępu do informacji o rachunku i dostawców świadczących usługę inicjowania płatności, w tym dostawców usług płatniczych prowadzących rachunek, którzy świadczą takie usługi, dostępnym w publicznym rejestrze państwa członkowskiego pochodzenia zgodnie z art. 14 dyrektywy (UE) 2015/2366 lub wynikającym z powiadomień o każdym zezwoleniu udzielonym na podstawie art. 8 dyrektywy Parlamentu Europejskiego i Rady 2013/36/UE ([1]) zgodnie z art. 20 tej dyrektywy.

3. Do celów niniejszego rozporządzenia kwalifikowane certyfikaty pieczęci elektronicznych lub kwalifikowane certyfikaty uwierzytelniania witryn internetowych, o których mowa w ust. 1, zawierają – w języku zwyczajowo używanym w dziedzinie finansów – dodatkowe szczególne atrybuty w stosunku do każdego z następujących elementów:

a) roli dostawcy usług płatniczych, która może obejmować jedno z następujących działań lub większą ich liczbę:

   (i) prowadzenie rachunku;

   (ii) inicjowanie płatności;

   (iii) dostęp do informacji o rachunku;

   (iv) wydawanie instrumentów płatniczych opartych na karcie;

b) nazwy właściwych organów, w których dostawca usług płatniczych jest zarejestrowany.

4. Atrybuty, o których mowa w ust. 3, nie wpływają na interoperacyjność i uznawanie kwalifikowanych certyfikatów pieczęci elektronicznych lub kwalifikowanych certyfikatów uwierzytelniania witryn internetowych.

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.U. L 176 z 27.6.2013, s. 338).

Artykuł 35

Bezpieczeństwo sesji komunikacyjnej

1. Dostawcy usług płatniczych prowadzący rachunek, dostawcy usług płatniczych wydający instrumenty płatnicze oparte na karcie, dostawcy świadczący usługę dostępu do informacji o rachunku i dostawcy świadczący usługę inicjowania płatności zapewniają, aby podczas wymiany danych za pośrednictwem internetu w komunikacji między komunikującymi się stronami stosowano bezpieczne szyfrowanie danych przez cały czas trwania odpowiednich sesji komunikacyjnych w celu zabezpieczenia poufności i integralności danych, wykorzystując do tego silne i powszechnie uznawane techniki szyfrowania.

2. Dostawcy usług płatniczych wydający instrumenty płatnicze oparte na karcie, dostawcy świadczący usługę dostępu do informacji o rachunku i dostawcy świadczący usługę inicjowania płatności zapewniają, by oferowane przez dostawców usług płatniczych prowadzących rachunek sesje dostępu były możliwie jak najkrótsze, a także czynnie kończą wszelkie sesje tego rodzaju, gdy tylko żądana czynność zostaje zakończona.

3. W przypadku utrzymywania równoległych sesji sieciowych z dostawcą usług płatniczych prowadzącym rachunek dostawcy świadczący usługę dostępu do informacji o rachunku i dostawcy świadczący usługę inicjowania płatności zapewniają bezpieczne powiązanie tych sesji z odpowiednimi sesjami ustanowionymi z użytkownikiem lub użytkownikami usług płatniczych, aby zapobiec możliwości nieprawidłowego przekierowania jakiejkolwiek wymienianej między nimi wiadomości bądź informacji.

4. Dostawcy świadczący usługę dostępu do informacji o rachunku, dostawcy świadczący usługę inicjowania płatności i dostawcy usług płatniczych wydający instrumenty płatnicze oparte na karcie wraz z dostawcą usług płatniczych prowadzącym rachunek zamieszczają jednoznaczne odwołania do każdej z następujących pozycji:

a) użytkownika lub użytkowników usług płatniczych oraz odpowiadającej im sesji komunikacyjnej, aby rozróżnić między wieloma żądaniami pochodzącymi od tego samego użytkownika lub tych samych użytkowników usług płatniczych;

b) w przypadku usług inicjowania płatności – niepowtarzalnie identyfikowanej transakcji płatniczej, którą zainicjowano;

c) w przypadku potwierdzenia dostępności środków pieniężnych, niepowtarzalnie identyfikowanego żądania związanego z kwotą niezbędną do dokonania transakcji płatniczej realizowanej w oparciu o kartę.

5. Dostawcy usług płatniczych prowadzący rachunek, dostawcy świadczący usługę dostępu do informacji o rachunku, dostawcy świadczący usługę inicjowania płatności i dostawcy usług płatniczych wydający instrumenty płatnicze oparte na karcie podczas przekazywania indywidualnych danych uwierzytelniających i kodów uwierzytelniających zapewniają brak bezpośredniej lub pośredniej możliwości odczytu tych danych przez kogokolwiek z personelu w którymkolwiek momencie.

W przypadku utraty poufności indywidualnych danych uwierzytelniających wchodzących w zakres ich kompetencji dostawcy ci bez zbędnej zwłoki informują o tym użytkownika usług płatniczych powiązanego z tymi danymi oraz wydawcę tych indywidualnych danych uwierzytelniających.

Artykuł 36

Wymiany danych

1. Dostawcy usług płatniczych prowadzący rachunek spełniają każdy z następujących wymogów:

a) przekazują dostawcom świadczącym usługę dostępu do informacji o rachunku te same informacje na temat wyznaczonych rachunków płatniczych i powiązanych transakcji płatniczych, które udostępniają użytkownikowi usług płatniczych, gdy ten bezpośrednio żąda dostępu do informacji o rachunku, pod warunkiem że informacje te nie zawierają szczególnie chronionych danych dotyczących płatności;

b) bezzwłocznie po otrzymaniu zlecenia płatniczego udostępniają oni dostawcom świadczącym usługę inicjowania płatności te same informacje na temat inicjowania i przeprowadzenia transakcji płatniczej, które przekazują lub udostępniają użytkownikowi usług płatniczych, gdy ten bezpośrednio zainicjuje transakcję;

c) na wniosek bezzwłocznie przekazują oni dostawcom usług płatniczych potwierdzenie dostępności na rachunku płatniczym płatnika kwoty koniecznej do przeprowadzenia transakcji płatniczej w prostym formacie „tak” lub „nie”.

2. W przypadku wystąpienia niespodziewanego zdarzenia lub błędu podczas procesu identyfikacji, uwierzytelniania lub wymiany elementów danych przedmiotowy dostawca usług płatniczych prowadzący rachunek wysyła zawiadomienie do dostawcy świadczącego usługę inicjowania płatności lub dostawcy świadczącego usługę dostępu do informacji o rachunku oraz dostawcy usług płatniczych wydającego instrumenty płatnicze oparte na karcie, w którym wyjaśnia przyczynę niespodziewanego zdarzenia lub błędu.

Jeżeli dostawca usług płatniczych prowadzący rachunek oferuje specjalny interfejs zgodnie z art. 32, interfejs ten musi umożliwiać wysyłanie zawiadomień dotyczących niespodziewanych zdarzeń lub błędów przez jakiegokolwiek dostawcę usług płatniczych, który wykryje tego rodzaju zdarzenie lub błąd, do innych dostawców usług płatniczych uczestniczących w sesji komunikacyjnej.

3. Dostawcy świadczący usługę dostępu do informacji o rachunku posiadają odpowiednie i skuteczne mechanizmy, które zapobiegają dostępowi do informacji innych niż dotyczące wyznaczonych rachunków płatniczych i powiązanych transakcji płatniczych, zgodnie z wyraźnie udzieloną zgodą użytkownika.

4. Dostawcy świadczący usługę inicjowania płatności przekazują dostawcom usług płatniczych prowadzącym rachunek te same informacje, których żąda się od użytkownika usług płatniczych, gdy ten bezpośrednio inicjuje transakcję płatniczą.

5. Dostawcy świadczący usługę dostępu do informacji o rachunku mają dostęp do informacji na temat wyznaczonych rachunków płatniczych i powiązanych transakcji płatniczych, które dostawcy usług płatniczych prowadzący rachunek posiadają, na potrzeby świadczenia usług dostępu do informacji o rachunku w następujących sytuacjach:

a) zawsze, gdy użytkownik usług płatniczych czynnie żąda takich informacji;

b) jeżeli użytkownik usług płatniczych nie żąda czynnie takich informacji, nie więcej niż cztery razy w ciągu 24 godzin, chyba że – za zgodą użytkownika usług płatniczych – dostawca świadczący usługę dostępu do informacji o rachunku i dostawca usług płatniczych prowadzący rachunek uzgodnią większą częstotliwość.

ROZDZIAŁ VI

PRZEPISY KOŃCOWE

Artykuł 37

Przegląd

Nie naruszając art. 98 ust. 5 dyrektywy (UE) 2015/2366, do dnia 14 marca 2021 r. EUNB dokonuje przeglądu wskaźników oszustw, o których mowa w załączniku do niniejszego rozporządzenia, oraz wyłączeń przyznanych na podstawie art. 33 ust. 6 w stosunku do specjalnych interfejsów, a także, w stosownych przypadkach, przedkłada Komisji projekty ich aktualizacji zgodnie z art. 10 rozporządzenia (UE) nr 1093/2010.

Artykuł 38

Wejście w życie

1. Niniejsze rozporządzenie wchodzi w życie następnego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

2. Niniejsze rozporządzenie stosuje się od dnia 14 września 2019 r.

3. Przepisy art. 30 ust. 3 i 5 mają jednak zastosowanie od dnia 14 marca 2019 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 27 listopada 2017 r.

W imieniu Komisji

Jean-Claude JUNCKER

Przewodniczący

ZAŁĄCZNIK

	Referencyjny wskaźnik oszustw (%) dotyczący:	
Wartość progu wyłączenia	Zdalnych płatności elektronicznych realizowanych w oparciu o kartę	Zdalnych elektronicznych poleceń przelewu
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015