Sygn. akt VI ACa 509/17

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 30 sierpnia 2018 r.

Sąd Apelacyjny w Warszawie VI Wydział Cywilny w składzie:

Przewodniczący - Sędzia - SA Grażyna Kramarska

Sędziowie: - SA Małgorzata Kuracka (spr.)

- SA Krzysztof Tucharz

Protokolant: - Olga Kamińska

po rozpoznaniu w dniu 30 sierpnia 2018 r. w Warszawie

na rozprawie sprawy

z powództwa A. K.

przeciwko (...) Bank (...) S.A. w W.

o zapłatę

na skutek apelacji powoda

od wyroku Sądu Okręgowego w Warszawie

z dnia 9 stycznia 2017 r.

sygn. akt III C 918/15

I. oddala apelację,

II. zasądza od A. K. na rzecz (...) Bank (...) S.A. w W. kwotę 4050,00 zł (cztery tysiące pięćdziesiąt złotych) tytułem zwrotu kosztów postępowania apelacyjnego.

VI ACa 509/17

UZASADNIENIE

Wyrokiem z dnia 9 stycznia 2017r., wydanym w sprawie z powództwa A. K. przeciwko pozwanemu (...) Bank (...) S.A. w W. o zapłatę Sąd Okręgowy w Warszawie oddalił powództwo i orzekł stosownie do tego o kosztach procesu.

Rozstrzygnięcie Sądu zapadło na podstawie następujących ustaleń i rozważań.

A. K. jest klientem (...) S.A. w W. (dalej: (...) S.A.) i posiada w tym banku dwa rachunki bankowe, tj. indywidualny o numerze (...) oraz firmowy o numerze (...). (dowód: okoliczności bezsporne)

A. K. zawarł w dniu 22 marca 2006 r. (...) S.A. umowę rachunku oszczędnościowo-rozliczeniowego (...), na mocy której bank zobowiązał się do otwarcia i prowadzenia rachunku oszczędnościowo-rozliczeniowego o numerze (...) na rzecz posiadacza rachunku oraz świadczenia na rzecz posiadacza rachunku kompleksowej indywidualnej obsługi w ramach programu bankowości prywatnej (...) i zapewnienia najwyższej staranności w realizacji wszelkich spraw

posiadacza rachunku wynikających ze współpracy z (...) S.A. (§ 1 umowy). Z tytułu prowadzenia kompleksowej obsługi w ramach pakietu (...) bank był uprawniony do pobierania od posiadacza miesięczną opłatę tzw. „opłatę pakietową", która obejmowała (§ 9 ust. 1 umowy) oraz prowizje oraz opłaty w wysokości określonej w Taryfie prowizji i opłat bankowych w (...) SA w części, w której usługi nie są objęte opłatą pakietową (§ 10 ust. 1 umowy). Za realizację wysokokwotowych zleceń na rachunki prowadzone w innych niż (...) S.A. bankach za pośrednictwem systemu (...) w kwocie niższej niż 1 mln zł (...) S.A. w dniu zawarcia umowy pobierał opłatę w kwocie 35 zł.

W dniu 30 czerwca 2011 r. strony zmieniły powyższą umowę na umowę rachunku oszczędnościowo-rozliczeniowego Konto (...), usług bankowości elektronicznej oraz karty debetowej bez (...). A. K. przypisano numer klienta (...). Bank został upoważniony do pobierania prowizji i opłat bankowych za świadczenie usług, w tym prowadzenie rachunku, zgodnie z Taryfą prowizji i opłat bankowych w (...) Banku (...) SA (§8 ust. 1). Posiadacz uzyskał dostęp w ramach usług bankowości elektronicznej (...) Bank (...) SA do swoich rachunków i korzystania z usług bankowości elektronicznej, na zasadach określonych w umowie i Regulaminie (§ 1 pkt 3 umowy). W Regulaminie świadczenia usług bankowości elektronicznej w (...) Banku (...) SA wydanym w 2015 r. określono m.in. zasady składania dyspozycji za pośrednictwem elektronicznych kanałów dostępu oraz bezpiecznego dostępu do systemu. Określono dostęp do usługi bankowości elektronicznej za pośrednictwem strony internetowej (...) który uzależniono od posiadania przez użytkownika - klienta urządzeń oprogramowania spełniającego wymagania techniczne, które (...) Bank (...) S.A. podaje do wiadomości klientów na stronie internetowej oraz w serwisie telefonicznym (§ 3 Regulaminu). Bank ustalił zasady autoryzacji zleceń w serwisie internetowym wskazując, że uznaje dyspozycję za autoryzowaną z chwilą jej potwierdzenia odpowiednio przez składającego dyspozycje klienta albo ustanowionego użytkownika (§ 9 ust. 2 Regulaminu). Klient został uprawniony do składania dyspozycji za pośrednictwem elektronicznych kanałów dostępu przez całą dobę z wyłączeniem okresu przerw niezbędnych do konserwacji, napraw technicznych lub przywrócenia poprawności funkcjonowania elektronicznych kanałów dostępu (§ 10 Regulaminu). Na mocy § 12 Regulaminu klient został zobowiązany do logowania oraz wykonywania dyspozycji za pośrednictwem elektronicznych kanałów dostępu wyłącznie osobiście z użyciem instrumentów uwierzytelniających oraz do zachowania w tajemnicy informacji zapewniających bezpieczne korzystania z usług bankowości elektronicznej, w tym informacji przekazywanych bankowi dla celów weryfikacji oraz nieudostępniania i nieujawniania innym osobom instrumentów uwierzytelniających (tj. rozwiązań technologicznych lub danych służących do powiązania danej dyspozycji ze składającym ją klientem lub działającym w jego imieniu użytkownikiem w elektronicznych kanałach dostępu) (§ 12 ust. 1 i 2). Klient został zobowiązany do należytego zabezpieczenia urządzeń i oprogramowania, którymi posługuje się w celu korzystania z usług bankowości elektronicznej poprzez stosowanie wyłącznie legalnego oprogramowania, jego bieżącej aktualizacji i instalacji poprawek systemowych zgodnie z zaleceniami producentów, aktualnego oprogramowania antywirusowego i antyspamowego oraz zapory firewall, najnowszych wersji przeglądarek internetowych, haseł zabezpieczających przed nieuprawnionym dostępem do komputera osób trzecich (§ 12 ust. 3). Szczegółowy opis środków, jakie powinien przedsięwziąć klient w celu zapewnienia bezpieczeństwa dostępu do usług bankowości elektronicznej podawany jest do wiadomości klientów i użytkowników na stronie internetowej oraz w serwisie telefonicznym (§ 12 ust. 4). W § 13 ust. 1 Regulaminu zobowiązano klienta do niezwłocznego zgłoszenia utraty, kradzieży, przywłaszczenia, nieuprawnionego użycia albo zniszczenia instrumentów uwierzytelniających bądź nieuprawnionego dostępu do usług bankowości elektronicznej. Na wypadek wystąpienia nieautoryzowanych transakcji płatniczych, w § 14 Regulaminu ustalono, że (...) S.A. jest obowiązany niezwłocznie zwrócić klientowi kwotę nieautoryzowanej transakcji płatniczej albo przywrócić rachunek klienta do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza, chyba że klient uchybił terminowi zgłoszenia, tj. bez zbędnej zwłoki, nie później niż w terminie 13 miesięcy od dnia realizacji transakcji płatniczej albo do dnia, w którym niewykonana transakcja płatnicza miała być zrealizowana. Klienta obciążają jednak w pełnej wysokości nieautoryzowane transakcje płatnicze, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia, co najmniej jednego z obowiązków określonych w § 12 ust. 1 -3 oraz § 13 ust. 1. Od momentu zgłoszenia dokonanego przez klienta (...) SA przejmuje odpowiedzialność za zobowiązania finansowe powstałe w wyniku nieautoryzowanych transakcji płatniczych, chyba że klient doprowadził do nich umyślnie (§ 14 ust. 5 Regulaminu). Odpowiedzialność banku obejmuje również opłaty i prowizje, którymi

został obciążony klient w rezultacie niewykonania lub nienależytego wykonania transakcji płatniczej (§ 14 ust. 6 Regulaminu).

Powód miał dostęp do platformy bankowości elektronicznej niezmiennie od maja 2015 r. poprzez stronę internetową banku. Prawidłowość certyfikatu bezpieczeństwa jest weryfikowalna na podstawie ikony zamkniętej kłódki w pasku adresu strony internetowej. (...) S.A. W bankowości elektronicznej pozwany stosuje system dwustopniowej autoryzacji dostępu do konta. System bankowy przy logowaniu wymaga podania poprawnego numeru klienta i odpowiadającego mu hasła ustalanego przez klienta, a następnie przed ostatecznym zatwierdzeniem zlecenia płatności w trybie przelewu jednorazowego, podania kodu autoryzacyjnego z karty kodów jednorazowych wydawanej klientowi lub wysłanego klientowi wiadomością sms na wskazany numer telefonu kodu jednorazowego lub tokena generowanego w formie aplikacji lub specjalnego urządzenia. Wybór formy autoryzacji kodem należy do klienta, wszystkie formy są równie bezpieczne, o ile stosowane są zgodnie z procedurą bezpiecznego korzystania z bankowości elektronicznej. Klient może zdefiniować nowy szablon odbiorcy, wskazując jego numer rachunku oraz dane, przez co z góry autoryzuje zlecenia płatności na jego rzecz. Autoryzacja za pomocą kodów nie jest wymagana dla przelewów wewnętrznych między rachunkami tego samego klienta korzystającego z jednego numeru klienta w banku. Bank oferował klientom funkcję powiadomień sms o dokonywanych transakcjach.

(...) S.A. od kwietnia 2015 r. na stronie internetowej podaje komunikat o braku wymogu podawania kodu z narzędzia autoryzacyjnego podczas logowania na platformę bankowości elektronicznej. Komunikat pojawił się po atakach typu malware i phishing na klientów banku.

Powód A. K. w maju 2015 roku korzystał z jednego konta klienta w systemie bankowości elektronicznej, w ramach którego obsługiwane były jego dwa rachunki bankowe – indywidualny i firmowy. Od 2014 roku autoryzacja dyspozycji dokonywanych przez pozwanego za pośrednictwem platformy bankowości elektronicznej z konta osobistego odbywała się poprzez kody sms wysyłane na numer telefonu (...). Powód nie miał ustanowionego alertu sms o dokonywanych na jego koncie transakcjach. Każdego dnia z rana otrzymywał wiadomość sms z banku z saldem konta.

A. K. korzystając z bankowości elektronicznej w maju 2015 roku posługiwał się telefonem komórkowym marki (...) wyposażonym w zabezpieczenia uniemożliwiające dostęp do niego osobom nieuprawnionym oraz innym sprzętem komputerowym. Powód sprzedał komputer i tablet na których także korzystał z bankowości internetowej pozwanego w sierpniu 2015 roku.

Na rachunkach bankowych przypisanych do A. K. w banku (...) S.A. odnotowywano miesięczny obrót sięgający kwoty ok. 8 mln zł, a dzienne dyspozycje przelewów przekraczały łączną kwotę 20.000 zł. W dniu 26 maja 2015 r. o godz. 12:23 oraz o godz. 12:25 A. K. autoryzował dwa przelewy z konta indywidualnego na kwoty po 16.644,84 zł.

W dniu 28 maja 2015 r. z rachunku bankowego A. K. o nr (...) w banku (...) S.A. nieustalony sprawca (sprawcy) złożyli dyspozycje przelewów natychmiastowych (...) w kwotach 19.570 zł, 17.000 zł, 19.800 zł, 19.915 zł, 19.100 zł, 24.000 zł, 18.000 zł (łącznie siedem przelewów na kwotę 137.285 zł) na rachunek bankowy o numerze (...) ze wskazaniem jako odbiorcy P. O.. Przelewy zostały dokonane podczas kilku logowań.

O godz. 10:11 nieznany sprawca zalogował się do systemu za pośrednictwem urządzenia o adresie (...) przynależnym do A. K. i złożył dyspozycję utworzenia nowego szablonu odbiorcy z konta A. K. na rzecz rachunku o numerze (...) z nazwą odbiorcy P. O.. A. K. o godz. 10:12 otrzymał wiadomość sms nr 1 z kodem do autoryzacji utworzenia nowego szablonu płatności, nie zwrócił na niego uwagi uznając, iż jest to sms ze saldem konta. Nie wykorzystał otrzymanego kodu do autoryzacji odbiorcy zdefiniowanego. Nikomu nie udostępniał wiadomości sms w celu utworzenia odbiorcy zdefiniowanego, jednak kod został wykorzystany.

Z tego samego adresu IP A. K. o godz. 10:35 zalogował się do systemu bankowości elektronicznej i złożył dyspozycję przelewu kwoty 18.900 zł na rachunek o numerze (...) tytułem „Zakup waluty symbol: (...)". Powód autoryzował

transakcję wpisując kod SMS nr 2 otrzymany na wskazany numer telefonu. Podczas korzystania z platformy bankowości elektronicznej komputer A. K. nie pokazywał komunikatów o zainfekowaniu systemu wirusem.

W okresie pomiędzy otrzymaniem pierwszej i drugiej wiadomości sms z banku zawierających kody autoryzacyjne, tj. o godz. 10:16, 10:19 i 10:22 A. K. wykonał trzy połączenia telefoniczne z wykorzystaniem numeru telefonu (...), co świadczy o tym, iż powód praktycznie nie rozstawał się telefonem.

O godz. 13:02:52 nieustalona osoba złożyła dyspozycję realizacji przelewu na kwotę 19.570 zł, zatytułowanego (...), na rzecz zdefiniowanego odbiorcy, za pośrednictwem urządzenia o adresie IP (...).

Następnie z urządzenia posiadającego adres IP (...), w sesjach rozpoczętych kolejno o godz. 14:04:01, godz. 14:35:22 oraz godz. 14:35:22 złożono dyspozycje przelewów na kwoty 19.800 zł o tytule (...), 19.100 zł o tytule (...), 19.915 zł o tytule (...), 24.000 zł o tytule (...) oraz 18.000 zł o tytule (...).

O godz. 14:38 (...) S.A. wysłał na numer telefonu komórkowego A. K. sms z kodem do autoryzacji przelewu na kwotę 19.915 zł na rachunek o numerze (...).. (...). Transakcja nie została zrealizowana wobec nieautoryzowania jej kodem. Zlecenie na tę kwotę ponowiono o godz. 14:39 i zostało zrealizowane na podstawie wcześniej zdefiniowanego szablonu odbiorcy.

Spod wskazanego adresu IP (...) logowano się do systemu również o godz. 15:10:36, podczas którego zrealizowano przelew między rachunkami A. K., tj. z rachunku o numerze (...) na rachunek o numerze (...) na kwotę 16.000 zł. Transakcję zrealizowano o godz. 15:26 bez użycia kodu autoryzacyjnego. Podczas tej sesji złożono również dyspozycję przelewu o tytule (...) na kwotę 17.000 zł na rachunek zdefiniowanego odbiorcy P. O..

(...) S.A. za dokonanie przelewów pobrał 7 opłat prowizyjnych po 40 zł.

Wszystkie środki finansowe z rachunku powoda zostały przekazane na rachunek zdefiniowanego odbiorcy P. O. w ciągu kilku minut od złożenia zleceń płatności w trybie przelewu natychmiastowego (...).

Podczas logowań w dniu 28 maja 2015 r. do konta A. K. w bankowości elektronicznej (...) nie doszło do przełamania zabezpieczeń systemu bankowego, zaś procedura autoryzacji przelewów z rachunku powoda na nowo zdefiniowany rachunek odbiorcy P. O., została przeprowadzona w sposób zgodny z obowiązującymi w Banku procedurami.

Wieczorem 28 maja 2015 roku, powód A. K., podczas codziennej weryfikacji stanu konta zorientował się o utracie środków pieniężnych z rachunków bankowych, po czym telefonicznie za pośrednictwem infolinii (...) S.A. oraz doradcy klienta indywidualnego J. K. złożył reklamację o nieautoryzowanych dyspozycjach z jego rachunku bankowego na łączną kwotę 137.285 zł. O godz. 21:25 złożył zawiadomienie o podejrzeniu popełnienia przestępstwa kradzieży w Komendzie Rejonowej (...). Reklamację ponowił osobiście udając się do oddziału banku w dniu 29 maja 2015 r.

Zawiadomienie o podejrzeniu popełnienia przestępstwa na szkodę A. K. złożył również bank (...) S.A.

Pismem z dnia 31 lipca 2015 r. (...) S.A. zawiadomił A. K. o nieuwzględnieniu reklamacji wskazując, że zlecenia płatności zostały złożone po poprawnym zalogowaniu w serwisie (...) numerem klienta oraz hasłem dostępu przynależnym do niego. Bank uznał, że klient logując się do konta korzystał ze zainfekowanej stacji roboczej.

W dniu 31 maja 2016 r. do Sądu Rejonowego Warszawa Praga Południe w Warszawie został skierowany akt oskarżenia przeciwko P. O., którym oskarżono go o to, że w okresie od dnia 11 maja 2015 r. do dnia 28 maja 2015 r. w W. działając wspólnie i w porozumieniu z innymi nieustalonymi osobami, w celu osiągniecia korzyści majątkowej, bez uprawnienia, po uprzednim przełamaniu elektronicznych zabezpieczeń prowadzonego przez bank (...) S.A. rachunku bankowego nr (...) na rzecz A. K. uzyskał nie przeznaczoną dla niego informację odnośnie stanu salda, a następnie zmienił zapis danych informatycznych w elektronicznym systemie bankowych w ten sposób, że z rachunku pokrzywdzonego A. K. dokonał niżej wymienionych transakcji-przelewów: kwoty 19.570 zł w dniu 28 maja 2015 r., kwoty 19.800 zł w dniu

28 maja 2015 r., kwoty 19.100 zł w dniu 28 maja 2015 r., kwoty 19.915 zł w dniu 28 maja 2015 r., kwoty 24.000 zł w dniu 28 maja 2015 r., kwoty 18.000 zł w dniu 28 maja 2015 r., kwoty 17.000 zł w dniu 28 maja 2015 r., tj. sumy 137.385 zł, którą to następnie kwotę przelał na założony przez siebie w dniu 11 maja 2015 r. w Oddziale Banku (...) w W. rachunek bankowy nr (...) na dane (...) P. O., po czym w dniu 28 maja 2015 r. dokonał wypłaty tych środków pieniężnych, działając tym na szkodę A. K. i Banku (...) S.A. z siedzibą w W., przy czym czynu tego dopuścił się w ciągu 5 lat po odbyciu co najmniej 6 miesięcy kary pozbawienia wolności za podobne przestępstwo umyślne, tj. o czyn z art. 278 § 1 kk w zw z art. 64 § 1 kk.

W rozważaniach prawnych Sąd Okręgowy naświetlił stan prawny wskazując, iż w niniejszej sprawie podstawy odpowiedzialności wynikające z wykonania zawartej między stronami postępowania umowy rachunku oszczędnościowo-rozliczeniowego Konto (...), usług bankowości elektronicznej oraz karty debetowej bez (...) z dnia 20 czerwca 2011 r. regulują przepisy ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (dalej: uup), które wyznaczają minimalny standard praw i obowiązków stron umowy o usługę płatniczą.

Zgodnie z art. 42 uup użytkownik, w niniejszej sprawie powód, korzystając z instrumentu płatniczego zobowiązany jest do korzystania z instrumentu płatniczego zgodnie z umową ramową (ust. 1 pkt 1) poprzez podejmowanie niezbędnych środków służących zapobieżeniu naruszenia indywidualnych zabezpieczeń tego instrumentu, w szczególności do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go innym osobom (ust. 2) oraz do zgłaszania niezwłocznego dostawcy – w niniejszej sprawie pozwanemu bankowi, lub podmiotowy wskazanemu przez dostawcę stwierdzenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego do tego instrumentu (ust. 1 pkt 2).

Dostawca zaś zobowiązany jest m. in. zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu (art. 43 ust. 1 pkt 1 uup) oraz uniemożliwienia korzystania z instrumentu płatniczego po dokonaniu zgłoszenia zgodnie z art. 42 ust. 1 pkt 2 (art. 43 ust. 1 pkt 5 uup). Na mocy art. 43 ust. 2 uup dostawcę obciąża ryzyko związane z wysłaniem płatnikowi instrumentu płatniczego lub jego indywidualnych zabezpieczeń.

Dostawca jest zobowiązany do niezwłocznego zwrotu płatnikowi kwoty nieautoryzowanej transakcji płatniczej, o ile transakcja była nieautoryzowana i jest skutkiem: 1) posłużenia się utraconym przez płatnika albo skradzionym płatnikowi instrumentem płatniczym lub 2) przywłaszczenia instrumentu płatniczego lub jego nieuprawnionego użycia w wyniku naruszenia przez płatnika obowiązku, o którym mowa w art. 42 ust. 2. (art. 46 ust. 1 uup).

Ustawodawca w art. 46 ust. 3 uup wskazuje natomiast, że płatnik odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 w/w ustawy.

Zgodnie z art. 50 § 2 prawa bankowego bank dokłada szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. Przepis art. 50 ust 2 ustawy z dnia 29 sierpnia 1997 r. prawa bankowego i art. 355 § 2 kc mają charakter norm imperatywnych, bezwzględnie obowiązujących. Stworzone zostały przez ustawodawcę w celu wspierania i ochrony strony słabszej, jaką wobec profesjonalisty, którym jest bank, pozostaje jego kontrahent - posiadacz rachunku bankowego. Od banku wymaga się bowiem należytej staranności w wykonaniu zobowiązania wynikającego z zawieranych z klientami banku umów prowadzenia rachunku.

W ocenie Sądu pozwany prawidłowo wywiązał się z nałożonych na niego obowiązków nieudostępniania innym osobom niż powód zabezpieczeń instrumentu płatniczego. Z opinii biegłego z zakresu informatyki i teleinformatyki jak również z zeznań świadków – pracowników pozwanego banku wynika, iż nie doszło do przełamania żadnych zabezpieczeń banku. Logowania do konta powoda w systemie bankowości elektronicznej odbywało się z wykorzystaniem jego osobistego numeru klienta oraz ustanowionego przez niego hasła. System bankowy odczytywał próby logowania na konto jako działanie uprawnionego użytkownika – powoda. Powód zaś mimo realnej możliwości niemalże natychmiastowego zgłoszenia bezprawnych działań skierowanych wobec przynależnych do niego rachunków bankowych, nie wykazał dbałości o własne życiowe sprawy i dopiero wieczorem złożył reklamację. Powód,

reprezentowany przez profesjonalnego pełnomocnika, nie wykazywał inicjatywy dowodowej zmierzającej do obalenia twierdzeń świadków, nie kwestionował również opinii biegłego w tym zakresie. Nie zgłaszał również wniosków dowodowych zmierzających do wykazania niepoprawności działania systemu bankowego.

W toku całego procesu nie doszło do wykazania przez powoda zgodnie z obciążającym go ciężarem dowodu, iż można przypisać pozwanemu działania umyślne lub będące skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków o których mowa w art.42 ustawy o usługach płatniczych (art.46 ust.3 ustawy o usługach płatniczych).

W ocenie Sądu nie można także przypisać pozwanemu odpowiedzialności na takiej podstawie, iż nie doszło do automatycznego zablokowania dostępu do instrumentu płatniczego po autoryzacji utworzenia zdefiniowanego odbiorcy, skorzystaniu z funkcji przelewu natychmiastowego (...), a następnie również po wykonaniu pierwszych dwóch transakcji, których ogólna wartość przekroczyła kwotę 20.000 zł. Fakt, iż powód wcześniej nie korzystał z funkcji zdefiniowanego odbiorcy oraz przelewów natychmiastowych, nie może stanowić podstawy dla systemu, w razie z niej skorzystania, że dostęp do instrumentu płatniczego uzyskała osoba nieuprawniona. Nie można bowiem oczekiwać od pozwanego, że wykorzystanie przez klienta nowo wprowadzonych funkcjonalności takich jak możliwość tworzenia zdefiniowanych odbiorców czy przelewy (...) będzie jednocześnie podstawą do zablokowania dostępu do systemu bankowości elektronicznej. Bank nie narzuca bowiem klientom obowiązku korzystania ze wszystkich narzędzi systemowych, pozostawia mu swobodę decydowania z jakich rozwiązań korzysta. Odnosząc się zaś do przekroczenia progu 20.000 zł w dwóch transakcjach, zdaniem Sądu, złożenie zleceń przelewów na kwoty przewyższające wskazany próg nie stanowiło nietypowego działania w ramach konta powoda w bankowości elektronicznej. Sam powód przyznał, iż miesięcznie obracał na swoich rachunkach kwotami kilkumilionowymi, biegły z zakresu informatyki i teleinformatyki odczytał zaś, że np. powód na dwa dni przed utratą środków finansowych w ciągu dwóch minut złożył autoryzowane zlecenia przelewów na łączną kwotę 33.289,68 zł. co dawało systemowi bankowemu informację o nietypowych zachowaniach powoda w zakresie korzystania ze zgromadzonych środków finansowych.

Wyniki postępowania dowodowego, zdaniem Sądu, pozwoliły na stwierdzenie, iż to powód nie wywiązał się z obowiązku wskazanego w art. 42 ust. 2 uup nieudostępniania instrumentu płatniczego osobom nieuprawnionym oraz nie podjął niezbędnych kroków mających na celu naruszenie indywidualnych zabezpieczeń urządzeń elektronicznych z których logował się do systemu bankowego pozwanego. Znamienny jest fakt, iż praktycznie 2 miesiące po utracie środków finansowych z konta powoda, powód sprzedał urządzenia elektroniczne z których m.in. korzystał z bankowości internetowej pozwanego, co uniemożliwiło weryfikację twierdzeń powoda w zakresie korzystania przez niego ze sprzętu rekomendowanego przez pozwanego, z aktualnym oprogramowaniem antywirusowym. Dla odpowiedzialności karnej sprawców którzy wyprowadzili środki finansowe z konta powoda ta okoliczność może pozostawać bez znaczenia albowiem doszło do przywłaszczenia środków finansowych wbrew woli powoda, jednakże dla odpowiedzialności cywilnej pozwanego ma to istotne znaczenie, z uwagi na wykazanie należytej staranności ze strony powoda w zakresie podjęcia niezbędnych środków służących zapobieżeniu naruszeniu indywidualnych zabezpieczeń oraz nieudostępnienia dostępu do konta osobom postronnym.

Trudno też w ocenie Sądu obciążać odpowiedzialnością pozwanego za dokonane nieautoryzowane przez powoda transakcje, w sytuacji gdy cała procedura autoryzacji przelewów w dniu 28 maja 2015 roku została przeprowadzona w sposób zgodny z obowiązującymi procedurami. Pozwany Bank mając na względzie bezpieczeństwo zgromadzonych środków finansowych, wydał zalecenia zarówno w zakresie stosowania sprzętu, oprogramowania jak również sposobu postępowania w zakresie bezpiecznego korzystania z bankowości elektronicznej. Także dwustopniowa procedura autoryzacji zleceń dodatkowo to bezpieczeństwo ma poprawiać. Nie można jednak wymagać od Banku i obciążać go odpowiedzialnością za własne niedbalstwo, oraz niedochowanie należytej staranności w zakresie zabezpieczeń sprzętu elektronicznego z którego użytkownik dokonuje transakcji w systemie bankowości elektronicznej.

Jak bowiem wynika z materiału dowodowego, logowanie do konta powoda w bankowości elektronicznej nastąpiło z IP z którego korzystał powód. Biegły sądowy z zakresu informatyki i teleinformatyki odczytał spójnie z zestawieniami sporządzonymi przez pozwany bank, iż logowanie do systemu podczas, którego utworzony nowy szablon płatności zdefiniowanego odbiorcy nastąpiło z tego samego IP, z którego po 26 minutach zalogował się powód by dać zlecenie

płatnicze zakupu waluty. Nadto powód w czasie, w którym nastąpiła autoryzacja utworzenia zdefiniowanego odbiorcy w ramach udostępnianego mu instrumentu płatniczego korzystał z telefonu komórkowego, do którego przypisany był numer telefonu, pod który pozwany bank kierował wiadomości sms z kodami autoryzacyjnymi. Powód nie kwestionował tej okoliczności. W toku procesu nie ustalono w jaki konkretnie sposób nieuprawnione przez powoda osoby lub osoba uzyskały informację o numerze klienta, haśle oraz kodzie autoryzacyjnym, jednak nie można w tym zakresie jakiekolwiek winy przypisać pozwanemu banku. Wskazać jednak należy, że czynności te zostały odczytane przez zautomatyzowany system bankowy jako czynności uprawnionego użytkownika. Zlecenie zostało złożone po pozytywnym przejściu systemu dwustopniowej autoryzacji.

W ocenie Sądu pozwany bank wykazał, że powód jako użytkownik autoryzował utworzenie nowego szablonu płatności, która to zgoda, stosownie do art. 40 ust. 1 uup odnosiła skutek do kolejnych transakcji płatniczych na rzecz tego odbiory. Stosownie do art. 45 ust. 1 i 2 upp ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika i polega na udowodnieniu innych niż wskazanie zarejestrowanego użycia instrumentu płatniczego okoliczności wskazujących na autoryzację transakcji płatniczej przez płatnika albo okoliczności wskazujące na fakt, że płatnik umyślnie doprowadził do nieautoryzowanej transakcji płatniczej, albo umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 w/w ustawy.

Sąd zauważył, że powód przyznał, iż w obsłudze instrumentu płatniczego posługiwał się kilkoma urządzeniami komputerowymi, w tym tabletem i laptopem, które po utracie środków finansowych z rachunku poddał badaniu pod kątem zawirusowania, a następnie zbył w obawie przed ponownymi atakami. Logowania do systemu poprzez inny sprzęt niż telefon komórkowy marki (...) zostały potwierdzone wydrukami z systemu informatycznego banku oraz opinią biegłego z zakresu informatyki i teleinfomartyki. W ocenie Sądu powodowi można przypisać co najmniej nieumyślne doprowadzenie do autoryzowania transakcji płatniczych, albowiem posługiwał się on komputerem, co do którego nie miał pewności o wyposażeniu w aktualne oprogramowanie antywirusowe, antyspamowe i zaporę firewall. Powód nadto przechowywał ten komputer w pracy, a więc w miejscu, gdzie teoretycznie dostęp do niego miała nieograniczona liczba osób o tożsamości niemożliwej do zidentyfikowania. Tymczasem pozwany bank w regulaminie korzystania z bankowości elektronicznej jasno określał użytkownikom wymagania dotyczących oprogramowania. Nadto bank na stronie internetowej umożliwiającej logowanie do systemu udostępniał użytkownikom kompendium wiedzy o bezpiecznym logowaniu do systemu, a w szczególności o metodach weryfikowania, czy logowanie odbywa się za pośrednictwem oryginalnej strony internetowej pozwanego banku. Powód logując się do systemu miał możliwość zapoznania się z choćby pojawiającymi się komunikatami o zagrożeniach w sieci ukierunkowanych na klientów bankowości elektronicznej. Komunikaty bowiem zostały ujawnione na stronie internetowej banku co najmniej na miesiąc przed spornym dniem, a powód każdego dnia sprawdzał salda rachunków za pośrednictwem systemu informatycznego. Zaniedbanie przez powoda zasad bezpieczeństwa stanowiło ułatwienie dla hakerów do włamania się do komputera czy tableta powoda i skopiowanie z tego sprzętu danych umożliwiających dostęp do konta w bankowości elektronicznej powoda.

W takim stanie rzeczy Sąd ocenił, że nie ma podstaw do uznania, że pozwany bank uchybił swoim obowiązkom wynikającym z art. 46 ust. 1 uup. W aktualnym stanie prawnym brak jest podstaw do uznania, iż dostawca instrumentu – bank, będący profesjonalistą w obrocie gospodarczym zobowiązany jest do zapewnienia zabezpieczeń indywidualnych dla systemów komputerowych płatników, a także do analizy prawdziwości danych wychodzących z komputerów użytkowników pod kątem, czy nie stanowią one wyniku działania przestępczego. Korzystanie z usług płatniczych w świetle obecnie obowiązującej ustawy opiera się na umowie stron i ich współdziałaniu w bezpiecznym korzystaniu z dobrodziejstwa postępu technologicznego umożliwiającego obrót bezgotówkowy. Z uwagi na fakt, iż regulamin świadczenia usług bankowości elektronicznej (...) powielał przepisy ustawy o prawach i obowiązkach stron dotyczących korzystania z instrumentu płatniczego, w tym zasadach autoryzacji zleceń płatniczych, to nie ma również podstaw do uznania odpowiedzialności kontraktowej pozwanego banku (art.471 k.c.). Zgromadzony materiał dowodowy nie stwarza warunków do uznania, iż pozwany banku dopuścił jakichkolwiek uchybień przy zabezpieczeniu

instrumentu płatniczego przypisanego powodowi przed dostępem dla nieuprawnionych użytkowników lub w inny sposób nienależycie wykonywał swoje zobowiązanie.

Gdyby nawet poszukiwać odpowiedzialności pozwanego ex delicto (art.415 k.c.) w ocenie Sądu również w tym zakresie nie można uznać, iż powód wykazał wszystkie przesłanki odpowiedzialności odszkodowawczej. Pomimo niewątpliwie istniejącej szkody jaką poniósł powód, nie została wykazana najmniejsza wina pozwanego związana z naruszeniem obowiązujących norm, czy też wynikająca z niesprawności systemów bankowych pozwanego, a wręcz przeciwnie biegły w swojej opinii wprost wskazywał, iż nie doszło do przełamania zabezpieczeń systemu bankowego pozwanego, zaś cała procedura autoryzacji przelewów została przeprowadzona zgodnie z wewnętrznymi procedurami Banku.

Mając na uwadze fakt, iż to powód uchybił wykonaniu obowiązku podjęcia niezbędnych środków służących zapobieżeniu naruszenia indywidualnych zabezpieczeń dostępu i używania konta w systemie bankowości elektronicznej, określonego w art. 42 ust. 2 uup, to on ponosi odpowiedzialność za nieautoryzowane przelewy z jego konta na obcy rachunek bankowy (art. 46 ust. 3 uup).

Z uwagi na powyższe Sąd oddalił powództwo w całości (pkt.1 wyroku).

Konsekwencją powyższego było orzeczenie o kosztach sądowych, które Sąd oparł o art. 98 k.p.c., normujący odpowiedzialność za wynik procesu.

Na podstawie art. 113 ust.1 ustawy o kosztach sądowych w sprawach cywilnych w zw. z art.98 k.p.c., Sąd nadto obciążył powoda obowiązkiem uiszczenia kosztów opinii biegłego w kwocie 1.422,67, które zostały tymczasowo pokryte przez Skarb Państwa.

Apelację od powyższego wyroku złożył powód, który zaskarżył go w całości, zarzucając:

1. naruszenie przepisów prawa materialnego, tj. art. 46 w zw. z art. 42 ustawy o usługach płatniczych w zw. z art. 471 k.c. w zw. z art. 725 k.c. w zw. z art. 726 k.c. w zw. z art. 50 ustawy – Prawo bankowe poprzez ich niezastosowanie w sytuacji, gdy pozwany nie wykazał, że powód doprowadził do wyprowadzenie środków pieniężnych z jego rachunku bankowego umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 ustawy o usługach płatniczych;

2. naruszenie art. 43 ust. 1 pkt 1 ustawy o usługach płatniczych poprzez jego niezastosowanie w sytuacji, gdy ze zgromadzonego w sprawie materiału dowodowego jednoznacznie wynika, iż pozwany nie zapewnił indywidualnego zabezpieczenia instrumentu płatniczego tak, by było ono niedostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu;

3. naruszenie art. 355 k.c. w zw. z art. 50 § 2 ustawy – Prawo bankowe poprzez ich niezastosowanie w sytuacji, gdy w toku postepowania dowiedziono, że pozwany nie zachował wymaganej od niego szczególnej staranności, wskutek czego umożliwił osobom nieuprawnionym pozyskanie bez zgody i wiedzy powoda danych umożliwiających zalogowanie się do jego rachunków bakowych i wykonanie reklamowanych transakcji;

4. naruszenie art. 40 ust. 1 ustawy o usługach płatniczych poprzez bezpodstawne przyjęcie, że powód wyraził zgodę na dokonanie na jego rachunkach bankowych reklamowanych transakcji, w sytuacji gdy ze zgromadzonego materiału dowodowego jednoznacznie wynika, iż powód nie wiedział o dokonywaniu tych transakcji i absolutnie w żaden sposób nie wyraził na nie zgody;

5. błąd w ustaleniach faktycznych przyjętych za podstawę rozstrzygnięcia polegający na przyjęciu, że powód nie wykazał dbałości o własne życiowe sprawy oraz że nie wywiązał się z obowiązku nieudostępniania instrumentu płatniczego osobom nieuprawnionym, a także że nie podjął niezbędnych kroków, mających na celu zabezpieczenie przed naruszeniem indywidualnych zabezpieczeń urządzeń elektronicznych, z których logował się do systemu bankowego pozwanego;

6. błąd w ustaleniach faktycznych przyjętych za podstawę rozstrzygnięcia polegający na przyjęciu, że system bankowy pozwanego działał poprawnie oraz że nie można przypisać mu rażącego niedbalstwa w zakresie ochrony środków zgromadzonych na rachunkach bankowych powoda;

7. błąd w ustaleniach faktycznych polegający na bezpodstawnym przyjęciu, że powód nie stosował odpowiednich zabezpieczeń sprzętu, z którego logował się do systemu bankowego oraz bezzasadnym przyjęciu, że przechowywanie go w pracy powoda stanowiło naruszenie zasad bezpieczeństwa;

8. naruszenie przepisów art. 6 k.c. poprzez jego niezastosowanie i ustalenie rażącego niedbalstwa powoda pomimo, że pozwana w tym zakresie nie przedstawiła żadnego dowodu;

9. naruszenie art. 233 § 1 k.p.c. poprzez zaniechanie wszechstronnej oceny dowodów zgromadzonych w sprawie, co doprowadziło do błędnego ustalenia stanu faktycznego sprawy, co miało wpływ na treść wyroku.

Wobec powyższego powód wniósł o zmianę zaskarżonego wyroku i zasądzenie od pozwanego na rzecz powoda kwoty 137.665 zł wraz z odsetkami ustawowymi od dnia 29 maja 2015 r. do dnia zapłaty oraz o zwrot kosztów postępowania, w tym kosztów zastępstwa procesowego oraz opłaty skarbowej od pełnomocnictwa – według norm przepisanych, za I i II instancję.

Sąd Apelacyjny ustalił i zważył co następuje.

Apelacja okazała się bezzasadna. Sąd Apelacyjny podziela ustalenia faktyczne Sądu I instancji, uznając je za własne, z poniższą modyfikacją i uzupełnieniem. Dla ścisłości należało doprecyzować, iż suma zakwestionowanych przelewów wynosi 137 385 zł , nie zaś- 137 285 zł, jak przyjęto w toku postępowania.

Natomiast Sąd Okręgowy trafnie ustalił na podstawie starannie przeanalizowanego materiału dowodowego, iż powód nie wywiązał się z obowiązku podjęcia niezbędnych środków w celu zapobieżenia naruszenia indywidualnych danych uwierzytelniających i starannego przechowywania instrumentu płatniczego oraz nieudostępniania go osobom nieuprawnionym. Powód korzystał z laptopa, jak sam twierdzi, zabezpieczonego jedynie bezpłatnym programem antywirusowym, a taki rodzaj programów, niezależnie od tego iż nie jest przeznaczony dla firm, to nie zapewnia należytej ochrony antyphishingowej i antywirusowej. Ponadto powód trzymał sprzęt, z którego korzystał w ramach łączenia się z bankiem/ tablet i laptop/ w pracy, gdzie miały do niego dostęp również inne osoby, co zasadnie zauważył Sąd I instancji, a która to sytuacja co najmniej stwarzała możliwość dostępu do tych urządzeń innych osób, również bez jego wiedzy. Należy zauważyć przy tym, iż A. K. utrzymywał, iż w firmie jego pracownik sprawdzał komputery i w ramach tej kontroli system antywirusowy nie wykrył programów szpiegujących /względnie wirusów etc./. Jest symptomatyczne, iż obydwa urządzenia zostały przez powoda zbyte za stosunkowo niewielkie kwoty pieniężne w sierpniu 2015r., z obawy – jak wskazywał – przed zawirusowaniem, a zatem po miesiącu od złożenia pozwu w niniejszej sprawie. Tymczasem sprawozdanie z badania tych urządzeń stanowiłoby cenny materiał dowodowy, z punktu widzenia pełnego wyjaśnienia przebiegu spornych transakcji, tym bardziej, iż sprawca składający dyspozycję utworzenia nowego szablonu odbiorcy na rzecz rachunku przynależnego do P. O., logował się za pośrednictwem urządzenia posiadającego I.P. przynależne do powoda.

Poczynione ustalenia wykluczają zarazem /opinia biegłego nie była kwestionowana w tym zakresie/, aby doszło do przełamania zabezpieczeń systemu banku, a zatem procedura autoryzacji szablonu przebiegła prawidłowo. Innymi słowy osoba odpowiedzialna za utworzenie stałego szablonu zdefiniowanego odbiorcy oraz jego aktywację przy pomocy sms-a nr 1 nie działała „włamując się" na rachunek powoda bezpośrednio do banku (...) S.A. Tym samym brak jest w ogóle podstaw do przypisywania pozwanemu bankowi naruszenia jakichkolwiek obowiązków staranności w zakresie nadzoru nad mieniem klientów, w szczególności niezapewnienia ze swojej strony należytej ochrony rozważanego instrumentu płatniczego. Należy przy tym zauważyć, iż sms przesyłany do klienta, z kodem aktywującym szablon, do wykorzystania przez odbiorcę, nie jest zapisywany nigdzie w systemie, a zatem zna go tylko i wyłącznie płatnik. O ile zatem ktoś posiadłby wiedzę odnośnie numeru klienta i hasła niezbędnych do zalogowania się jako

dany użytkownik , to i tak nie mógłby dokonać aktywacji szablonu/ niezbędnej do jego skuteczności/ bez znajomości kodu z sms-a. Tymczasem, jak zostało ustalone na podstawie niekwestionowanej opinii biegłego, telefon powoda był doskonale zabezpieczony, zapory te nie byłe przełamane, innymi słowy - nie został „zhakowany". Nikt zatem tego szyfru bez zgody właściciela telefonu nie mógł poznać. Powód stanowczo przy tym utrzymywał, iż w ogóle nie użył powyższego kodu /"Nie wpisywałem nigdzie sms-a z autoryzacją odbiorcy zdefiniowanego" – k. 421/. Oznacza to, iż A. K. nie mógł nieświadomie skorzystać z fałszywej strony internetowej banku, podsuniętej przez osobę, która zmierzałaby do kradzieży środków pieniężnych, umożliwiając jej stworzenie i aktywację szablonu stałych przelewów, a zatem nie był ofiarą podstępnych działań hakera, skoro ten ostatni bez udziału powoda nie miałby możliwości poznania kodu z sms-a, otrzymanego wyłącznie na telefon, co z kolei uniemożliwiało aktywację szablonu. Powyższe dodatkowo wyklucza odpowiedzialność banku z tytułu ewentualnego nienależytego wykonywania umowy względem powoda, a zatem różnicuje przedmiotową sytuację w stosunku do opisanych z orzeczeniach Sądów, które przyjęły odpowiedzialność banku za nieautoryzowane transakcje w rozważanych tam stanach faktycznych /wyrok SN z dnia 18.01.2018 r., V CSK 141/17, wyrok SO w Warszawie z dnia 12.05.2018 r., I C 566/17 – k. 553 i nast., wyrok SO w Łodzi z dnia 10.04.2017 r., III Ca 43/17-k 517/. W niniejszym przypadku kwestionowane transakcje były należycie uwierzytelnione przy użyciu pochodzących z banku: loginu, hasła i kodu.

W dalszej kolejności należy doprecyzować ustalenia Sądu I instancji, iż całokształt twierdzeń i zeznań powoda wskazuje, iż nie tylko otrzymał w dniu 28.05.2015r. o godzinie 10:12 sms nr1 z kodem do autoryzacji szablonu, za pomocą którego dokonano kwestionowanych serii przelewów, ale odczytał go najpóźniej przy okazji powzięcia informacji o treści sms-a nr 2 i autoryzowaniu przy pomocy tego drugiego sms-a transakcji przelewu/ na inny rachunek/ na kwotę 18 900zł, której istnienia nie kwestionował, a która to dyspozycja ze strony miała miejsce o godzinie 10:35. Zeznania A. K. w tym zakresie są wzajemnie sprzeczne i nielogiczne. Najpierw bowiem twierdził on , iż odczytał wszystkie sms-y, następnie, że nie pamięta, czy odczytał rozważany sms nr 1 razem z sms-em nr 2, potem że go nie odczytywał, bo myślał, iż jest to sms, zawierający saldo transakcji na koncie. Jest to nielogiczne, skoro powód nie otrzymywał sms-ów z informacją o saldzie dotyczących konta osobistego /co wynika z opinii biegłego, jak i zestawu sms-ów złożonych przez pozwanego/, lecz jedynie firmowego, ponadto taki sms, odnośnie tego ostatniego konta, dostał tego dnia, tj. 28.05.2015 r., po godzinie siódmej rano, brak było zatem podstaw do formułowania sądu, iż przyjdzie on jeszcze raz. Powód, przy tym, jak wskazano wyżej, stanowczo utrzymywał, iż z powyższego sms-a nie skorzystał /kodu nigdzie nie wpisywał/. Zeznania te są z kolei sprzeczne z twierdzeniami złożonymi w jego imieniu na rozprawie apelacyjnej przez pełnomocnika, który wyraził wcześniej nie formułowany pogląd, iż powód „musiał użyć" rozważany sms, tylko o tym nie wiedział lub nie zwrócił na to uwagi. Dodatkowo należy podnieść, iż sms-y na smartfonie są wyświetlane i numerowane w czytelny sposób i można się szybko zorientować co do ich kolejności i treści. A. K. jest doświadczonym użytkownikiem rachunku oszczędnościowo-rozliczeniowego, korzysta na co dzień wielokrotnie z instrumentów elektronicznych, zaś dzienne dyspozycje przelewów czasami przekraczały 20 000zł, a miesięczne obroty sięgały kwoty 8 000 000zł. Omówione twierdzenia powoda w świetle powyższych okoliczności sprawy, zdaniem Sądu Apelacyjnego, w sposób nie budzący wątpliwości pozwalają przyjąć, iż powód wskazanego sms-a nr 1 odczytał najpóźniej o godzinie 10:35, kiedy złożył i autoryzował dyspozycję kolejnego przelewu. W związku z tym już wtedy, w założeniu, że nic nie wiedział o ustanowieniu stałego szablonu, winien bezzwłocznie / § 13 ust. 1 Regulaminu/ zawiadomić bank o niezrozumiałej informacji, dotyczącej przysłania mu kodu, którego nie zamawiał i w swoim mniemaniu – nie potrzebuje. Pozwoliłoby to zapobiec wykonaniu wszystkich kwestionowanych transakcji, które rozpoczęły się blisko trzy godziny później /pierwsza dyspozycja co do kwoty 19.570 zł miała miejsce o 13:08/. Dodatkowo należy zauważyć, iż powód otrzymał ponadto o godzinie 14:38 sms, dotyczący kodu autoryzacji transakcji na kwotę 19.915 zł, początkowo oznaczonej jako oddzielna, przelanej ostatecznie o godzinie 14:39 w ramach szablonu. Wówczas również winien się zaniepokoić i podjąć stosowne czynności w celu zawiadomienia banku i wyjaśnienia sytuacji, tym bardziej, iż z telefonu korzystał nieustannie przez cały dzień i jak to określił Sąd I instancji, praktycznie się z nim nie rozstawał. W tym czasie pozostawała otwarta możliwość nie tylko zatrzymania kolejnych przelewów i dezaktywowania szablonu, ale i „zamrożenia" /w porozumieniu z bankiem odbiorcy środków/ przelanych kwot, celem ich odzyskania. Powyższe oznacza naruszenie §13 Regulaminu /zaniechanie powiadomienia o nieuprawnionym użyciu instrumentu i nieuprawnionego dostępu – k. 86/ oraz art. 42 ust. 1 pkt 2 ustawy z dnia 19 sierpnia 2011r. o usługach płatniczych /D.U. 2011.199.1175 ze zm./. Całokształt omówionych okoliczności /

przy podkreślanym braku „włamania” do systemu banku i wykluczeniu zalogowania się przez powoda na fałszywej stronie internetowej/ wskazuje, iż powód udostępnił instrument finansowy, pozwalający wykonać przedmiotowe, kwestionowane transakcje innej osobie, względnie doprowadził do tego wskutek rażącego niedbalstwa, w tym ujawnił treść kodu aktywującego szablon, zawartego w sms-ie nr 1.Ten ostatni, jak podkreślono wyżej, przesłany na telefon, bez udziału powoda byłby niedostępny nawet dla osoby, która przełamałaby zabezpieczenia jego komputera. Z powyższą konstatacją koresponduje okoliczność, iż dyspozycja utworzenia szablonu, podparta właściwym użyciem instrumentu finansowego, z wpisaniem numeru klienta i hasła /stanowiących I stopień ochrony, w stosunku do użycia kodu jako czynności II, następczej/ została dokonana z urządzenia posiadającego ten samo adres I.P., co komputer powoda, z którego wykonywał 20 minut później transakcję, niezakwestionowaną przez siebie /odnośnie przelewu sumy 18 900zł, na podstawie dyspozycji złożonej o godzinie 10:35/. Są to wszystko okoliczności, których mowa w art. 45 ustawy o usługach płatniczych w brzmieniu obowiązującym przed dniem 20.06.2018 r., tj. przed zmianami wprowadzonymi ustawą z dnia 10.05.2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw/D.U. 2018.1075/. Natomiast w niniejszym postępowaniu nie zostało wykazane, a w każdym razie A. K. nawet takich wniosków dowodowych nie składał, ani nie podnosił, aby doszło do podrobienia I.P. jego komputera. W konsekwencji należy uznać, iż zostało wykazane, że powód umyślnie, a co najmniej wskutek rażącego niedbalstwa, nie zgłosił niezwłocznie nieuprawnionego użycia instrumentu finansowego /a dopiero wieczorem/, a ponadto nie podjął należytych środków ostrożności w zakresie przechowywania instrumentu płatniczego i nieudostępniania go osobom trzecim, jak również w zakresie zabezpieczenia sprzętu, na którym dokonywano transakcji. Powyższe oznaczało naruszenie obowiązków określonych w art. 42 ustawy o usługach płatniczych, co w konsekwencji skutkowało jego odpowiedzialnością za przedmiotowe transakcje, na podstawie art. 46 ust. 3 tej ustawy. Powyższe implikuje nietrafność podnoszonych, wskazanych w apelacji zarzutów naruszenia prawa materialnego oraz uprawnia do konstatacji, iż pozwany przeprowadził skuteczną egzoneracją w rozumieniu art. 471 k.c. W związku z powyższym apelacja jako bezzasadna na podstawie art. 385 k.p.c. podlegała oddaleniu, zaś postanowienie o kosztach postępowania apelacyjnego uzasadnia treść art. 108 § 1 k.p.c. w zw. art. 98 § 1 i 3 k.p.c.