

Sygn. akt I C 338/17

WYROK W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 6 grudnia 2018r.

Sąd Okręgowy w Bielsku-Białej I Wydział Cywilny w składzie następującym:

Przewodniczący: SSO Jerzy Strzygocki

Protokolant: protokolant sądowy Klaudia Słowik-Przybyła

po rozpoznaniu w dniu 22 listopada 2018r. w Bielsku-Białej

na rozprawie

sprawy z powództwa A. Ł.

przeciwko (...) Bankowi (...) Spółce Akcyjnej z siedzibą w W.

o zapłatę

1/ zasądza od strony pozwanej na rzecz powódki kwotę 108.655 zł (sto osiem tysięcy sześćset pięćdziesiąt pięć złotych) wraz z odsetkami ustawowymi za opóźnienie od dnia 4 lipca 2015 r. do dnia zapłaty;

2/ zasądza od strony pozwanej na rzecz powódki kwotę 10.833 zł (dziesięć tysięcy osiemset trzydzieści trzy złote) tytułem zwrotu kosztów procesu;

3/ nakazuje pobrać od strony pozwanej na rzecz Skarbu Państwa – Sądu Okręgowego w Bielsku-Białej kwotę 1.012,27 zł (jeden tysiąc dwanaście złotych 27/100) tytułem kosztów sądowych.

SSO Jerzy Strzygocki

Sygn. akt I C 338/17

UZASADNIENIE

Pozwem z 17.07.2017 r. powódka A. M. (obecnie A. Ł.) wniosła o zasądzenie od pozwanego (...) Banku (...) spółki akcyjnej z siedzibą w W. na rzecz powódki kwoty 108 655,00 zł z odsetkami ustawowymi od 04.07.2015 r. do 31.12.2015 r. i odsetkami ustawowymi za opóźnienie od 01.01.2016 r. do dnia zapłaty, a także zasądzenia od pozwanego kosztów procesu.

W uzasadnieniu podała, że zawarła ze stroną pozwaną umowę rachunku bankowego. W dniu 29.05.2015 r. zostały zrealizowane nieautoryzowane przez powódkę transakcje na łączną kwotę 108655 zł. O fakcie tym powódka zawiadomiła stronę pozwaną w dniu 03.06.2015 r., a w dniu 05.06.2015 r. Komisariat Policji w B.. Zdaniem powódki strona pozwana nie zapewniła, aby indywidualne zabezpieczenia instrumentu płatniczego nie były dostępne dla osób trzecich. Równocześnie powódce nie można przypisać odpowiedzialności za powyższe transakcje płatnicze, gdyż nie doprowadziła do nich z winy umyślnej, ani w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia swoich obowiązków.

W odpowiedzi na pozew strona pozwana domagała się oddalenia powództwa w całości oraz zasądzenia od powódki na swoją rzecz kosztów procesu.

W uzasadnieniu potwierdziła, że zawarła z powódką umowę rachunku bankowego, jednakże płatności dokonane z w dniu 29.05.2015 r. nastąpiły w związku z niezastosowaniem się przez powódkę do podstawowych zasad bezpieczeństwa tj. na skutek ujawnienia w dniu 28.05.2015 r. kodu autoryzacyjnego znajdującego się w wyłącznym posiadaniu powódki. Strona pozwana na stronie logowania do serwisu (...) każdorazowo podaje informacje, że logowanie nie wymaga podania kodu z narzędzia autoryzacyjnego. Ponadto bank nigdy nie prosi o podanie jednocześnie kilku kodów z narzędzia autoryzacyjnego lub danych karty płatniczej. Prośba o podanie danych była wynikiem uprzedniego zainfekowania komputera złośliwym oprogramowaniem. Wobec tego powódka nie zachowała należytej staranności, dodatkowo naruszyła w sposób rażący ciężące na niej obowiązki użytkownika systemu bankowości elektronicznej. Tym samym strona pozwana nie jest zobowiązana do zwrotu środków.

Sąd ustalił następujący stan faktyczny:

W dniu 22.11.2001 r. powódka zawarła z (...) Bankiem (...) S.A. umowę rachunku oszczędnościowo-rozliczeniowego w oparciu o którą prowadzony był rachunek indywidualny nr (...) - (...) - 270-41 w ofercie (...). Do konta tego została wydana międzynarodowa karta (...) ze znakiem V. E.. W dniu 28.02.2002 r. powódka złożyła wniosek o świadczenie usługi bankowej (...), dzięki której strona pozwana mogła informować powódkę o saldzie rachunku za pośrednictwem SMS-a wysyłanego na nr (...). Od 17.11.2003 r. powódka złożyła dyspozycję przekazywania informacji o zmianach salda na adres mailowy: (...)

Powyższa umowa została zastąpiona umową rachunku oszczędnościowo-rozliczeniowego (...) (z (...)), usług bankowości elektronicznej oraz karty debetowej z 14.01.2008 r. Na podstawie nowej umowy strona pozwana zobowiązała się do prowadzenia rachunku oszczędnościowo-rozliczeniowego (...), w walucie polskiej o numerze (...), na zasadach określonych w umowie i regulaminie rachunku oszczędnościowo-rozliczeniowego usług bankowości elektronicznej oraz karty debetowej, a także rachunku oszczędnościowego w walucie polskiej i walutach obcych. Ponadto wydała powódce kartę debetową do (...). Zapewniła powódce dostęp do jej rachunków i korzystania z usług bankowości elektronicznej, na zasadach określonych w umowie i regulaminie.

(dowód: umowa rachunku oszczędnościowego lub oszczędnościowo-rozliczeniowego z 22.11.2001 r. – k. 75-76, karta posiadacza rachunku – k. 76v-77, wniosek o świadczenie usługi bankowej – k. 78, potwierdzenie otwarcia rachunku – k. 79, umowa rachunku oszczędnościowo-rozliczeniowego (...), usługi bankowości elektronicznej oraz karty debetowej z 14.01.2008 r. – k. 79v-80, dokumenty związane z prowadzeniem rachunku bankowego – k. 80v-87)

Zgodnie z § 11 ust. 1 Regulaminu świadczenia usług bankowości elektronicznej w (...) Banku (...) S.A. strona pozwana wprowadza mechanizmy zapewniające bezpieczeństwo korzystania z usług bankowości elektronicznej m.in. poprzez stosowanie weryfikacji klienta bądź ustanowionego użytkownika i autoryzacji z wykorzystaniem instrumentów uwierzytelniających. Zgodnie z § 11 ust. 3 zdanie 1 regulaminu wszelkie dyspozycje złożone w formie elektronicznej przez osobę, która została prawidłowo zweryfikowana, są traktowane jako dyspozycje klienta lub ustanowionego użytkownika. Zgodnie z § 12 ust. 1, ust. 2, ust. 3 i ust. 4 regulaminu klient jest zobowiązany do logowania oraz wykonywania dyspozycji za pośrednictwem elektronicznych kanałów dostępu wyłącznie osobiście z użyciem instrumentów uwierzytelniających, z uwzględnieniem § 5 ust. 2 (ust. 1). Klient jest zobowiązany do zachowania w tajemnicy informacji zapewniających bezpieczne korzystanie z usług bankowości elektronicznej, w tym informacji przekazanych (...) Bankowi (...) SA dla celów weryfikacji oraz nieudostępniania i nieujawniania innym osobom instrumentów uwierzytelniających (ust. 2). Klient jest zobowiązany do należytego zabezpieczenia urządzeń i oprogramowania, o których mowa w § 3 ust. 2, za pośrednictwem których korzysta z usług bankowości elektronicznej w celu zapewnienia bezpieczeństwa dostępu do usług bankowości elektronicznej poprzez stosowanie:

1) wyłącznie legalnego oprogramowania, jego bieżącą aktualizację i instalację poprawek systemowych zgodnie z zaleceniami producentów,

2) aktualnego oprogramowania antywirusowego i antyspamowego oraz zapory firewall,

3) najnowszych wersji przeglądarek internetowych,

4) stosowanie haseł zabezpieczających dostęp do komputera, w szczególności jeśli z urządzenia korzysta więcej osób (ust. 3). Szczegółowy opis środków, jakie powinien przedsięwziąć Klient w celu zapewnienia bezpieczeństwa dostępu do usług bankowości elektronicznej podawany jest do wiadomości klienta i ustanowionych użytkowników na stronie internetowej (...) oraz w serwisie telefonicznym (ust. 4).

(dowód: regulaminy świadczenia usług bankowości elektronicznej u strony pozwanej – k. 101-108)

Zgodnie z procedurami obowiązującymi ówczynie u strony pozwanej warunkiem wykonania transakcji za pośrednictwem bankowości elektronicznej było podanie konkretnego kodu autoryzacyjnego (zlecający proszony był o podanie kodu autoryzacyjnego o określonym numerze), który zgodnie z zapisami umowy, może posiadać tylko klient. Kody autoryzacyjne znajdują się na karcie zdrapce, która zawiera około 40 takich kodów. Nie jest możliwe dokonanie transakcji przy użyciu niewłaściwego kodu, tj. z innego pola na karcie kodów. Możliwe jest utworzenie szablonu zaufanego odbiorcy, który tworzony jest przy wykorzystaniu konkretnego kodu autoryzacyjnego. W oparciu o szablon zaufanego odbiorcy możliwe jest wykonanie wielu przelewów, bez konieczności ich dodatkowej autoryzacji. Po 2015 r. w pozwanym banku zmodyfikowano sposób zabezpieczenia transakcji w ten sposób, że jeżeli tworzony jest szablon zaufanego odbiorcy to pierwsza transakcja z tego szablonu wymaga autoryzacji.

(dowód: zeznania świadka D. P. – k. 283-284 i nagranie audiowizualne z rozprawy z 9 listopada 2017 r., oświadczenie J. G. z 16.11.2017 r. – k. 297, oświadczenie D. P. z 20.11.2017 r. – k. 298, zeznania świadka J. G. – k. 593-594 i nagranie audiowizualne z rozprawy z 22.11.2018 r.)

W dniu 26.05.2015 r. na komputerze służbowym powódka chciała zalogować się do systemu bankowości elektronicznej (...). Podczas logowania wyskoczył jej komunikat, że nie można się zalogować z uwagi na nieprawidłowe hasło. Wtedy powódka zadzwoniła na infolinię (...), podała kod dostępu do infolinii, a następnie zmieniła hasło do logowania do systemu bankowości elektronicznej. Zalogowała się do systemu używając zmienionego hasła i wykonała przelew.

Po kilku dniach powódka ponownie próbowała zalogować się do bankowości elektronicznej (...). Ponownie pojawił się komunikat o nieprawidłowym hasle. Powódka powtórzyła czynności konieczne do zmiany hasła. Po zalogowaniu powódka zobaczyła, że na jej rachunku bankowym brakuje znacznej kwoty pieniędzy. Po przesłaniu historii transakcji zorientowała się, że w dniu 29.05.2015 r. przelano z jej rachunku oszczędnościowego na rachunek bieżący środki pieniężne, a następnie dokonano 6 nieautoryzowanych przez nią transakcji na łączną kwotę 108 655 zł, na rachunek bankowy nr (...), którego posiadaczem był J. N.. Transakcje te opiewały kolejno na kwoty 19 350 zł, 19 705 zł, 19 400 zł, 19 200 zł, 19 000 zł oraz 12 000 zł. W tym okresie również z rachunków bankowych innych klientów strony pozwanej dochodziło do nieautoryzowanych transakcji, skutkujących wyprowadzeniem z ich kont znacznych kwot.

Powódka była zaskoczona powyższym zdarzeniem, gdyż logowała się do bankowości elektronicznej najczęściej z komputera służbowego, który posiadał wysokiej jakości zabezpieczenia antywirusowe. Ponadto nie podawała nikomu kodów z karty zdrapki. Nigdy nie korzystała z szablonu zaufanego odbiorcy. Przy logowaniu zawsze sprawdzała, czy jest to strona banku. Korzystała z bankowości elektronicznej praktycznie od samego początku, kilka lub kilkanaście razy w miesiącu.

(dowód: zestawienie operacji z dnia 29.05.2015 r. – k. 12, karta zgłoszenia nr (...) – k. 13, artykuły internetowe – k. 35-39, zeznania powódki – k. 311v-312 i nagranie audiowizualne z rozprawy z 25.01.2018 r., k. 594 i nagranie audiowizualne z rozprawy z 22.11.2018 r.)

Powódka w dniu 03.06.2015 r. zgłosiła powyższe zdarzenie w oddziale strony pozwanej, wnosząc o zwrot tych środków. W odpowiedzi na powyższe zgłoszenie strona pozwana potwierdziła, że dokonane transakcje zostały wykonane po

poprawnym zalogowaniu w serwisie (...). Zdaniem strony pozwanej ich realizacja nastąpiła w wyniku zainfekowania stacji roboczej, z której powódka logowała się do serwisu, złośliwym oprogramowaniem. Powódka podczas próby logowania w wyniku zainfekowania komputera została poproszona o podanie kodu nr 41 z karty kodów, co uczyniła. W ten sposób osoba nieupoważniona zdefiniowała nowy szablon płatności na podstawiony rachunek odbiorcy, który następnie został wykorzystany do realizacji zakwestionowanych przelewów. Strona pozwana nie uwzględniła reklamacji powódki. W toku wyjaśnienia całego zdarzenia nie zabezpieczyła również komputera powódki, z którego logowała się do bankowości elektronicznej. Mimo odwołania powódki od takiego sposobu rozwiązania reklamacji strona pozwana pismem z 20.08.2015 r. w dalszym ciągu nie uznała roszczeń powódki.

(dowód: karta zgłoszenia nr (...) – k. 13, 88, odpowiedź na zgłoszenia nr (...) – k. 89-90, odpowiedź z 20.08.2015 r. na zgłoszenie skierowane do Banku – k. 91, pismo z 08.09.2015 r. – k. 92-93, odpowiedź strony pozwanej z 21.09.2015 r. – k. 94, zeznania świadka D. P. – k. 283-284 i nagranie audiowizualne z rozprawy z 9 listopada 2017 r., zeznania powódki – k. 311v-312 i nagranie audiowizualne z rozprawy z 25.01.2018 r., zeznania świadka J. G. – k. 593-594 i nagranie audiowizualne z rozprawy z 22.11.2018 r.)

W dniu 05.06.2015 r. powódka zgłosiła powyższe zdarzenia na Komisariacie III Policji w B.. Postanowieniem z 22.06.2015 r. wszczęto dochodzenie w sprawie. W toku postępowania zatrzymano komputer z którego powódka logowała się do systemu bankowości elektronicznej. Ustalono, że na dysku twardym tego komputera nie ma zainstalowanego oprogramowania, które przyczyniło się do zrealizowania nieautoryzowanych przelewów. Na nośniku danych zostały znalezione ślady otwierania linków, które wskazywały że pochodzą od firmy kurierskiej (...), a w rzeczywistości otwierały strony zawierające złośliwe oprogramowanie. Nie było możliwości ustalenia sprawcy infekcji. W toku postępowania ustalono, że rachunek bankowy, na który trafiły środki z rachunku powódki należy do J. N. zamieszkałego w B., (...)N. B. J. N.. Założył on rachunek bankowy drogą elektroniczną. Nie udało ustalić się miejsca pobytu J. N.. Z zeznań jego ojca – K. N. wynika, iż w kwietniu 2015 r. J. N. wyprowadził się z miejsca zamieszkania i nie wrócił do domu. Jego ojciec nie miał wiedzy o miejscu jego pobytu. Wobec braku możliwości przesłuchania w charakterze świadka J. N., którego zeznania miałyby istotny wpływ na wynik postępowania, postanowieniem z dnia 31.12.2015 r. zawieszono dochodzenie w sprawie. Zażalenie na to postanowienie złożyła powódka. Postanowieniem z dnia 29.03.2016 r. Sąd Rejonowy w Bielsku-Białej uwzględnił to zażalenie i uchylił postanowienie o zawieszeniu dochodzenia.

(dowód: zaświadczenia Komisariatu Policji nr III w B. z dnia 05.06.2015 r. – k. 14, dokumenty z postępowania 2 Ds. 876/15/D nadzorowanego przez Prokuraturę Rejonową B. P. w B. – k. 201-281, odpisy dokumentów z akt sprawy PK II WZ Ds. 7.2016 w zakresie dotyczącym powódki – k. 417-591)

Logowanie do systemu bankowego strony pozwanej w dniu 28.05.2015 r. nastąpiło przy użyciu prawidłowego loginu i hasła powódki, a utworzenie szablonu zaufanego odbiorcy nastąpiło przy użyciu jednorazowego kodu autoryzacyjnego o numerze 41. Po utworzeniu szablonu zaufanego odbiorcy, wykonywanie przelewów nie wymagało podawania innych kodów autoryzacyjnych. Następnie wykonano serię przelewów między kontem oszczędnościowym, a rachunkiem bieżącym powódki. Następnie przy użyciu szablonu zaufanego odbiorcy wykonano serię przelewów na rachunek bankowy zapisany w utworzonym szablonie.

W dacie dokonywania powyższych czynności system bankowości strony pozwanej posiadał szereg zabezpieczeń, uniemożliwiających dostęp osób postronnych do kont swoich klientów. Prawidłowo zabezpieczony system bankowy powinien żądać jednorazowego kodu autoryzacyjnego, do każdej czynności mającej wpływ na wykorzystanie środków pieniężnych, przechowywanych na koncie bankowym. Jedynym wyjątkiem jest możliwość zastosowania szablonu zaufanego odbiorcy, przy wykorzystaniu kodu autoryzacyjnego, co miało miejsce w niniejszym przypadku.

Nie można jednoznacznie stwierdzić jak wyglądał proceder wyprowadzenia środków pieniężnych z rachunku powódki. Prawdopodobne jest, że za pomocą złośliwego oprogramowania podmieniona została strona logowania do konta, a następnie nieświadoma powódka podając dane do logowania udostępniła je przestępcy, który następnie wykonał

nieautoryzowane transakcje. Nie jest możliwe jednoznaczne stwierdzenie, czy powódce można postawić zarzut jakiegokolwiek zaniedbania przy dokonywaniu czynności przy korzystaniu z bankowości elektronicznej.

(dowód: opinia biegłego z zakresu informatyki śledczej oraz analizy kryminalnej z dnia 26.07.2018 r. – k. 339-350)

Pismem z 18.01.2015 r. powódka wezwała stronę pozwaną do zapłaty kwoty 108 655 zł, wraz z ustawowymi odsetkami od dnia 30.05.2015 r. do dnia zapłaty. W odpowiedzi strona pozwana podniosła, iż transakcje zostały zlecone w wyniku niezastosowania się przez powódkę do zasad bezpieczeństwa korzystania z serwisu (...), pomimo informowania o zasadach bezpiecznego logowania. Prowadzone przez stronę pozwaną działania w celu odzyskania środków niestety nie zakończyły się powodzeniem.

(dowód: ostateczne przedsądowe wezwanie do zapłaty z 18.01.2015 r. – k. 15-18, 95-96, potwierdzenie nadania – k. 19, pełnomocnictwo – k. 20, 97, upoważnienie z podpisem notarialnie poświadczonym – k. 21-24, 97v-98, odpowiedź strony pozwanej na pismo z dnia 18.01.2015 r. – k. 25-26, 99-100)

Między stronami toczyło się sprawa o zawezwanie do próby ugodowej wniesiona przez powódkę. Postępowanie toczyło się przed Sądem Rejonowym dla Warszawy-Mokotowa w W. pod sygn. akt XVI Co 2586/16. W dniu 14.03.2017 r. odbyło się posiedzenie, na którym nie stawiał się żaden reprezentant strony pozwanej. Do pojednania pomiędzy stronami nie doszło.

(dowód: wniosek o zawezwanie do próby ugodowej z 14.12.2016 r. – k. 27-33, protokół z posiedzenia z dnia 14.03.2017 r. w sprawie XVI Co 2586/16 Sądu Rejonowego dla Warszawy M. w W. – k. 34, dokumenty zgromadzone w aktach sprawy I Co 2586/16 Sądu Rejonowego dla Warszawy-Mokotowa w W.)

Ustalając stan faktyczny sprawy Sąd oparł się na wskazanych wyżej dowodach. Strony nie kwestionowały dowodów z dokumentów. Sąd również nie znalazł podstaw do odmówienia im wiarygodności.

Na rozprawie w dniu 25.01.2018 r. Sąd oddalił wniosek strony pozwanej o dopuszczenie dowodu z przedłożonych na tej rozprawie orzeczeń, w szczególności, jako bezprzedmiotowe dla rozstrzygnięcia w niniejszej sprawie.

Sąd oparł się również na opinii biegłego, która była rzetelna, logiczna i spójna. Strony nie kwestionowały wniosków w niej zawartych.

Zeznania świadków i powódki w całości należało uznać za wiarygodne. Z uwagi na charakter sprawy i stanowisko strony pozwanej dowód z przesłuchania stron ograniczono do zeznań powódki.

Sąd zważył, co następuje:

Powództwo zasługiwało na uwzględnienie.

Zgodnie z treścią art. 725 k.c. przez umowę rachunku bankowego bank zobowiązuje się względem posiadacza rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych oraz, jeżeli umowa tak stanowi, do przeprowadzania na jego zlecenie rozliczeń pieniężnych.

Zawarcie umowy rachunku bankowego powoduje, że środki pieniężne posiadacza przechodzą na własność banku. Mimo braku jednoznacznego sformułowania w przepisach ustawy, w doktrynie i w orzecznictwie, powszechny i w zasadzie niekontrowersyjny jest pogląd, że bank uzyskuje własność deponowanych pieniędzy (wyrok Sądu Najwyższego z 13 lutego 2004 r., sygn. akt IV CK 40/03, Legalis nr 66917; wyrok Sądu Apelacyjnego w Krakowie z 5 lutego 2014 r., sygn. akt I ACa 917/12, Legalis nr 1093113; wyrok Sądu Apelacyjnego w Poznaniu z 27 października 2010 r., sygn. akt I ACa 733/10, Legalis nr 270878). Zgodnie z treścią art. 726 k.c. bank może obracać czasowo wolne środki pieniężne zgromadzone na rachunku bankowym z obowiązkiem ich zwrotu w całości lub w części na każde żądanie, chyba że umowa uzależnia obowiązek zwrotu od wypowiedzenia. Wynikające z umowy uprawnienie posiadacza rachunku stanowi wierzytelność do banku każdorazowo wymagalną, a jej rozmiary wskazuje stan konta.

Z chwilą realizacji wierzytelności, przez zwrot środków pieniężnych, posiadacz rachunku odzyskuje ich posiadanie i także własność, bądź inne prawo rzeczowe lub obligacyjne, które było z nimi związane przed zdeponowaniem.

Reasumując mimo wyłudzenia przez osobę nieuprawnioną mienia stanowiącego własność banku, nie dojdzie do powstania szkody po stronie posiadacza rachunku, gdyż bank nadal pozostanie zobowiązany do zaspokojenia jego wierzytelności w pełnej wysokości ze swoich środków. Ochronę wierzytelności gwarantują posiadaczowi przepisy prawa cywilnego, finansowego i oparta na nich umowa z bankiem (postanowienie Sądu Najwyższego z 28 kwietnia 2016 r., sygn. akt I KZP 3/16, Legalis nr 1442847). Ze swojego długu wobec posiadacza rachunku bank nie zwolni się nawet wtedy, gdy dochowa należytej staranności przy dokonywaniu wypłaty osobie nieuprawnionej.

Tym samym zapewnienie bezpieczeństwa depozytów jest jednym z najistotniejszych obowiązków banku, a sposób jego wykonywania jest najbardziej wymierną podstawą oceny jego wiarygodności, w związku z czym wszelkie próby interpretacji przez banki postanowień zawartych w stosowanych przez nie wzorcach umownych, zmierzające do zaniżania standardów bezpieczeństwa powierzonych bankowi środków pieniężnych, powinny być oceniane jako zachowania sprzeczne z dobrymi obyczajami i celem umowy rachunku bankowego (zob. wyrok Sądu Najwyższego z 14 kwietnia 2003 r., sygn. akt I CKN 308/01, Legalis nr 61218).

Ryzyko dokonania wypłaty z rachunku bankowego do rąk osoby nieuprawnionej oraz dokonanie rozliczenia pieniężnego na podstawie dyspozycji wydanej przez osobę nieuprawnioną obciąża bank, także w sytuacji objęcia umowy rachunku bankowego bankowością internetową. Wynika to z tego, iż równoległą podstawą odpowiedzialności banku – strony pozwanej jest ustawa z 19 sierpnia 2011 r. o usługach płatniczych. Ustawa ta była kilkakrotnie nowelizowana do dnia wyrokowania. Zgodnie jednak z art. 3 k.c. ustawa nie ma mocy wstecznej, chyba że to wynika z jej brzmienia lub celu. W nowelizowanych przepisach nie przewidziano norm temporalnych. W konsekwencji nowe prawo co do zasady, nie modyfikuje sytuacji prawnych (praw i obowiązków) ukształtowanych przed jego wejściem w życie. Skutki dawnych zdarzeń prawnych należy generalnie ustalać przy zastosowaniu norm obowiązujących w chwili, w której do nich doszło. Dlatego przepisy wskazanej wyżej ustawy, których treść została zmieniona powoływane będą w brzmieniu z dnia, kiedy doszło do nieautoryzowanych transakcji.

Zgodnie z przepisami wskazanej wyżej ustawy na stronie pozwanej jako dostawcy wydającymemu instrument płatniczy ciążył na mocy art. 43 pkt 1 tej ustawy, obowiązek zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, na powódce natomiast - jako użytkownikowi instrumentu płatniczego - spoczywał obowiązek korzystania z instrumentu płatniczego zgodnie z umową oraz zgłaszania niezwłocznie dostawcy utraty, kradzieży, przywłaszczenia albo nieuprawnionego dostępu do tego instrumentu. (art. 42 ust. 1 pkt 1 i 2 ww. ustawy). Użytkownik, z chwilą otrzymania instrumentu płatniczego, winien podejmować niezbędne środki, zapobiegające naruszeniu indywidualnych zabezpieczeń instrumentu, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nie udostępniania go osobom nieuprawnionym. (art. 42 ust. 2 ww. ustawy)

Z okoliczności sprawy wynika, iż powódka nie autoryzowała przedmiotowych transakcji, zostały one dokonane przez osoby trzecie wbrew jej wiedzy i woli. Udostępnienie przez powódkę za pośrednictwem podstawionej witryny internetowej swoich danych identyfikacyjnych oraz hasła osobom nieuprawnionym umożliwiło tym osobom zalogowanie się do konta powódki i dokonanie przestępstwa polegającego na przelaniu znajdujących się na jej rachunku środków pieniężnych na inne konto bez jej wiedzy i woli. Czynności te z punktu widzenia systemu informatycznego banku zostały wykonane poprawnie przy wykorzystaniu właściwych narzędzi autoryzacyjnych. Mimo tego transakcji tych nie można uznać za transakcje autoryzowane w rozumieniu art. 40 ust. 1 ww. ustawy. Podkreślić w tym miejscu trzeba, że powódkę nie mogły wiązać te postanowienia regulaminu, które były dla niej mniej korzystne niż przepisy ustawy o usługach płatniczych. Zgodnie bowiem z treścią art. 8 ust. 1 ustawy o usługach płatniczych postanowienia umów o usługi płatnicze oraz umów o wydanie pieniądza elektronicznego nie mogą być mniej korzystne dla użytkowników i posiadaczy pieniądza elektronicznego niż przepisy ustawy, chyba że ustawa stanowi inaczej. Postanowienia umów o usługi płatnicze oraz umów o wydanie pieniądza elektronicznego

mniej korzystne dla użytkowników i posiadaczy pieniądza elektronicznego niż przepisy ustawy są nieważne zamiast nich stosuje się odpowiednie przepisy ustawy (art. 8 ust. 2 ustawy o usługach płatniczych). Wprowadzenie tym samym przez pozwanego Banku mniej korzystnych dla klienta regulacji niż ustawowe stanowi naruszenie przepisu art. 8 ust. 1 ustawy o usługach płatniczych, prowadząc do nieważności regulaminowych postanowień w zakresie w jakim przewidywały, że wszelkie dyspozycje złożone w formie elektronicznej przez osobę, która została prawidłowo zweryfikowana, są traktowane jako dyspozycje klienta lub ustanowionego użytkownika.

Powódka nie wyraziła zgody na wykonanie kwestionowanych transakcji, o czym świadczy jej natychmiastowa reakcja po ich wykryciu, w postaci niezwłocznego zawiadomienia strony pozwanej oraz zawiadomienia Policji o popełnieniu przestępstwa, wypełniając tym samym obowiązek o którym mowa w art. 44 ustawy. Zgodnie bowiem z art. 44 ust. 1 i 2 cytowanej ustawy użytkownik niezwłocznie powiadamia dostawcę o stwierdzonych nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcjach płatniczych (ust. 1). Jeżeli użytkownik nie dokona powiadomienia, o którym mowa w ust. 1, w terminie 13 miesięcy od dnia obciążenia rachunku płatniczego albo od dnia, w którym transakcja miała być wykonana, roszczenia użytkownika względem dostawcy z tytułu nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcji płatniczych wygasają (ust. 2).

Zgodnie natomiast z treścią art. 46 ust. 1 powołanej ustawy, w brzmieniu z dnia dokonania nieautoryzowanych transakcji, z zastrzeżeniem art. 44 ust. 2, w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany niezwłocznie zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, a w przypadku gdy płatnik korzysta z rachunku płatniczego, przywrócić obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

Przepis art. 45 ust. 1 i 2 powołanej ustawy, w brzmieniu z dnia dokonania nieautoryzowanej transakcji, stanowi, że ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika (ust. 1). Wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana. Dostawca jest obowiązany udowodnić inne okoliczności wskazujące 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. (ust. 2).

Ponadto stosownie do dyspozycji przepisu art. 46 ust. 3 ustawy o usługach płatniczych, w brzmieniu z dnia dokonania nieautoryzowanych transakcji, płatnik (w niniejszej sprawie powódka) 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 przywołanej ustawy.

Należy również mieć na uwadze, że zobowiązanie banku względem posiadacza rachunku kształtuje również przepis art. 50 ust. 2 ustawy z 29 sierpnia 1997 r. - Prawo bankowe, który stanowi, iż bank jest zobowiązany do dołożenia szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. W ocenie Sądu w niniejszym przypadku Bank nie dołożył szczególnej staranności w tym zakresie. Wprowadzając możliwość utworzenia szablonu zaufanego odbiorcy na podstawie jednego kodu autoryzacyjnego, nie zapewnił należytych zabezpieczeń. W konsekwencji nieuprawniona osoba mogła dokonywać wiele transakcji opiewających na znaczne kwoty, nawet w krótkich odstępach czasu, bez dokonywania dodatkowych autoryzacji za pomocą karty kodów. W tej sytuacji zabezpieczenia w postaci karty kodów do autoryzacji transakcji były całkowicie nieskuteczne i nie spełniały swojej roli. Należy jednocześnie dodać, że takich przypadków - jak w rozpoznawanej sprawie - było w pozwanym Banku znacznie więcej, co świadczy o tym, że zabezpieczenia stosowane przez stronę pozwaną nie były właściwe. Ponadto sam fakt, że w wyniku powyższych zdarzeń strona pozwana zmodyfikowała zabezpieczenia transakcji dokonywanych za pośrednictwem szablonu zaufanego odbiorcy, świadczy o tym, że zabezpieczenia stosowane u strony pozwanej były niewystarczające.

W ocenie Sądu powódka jako klientka strony pozwanej nie naruszyła obowiązków, o których mowa w art. 42 ustawy o usługach płatniczych umyślnie lub wskutek rażącego niedbalstwa. Powódka logowała się na stronę Banku zazwyczaj z komputera służbowego, który był wyposażony w aktualne oprogramowanie antywirusowe. Jednocześnie powódka nie udostępniła nikomu danych pozwalających zalogować się do jej rachunku bankowego drogą elektroniczną, a także nie podawała nikomu hasła logowania do Banku. Nie sposób przypisać jej rażącego niedbalstwa także dlatego, iż w toku postępowania stwierdzono faktyczny brak możliwości określenia sposobu, w jaki osoby, które zrealizowały sporny przelew bankowy uzyskały dostęp do danych pozwalających na dostęp do bankowości elektronicznej powódki. Nie wykazane więc zostało na czym miałyby polegać umyślność czy rażące niedbalstwo powódki. Wersja zdarzeń zaprezentowana przez biegłego w opinii, jest jedynie hipotetyczną wersją zdarzeń. Nawet gdyby wersja ta okazała się zgodna z prawdą, to nie pozwalałoby to na przyjęcie, że działania powódki nosiło znamiona umyślności czy rażącego niedbalstwa. Sposób działania sprawcy, był na tyle zorganizowany, że powódka miała małe możliwości na zapobieżenie przestępstwu. Podanie bowiem loginu i hasła na fałszywej stronie logowania należy uznać za dopuszczalny błąd w obliczu podmienionej strony, trudnej do zweryfikowania w pierwszym momencie. Jedyne zaniedbanie można by dopatrzeć się w podaniu przez powódkę podczas logowania konkretnego jednorazowego kodu autoryzacyjnego, w sytuacji kiedy na stronie logowania strona pozwana informuje, że nie jest to nigdy wymagane. Jednakże brak jest podstaw do zakwalifikowania go jako rażącego niedbalstwa, w sytuacji, gdy nie zostało ustalone w jaki sposób doszło do wyprowadzenia środków z konta powódki. Ponadto na korzyść powódki przemawia również to, że w sytuacji pojawienia się błędów podczas prób logowania, natychmiast podjęła ona kroki celem zmiany danych do logowania, co jednak nie uchroniło jej od nieuprawnionej utraty środków.

Tym samym powódka nie naruszyła obowiązków, o których mowa w art. 42 ustawy o usługach płatniczych, a co za tym idzie - jako bezzasadne jawiło się twierdzenie pozwanego, że powódka przyczyniła się do powstania szkody. Tym bardziej, że w toku prowadzonego postępowania - jak już wyżej wskazano - nie udało się ustalić dokładnego sposobu działania osób, które doprowadziły do wyprowadzenia środków pieniężnych zgromadzonych na rachunku bankowym należącym do powódki, a wyłącznie konkretne ustalenia mogły stanowić podstawę ku temu, aby ocenić, czy - a jeżeli tak, to w jakim zakresie - powódka przyczyniła się do powstania szkody po stronie Banku. Ciężar dowodu w tym zakresie spoczywał na pozwanym, który nie sprostał obowiązkowi nałożonemu na niego z mocy art. 6 k.c. Jednocześnie powódka spełniła wynikający z art. 42 ust. 1 punkt 2 ustawy o usługach płatniczych obowiązek niezwłocznego zawiadomienia o zaistnieniu nieautoryzowanej transakcji płatniczej. Dlatego też pozwany Bank, stosownie do dyspozycji przepisu art. 46 ust. 1 ustawy o usługach płatniczych, był zobowiązany niezwłocznie zwrócić stronie powodowej kwotę nieautoryzowanej transakcji płatniczej w łącznej wysokości 108 655 zł.

Na marginesie należy wskazać, iż Sąd rozważał, aby dochodzoną przez powódkę kwotę ewentualnie pomniejszyć o wysokość jedynie pierwszej z nieautoryzowanych transakcji. Powódka bowiem bezspornie udostępniła tylko jeden z kodów z karty zdrapki, co powinno umożliwić dokonanie wyłącznie jednego z nieautoryzowanych przelewów. Tylko w tym przypadku można by rozważać dopuszczenie się przez powódkę niedbalstwa. W pozostałym zakresie odpowiedzialność za nieautoryzowane transakcje ponosi jednoznacznie bank, skoro wprowadził możliwość dokonywania dowolnej liczby transakcji autoryzowanych tylko jednym kodem za pomocą tzw. „szablonu zaufanego odbiorcy”. Z uwagi na jednoznaczne brzmienie art. 46 ust. 3, oraz brak w zachowaniu powódki niedbalstwa w stopniu rażącym, Sąd ostatecznie doszedł do przekonania, że powództwo winno być jednak uwzględnione w całości.

Wobec tego należało zasądzić od strony pozwanej na rzecz powódki całą dochodzoną pozwym kwotę.

W zakresie żądania odsetkowego Sąd uznał, iż stosownie do przepisu art. 481 § 1 k.c., jeżeli dłużnik opóźnia się ze spełnieniem świadczenia, wierzyciel może żądać odsetek za czas opóźnienia, choćby nie poniósł żadnej szkody i chociażby opóźnienie było następstwem okoliczności, za które dłużnik odpowiedzialności nie ponosi. Stosownie do dyspozycji przepisu art. 46 ust. 1 ustawy o usługach płatniczych pozwany Bank miał obowiązek niezwłocznego zwrotu kwoty nieautoryzowanych transakcji. Przyjmuje się, iż termin „niezwłocznie” oznacza termin realny, mający na względzie okoliczności miejsca i czasu. W ocenie Sądu żądanie przyznania odsetek od zasądzonej należności głównej

w terminie 30 dni od dnia złożenia przez powódkę reklamacji dotyczących nieautoryzowanych transakcji jest zasadne w okolicznościach sprawy. Powódka zgłosiła reklamację 03.06.2015 r., a więc odsetki od zasądzonej kwoty należało liczyć od 04.07.2015 r.

O kosztach procesu Sąd orzekł na podstawie art. 98 §1 i §3 w zw. z art. 99 k.p.c. zasądzając je w całości od strony pozwanej na rzecz powódki, jako strony wygrywającej proces. Koszty jakie poniosła powódka stanowią opłatę od pozwu w kwocie 5 433 zł, a także koszty zastępstwa procesowego w kwocie 5 400 ustalone na podstawie §2 pkt 6) Rozporządzenie Ministra Sprawiedliwości z dnia 22 października 2015 r. w sprawie opłat za czynności radców prawnych. Łącznie koszty te wyniosły 10 833 zł.

O kosztach sądowych nieuiszczonych przez żadną ze stron Sąd orzekł na podstawie art. 113 ust. 1 ustawy o kosztach sądowych w sprawach cywilnych. Koszty te stanowiły kwotę 1012,27 zł jako część wynagrodzenia biegłego wypłaconego tymczasowo ze środków Skarbu Państwa. Stosując odpowiednio zasady obowiązujące przy zwrocie kosztów procesu, Sąd nakazał pobrać całą tę kwotę od strony pozwanej na rzecz Skarbu Państwa – Sądu Okręgowego w Bielsku-Białej.