

Odpowiedzialność dostawców usług płatniczych w przypadku braku stosowania silnego uwierzytelniania użytkownika (SCA)

W artykule analizie została poddana cywilnoprawna i administracyjnoprawna odpowiedzialność dostawców usług płatniczych związana z brakiem stosowania silnego uwierzytelniania użytkownika. W szczególności analiza obejmuje normę wynikającą z art. 46 ust. 4a u.u.p.¹, zgodnie z którą (z wyjątkiem winy umyślnej) płatnik nie odpowiada za nieautoryzowane transakcje płatnicze, kiedy dostawca płatnika nie wymagał silnego uwierzytelniania użytkownika.

MICHAŁ GRABOWSKI

Rozwój techniki umożliwia w coraz szerszym stopniu zdalny dostęp do usług bankowych i do usług określanych pojęciem FinTech. Kluczowym elementem zdalnego dostępu jest zapewnienie użytkownikom bezpieczeństwa korzystania z tych usług. Dotyczy to w szczególności możliwości „przechwycenia” danych dostępowych użytkowników oraz użycia ich do dokonywania oszustw. W celu zapobieżenia takiemu zjawisku ustawodawca unijny wprowadził szereg wymogów co do oferowania klientom zdalnego dostępu do produktów i usług. Na obecnym etapie prym w uregulowaniu wiodą usługi płatnicze, a to dzięki tzw. drugiej dyrektywie o usługach płatniczych (PSD2)² i RTS³. Przepisy te określają sytuacje, w których od dostawcy usług jest wymagane stosowanie tzw. silnego uwierzytelniania użytkownika (ang. *strong customer authentication*, dalej: „SCA”), czyli procedury służącej zabezpieczeniu dostępu i potwierdzeniu tożsamości użytkownika. Dla dostawców ustawodawca przewidział „zachęty” w postaci zwiększonego ryzyka ponoszonego w przypadku zaakceptowania transakcji bez SCA.

¹ Ustawa z 19.08.2011 r. o usługach płatniczych (t.j. Dz.U. z 2020 r., poz. 794), dalej: „u.u.p.”.

² Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z 25.11.2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. UE L nr 337, s. 35), dalej: „PSD2”.

³ Rozporządzenie delegowane Komisji (UE) 2018/389 z 27.11.2017 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 (Dz.U. UE L nr 69, s. 23), dalej: „RTS”.