Warszawa, dnia 12 kwietnia 2018 r.

DL-III-0520-13/18
BM-I-0520-171/18/2

Pani
Maria Koc
Wicemarszałek Senatu
Rzeczypospolitej Polskiej

Szanowna Pani Marszałek,

W odpowiedzi na oświadczenie złożone dnia 15 lutego 2018 r. przez senatora Andrzeja Kobiaka, podczas 56. posiedzenia Senatu RP, dotyczące działań zmierzających do zabezpieczenia klientów bankowości internetowej przed oszustwami, uprzejmie wyjaśniam, co następuje.

Tytułem wstępu należy wskazać, że bankowość elektroniczna (internetowa) to platforma umożliwiająca użytkownikowi – klientowi banku korzystanie z usług oferowanych przez bank, a sama problematyka przestępczości związanej z bankowością internetową jest niezwykle skomplikowana oraz występująca pod różnymi formami tudzież określeniami, np. *hacking* – zachowanie polegające na nieuprawnionym uzyskaniu dostępu do informacji w wyniku przełamania zabezpieczeń, *skimming* - działanie przestępcze polegające na skopiowaniu przy użyciu urządzenia zainstalowanego np. na wlocie kart w bankomacie (tzw. *skimmera*) danych z paska magnetycznego karty płatniczej, co następnie umożliwia zdublowanie takiej karty, *phishing* – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub organizację w celu wyłudzenia określonych informacji (np. danych logowania do bankowości internetowej) lub nakłonienia ofiary do realizacji określonych działań, *sniffing* – przechwytywanie przez nieuprawnione osoby informacji przesyłanych w lokalnych sieciach, a także sieciach WiFi, czy *spoofing* – rozumiany jako podszywanie się pod inny element systemu informatycznego, np. komputer innego użytkownika, w celu wykorzystania go jako narzędzia do dokonywania innych bezprawnych działań, np. do przeprowadzenia ataków na określone strony internetowe.

Al. Ujazdowskie 11, 00-950 Warszawa
tel.: +48 22 52 12 888, www.ms.gov.pl

Rozwój bankowości elektronicznej, w tym dynamicznie rozwijającej się bankowości internetowej, opartej na elektronicznym przetwarzaniu danych, pociąga za sobą wzrost liczby różnorodnych form przestępczej aktywności wymierzonej przeciwko bezpieczeństwu danych, zagrażających bezpieczeństwu finansowemu na rynku usług bankowych, w szczególności bezpieczeństwu środków zgromadzonych na rachunku bankowym, do których dostęp możliwy jest na odległość za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych, takich jak komputer, telefon itp.

Nie ulega wątpliwości, że skala zagrożeń przestępczością w bankowości elektronicznej będzie wciąż rosła wraz z nieuniknionym, dalszym rozpowszechnianiem się usług bankowości elektronicznej, m.in. ze względu na coraz łatwiejszy do nich dostęp oraz atrakcyjność tych usług polegającą na wygodnym, niewymagającym osobistego udania się do banku, dostępie do środków zgromadzonych na rachunku bankowym, praktycznie nieograniczonym co do miejsca i czasu.

Nie można pominąć faktu, że na rozmiar przestępczości w elektronicznym obrocie bankowym ma również wpływ zachowanie indywidualnych uczestników rynku finansowego, którzy nie zawsze w dostatecznym stopniu są świadomi istniejących zagrożeń. Często nie posiadają też wiedzy o tym, jak mogą się przed nimi bronić. Przestrzeganie bowiem podstawowych zasad bezpieczeństwa finansowego w bankowości elektronicznej jest w stanie zapewnić w znacznym stopniu skuteczną ochronę przed zagrożeniami związanymi z korzystaniem przez klientów banków z usług bankowości elektronicznej i obniżyć prawdopodobieństwo stania się ofiarą nadużyć dokonywanych w elektronicznym obrocie bankowym.

Warto w tym miejscu zwrócić uwagę na trudności dowodowe związane z procesem pozyskiwania i zabezpieczania dowodów elektronicznych w celu zapewnienia możliwości wykorzystania ich jako pełnowartościowych dowodów w postępowaniu przed sądem, wymagające uwzględnienia specyficznych właściwości tych dowodów, które wymuszają stosowanie odmiennych niż w przypadku tradycyjnych przestępstw zasad gromadzenia materiału dowodowego, opartych na fachowości i specjalistycznej wiedzy osób uczestniczących w czynnościach procesowych, w toku których dochodzi do zabezpieczenia śladów dowodowych w postaci elektronicznej.

Na gruncie polskiego ustawodawstwa karnego przestępstwa związane z bankowością elektroniczną nie stanowią odrębnej kategorii czynów karalnych. Brak jest także odrębnego rozdziału w kodeksie karnym, który byłby poświęcony tylko tego rodzaju przestępstwom. Nie oznacza to, że przestępcze formy zachowania związane z wykorzystaniem

w elektronicznym obrocie bankowym nowoczesnych technologii teleinformatycznych opartych na przesyłaniu danych elektronicznych, pozostają poza zakresem penalizacji na gruncie polskiego prawa karnego, i że sprawcy tych czynów nie poniosą odpowiedzialności karnej. Trzeba w tym miejscu również zaznaczyć, że wykorzystanie na rynku usług bankowości elektronicznej wspomnianych wyżej technologii, w tym sieci Internet oznacza, że przestępstwa popełniane w elektronicznym obrocie bankowym wpisują się w szeroki nurt przestępczej aktywności zwanej cyberprzestępczością.

W polskim ustawodawstwie karnym brak jest definicji legalnej pojęcia cyberprzestępczość. W jej ustaleniu może natomiast okazać się pomocna analiza treści preambuły zawartej w Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. (Dz. U. z 2015 poz. 728), której stroną jest również Polska. Na marginesie należy jedynie dodać, że w celu implementowania do prawa polskiego przepisów Konwencji o cyberprzestępczości znowelizowane zostały odnośne przepisy ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2017 r. poz. 2204, z późn. zm., dalej jako: k.k.), w tym w szczególności zawarte w rozdziale XXXIII k.k. zatytułowanym *Przestępstwa przeciwko ochronie informacji*. We wspomnianej preambule czytamy m.in., że celem Konwencji jest powstrzymanie działań skierowanych przeciwko poufności, integralności i dostępności systemów informatycznych, sieci i danych informatycznych, jak również nieprawidłowemu wykorzystywaniu tych systemów, sieci i danych, poprzez uznanie takiego postępowania za przestępstwo. Przez określenie cyberprzestępczość należy zatem najogólniej rozumieć czyny zabronione pod groźbą kary przez ustawę dokonywane przeciwko bezpieczeństwu systemów informatycznych, sieci, elektronicznie przetwarzanych danych, jak również przy użyciu tych systemów, sieci i danych. Uwzględniając powyższe uwagi, należy stwierdzić, że przestępstwa związane z bankowością elektroniczną będą realizowały przede wszystkim znamiona ustawowe ogólnych typów czynów zabronionych określonych w przepisach części szczególnej kodeksu karnego, w szczególności w rozdziale XXXIII. Zachowanie sprawcy może także wypełniać ustawowe znamiona innych czynów zabronionych stypizowanych w przepisach zawartych m.in. w rozdziale XXIII k.k. zatytułowanym *Przestępstwa przeciwko wolności* np. w art. 190 a § 2 k.k., czy też w rozdziale XXXV k.k. zatytułowanym *Przestępstwa przeciwko mieniu* np. w art. 287 k.k. (oszustwo komputerowe). Należy zauważyć, że katalog czynów zabronionych popełnianych w bankowości elektronicznej nie ogranicza się do przestępstw kodeksowych, bowiem odpowiedzialność karna może wynikać również z ustaw szczególnych, np. jeżeli w związku z elektronicznym przetwarzaniem danych w obrocie bankowym dojdzie do naruszenia ustawowo chronionej tajemnicy np. tajemnicy

bankowej, zastosowanie znajdzie art. 171 ust. 5 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2017 r. poz. 1876, z poźn. zm.) przewidujący odpowiedzialność karną za nieuprawnione ujawnienie lub wykorzystanie informacji stanowiących tajemnicę bankową.

Reasumując powyższe, w aktualnym systemie karnoprawnym, w odniesieniu do bankowości elektronicznej, przestępstwa z nią związane zostały stypizowane w części szczególnej kodeksu karnego w art. 267 k.k. (bezprawne uzyskanie informacji), art. 268 § 1 i § 2 k.k. (utrudnianie zapoznania się z informacją osobie uprawnionej, niszczenie informacji), art. 268a § 1 k.k. (niszczenie, uszkadzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych), art. 286 § 1 k.k (oszustwo), art. 287 § 1 k.k. (oszustwo komputerowe) oraz art. 190 a § 2 k.k. (podszywanie się pod inną osobę, wykorzystując jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej).

Odpowiadając już w sposób bezpośredni na oświadczenie senatora Andrzeja Kobiaka, pragnąłbym poinformować, że w Ministerstwie Sprawiedliwości trwają obecnie prace koncepcyjno-analityczne nad nowym brzmieniem poszczególnych przepisów kodeksu karnego, w tym m.in. mających za zadanie chronić klientów bankowości internetowej i osób korzystających z bankowości mobilnej. Powyżej zakreślona zmiana miałaby polegać na tym, że osoba, która dokonałaby transakcji płatniczej przy użyciu pieniądza elektronicznego bez zgody osoby uprawnionej do dysponowania tym pieniądzem, podlegać będzie karze pozbawienia wolności od roku do lat 10. Jeżeli zaś ten czyn zostałby popełniony na szkodę osoby najbliższej, ściganie następowałoby na wniosek pokrzywdzonego.

z upoważnienia
MINISTRA SPRAWIEDLIWOŚCI

Marcin Warchoł
PODSEKRETARZ STANU