Sygn. akt II C 342/17

UZASADNIENIE

Pozwem z 20 lutego 2017r. Powiat (...) – Powiatowy Urząd Pracy w K. wystąpił przeciwko Bankowi (...) Spółka Akcyjna z siedzibą w W. o zasądzenie na jego rzecz kwoty 89.538,96 zł wraz z odsetkami ustawowymi od dnia 19 września 2015 r. do dnia 31 grudnia 2015 r. oraz z odsetkami ustawowymi za opóźnienie od dnia 1 stycznia 2016 r. do dnia zapłaty oraz o zasądzenie od pozwanego na jego rzecz zwrotu kosztów procesu (pozew – k. 3-7; pismo, k. 57).

W odpowiedzi na pozew pozwany Bank (...) Spółka Akcyjna z siedzibą w W. wniósł o oddalenie powództwa w całości i o zasądzenie kosztów postępowania, w tym kosztów zastępstwa adwokackiego według norm przepisanych (odpowiedź na pozew k. 63-68).

Sąd Okręgowy ustalił następujący stan faktyczny:

W dniu 12 kwietnia 2010 r. Powiatowy Urząd Pracy w K. zawarł z Bankiem (...) S.A. z siedzibą w W. umowę kompleksową Pakietu (...)

W ramach zawartej umowy pozwany zobowiązał się do prowadzenia m.in. rachunku Funduszu Pracy o numerze: (...). W ramach łączącej strony umowy powód korzystał z udostępnionego przez pozwanego elektronicznego dostępu do rachunku bankowego za pośrednictwem internetu ((...)). Zgodnie z § 7 ust 2. umowy powód potwierdził otrzymanie Regulaminu „system Bankowości Internetowej (...) dla (...) Banku (...) S.A." oraz oświadczył, ze zapoznał się z jego treścią i uznał jego wiążący charakter (okoliczności bezsporne; umowa, k. 10-11v.; regulamin systemu bankowości internetowej, k. 13-16).

Zgodnie z Regulaminem systemu Bankowości Internetowej (...) dla (...) Banku (...) S.A. :

- Użytkownik zobowiązany jest z należytą starannością chronić hasło startowe, hasło logowania, identyfikator, klucz oraz hasło podpisu elektronicznego, a także kody autoryzacyjne otrzymywane za pośrednictwem SMS i skutecznie zabezpieczać je przed dostępem osób trzecich (§ 18 ust 2).

- W przypadku wystąpienia podejrzeń, że osoba trzecia weszła w posiadanie któregokolwiek z instrumentów uwierzytelniających, Użytkownik powinien niezwłocznie dokonać jego zmiany lub zgłosić Bankowi blokadę dostępu do systemu (§ 18 ust. 3).

- Dyspozycja złożona przez użytkownika za pośrednictwem Systemu (...) i prawidłowo uwierzytelniona jest traktowana jak pisemna dyspozycja osoby uprawnionej do dysponowania środkami zgromadzonymi na rachunku klienta (§ 21 ust. 1).

- Realizacja dyspozycji złożonych za pośrednictwem Systemu (...) następuje automatycznie, z zastrzeżeniem ust. 2. i 3. , bez możliwości ich odwołania – z wyjątkiem dyspozycji złożonych z przyszłą datą realizacji (§ 25 ust. 1).

- Bank nie ponosi odpowiedzialności za szkody spowodowane nieprawidłowym funkcjonowaniem sprzętu i sieci komputerowej u Klienta oraz sieci operatorów zewnętrznych, a także działaniami Klienta i/lub Użytkowników niezgodnymi z Umową lub z obowiązującymi przepisami prawa (§ 43 ust.1).

- Klienta obciążają operacje dokonane przez osoby, którym ujawnił informacje dotyczące funkcjonalności Systemu (...), mogące spowodować brak skuteczności mechanizmów zapewniających bezpieczeństwo zlecanych operacji (§ 43.2) (regulamin, k. 13-16).

W 2013 roku system bankowości internetowej pozwanego przewidywał kilka możliwości autoryzacji przelewów, o której decydował klient. Możliwe było korzystanie z klucza, z podpisu elektronicznego, można też było ustalić schematy akceptacji, tj. wybrać jakie osoby muszą autoryzować przelewy (np. wymagany będzie podpis więcej niż jednej osoby).

Bank nie miał dostępu do komputera klienta. System bankowy generował automatycznie niezbędne informacje dotyczące bezpieczeństwa użytkownika. Komunikaty ostrzegawcze pojawiały się w systemie cyklicznie. Komunikaty o bezpieczeństwie pojawiały się też po zalogowaniu użytkownika. W systemie była też zakładka "bezpieczeństwo" ze wszystkimi najważniejszymi informacjami o bezpieczeństwie dla użytkownika (zeznania świadków: M. S., k. 404-405 – od 03:07:44 i k. 405v. – od 03:31:34, A. B., k. 403v.-404v. – od 02:41:07).

W dniu 15 października 2013 r. pracownicy Działu Finansowo - Księgowego Powiatowego Urzędu Pracy w K. korzystając z rachunku bankowego urzędu poprzez system bankowości internetowej pozwanego banku ujawnili fakt złożenia dyspozycji: 5 przelewów w polskich złotych na łączną kwotę 71.074,58 zł oraz 4 przelewów walutowych w łącznej wysokości 25.787 euro. Łączna kwota dokonanych przelewów (po przeliczeniu na złotówki) wynosiła około 182.595,62 zł

Przedmiotowe przelewy nie zostały złożone do wykonania przez pracowników powoda, lecz przez niezidentyfikowane osoby trzecie. Jeden z przelewów udało się usunąć, natomiast osiem przelewów zostało skierowanych do realizacji (historia operacji, k. 17-18; oświadczenie, k. 19-21; zeznania świadków: U. W., k. 398-400 – od 00:11:13 do 01:13:42 i k. 402v. – 02:11:54, E. D., k. 400-401 – od 01:16:44 do 01:27:15, A. R., k. 401-402v. -01:33:37-02:02:35; reklamacje, k. 22-29; korespondencja, k. 87-96).

Dnia 15 października 2013 r., jeden z pracowników Powiatowego Urzędu Pracy w K. przygotował przelewy. Około godziny 8:30 U. W. – główna księgowa - weszła na stronę internetową pozwanego banku, zalogowała się do komputera i sytemu bankowego na swój login i hasło. Włożyła kartę do czytnika i wpisała PIN. Po wpisaniu numeru PIN, komputer „wyrzucił ją" z systemu bankowego. Pojawił się czarny ekran na monitorze. Informatyk Powiatowego Urzędu Pracy w K. stwierdził, że coś się dzieje z jej komputerem. U. W. chciała ponownie wejść do systemu bankowego celem wykonania przelewów. Ponownie wpisała dane do logowania, ale nie mogła wejść do systemu transakcyjnego, próbowała kilkukrotnie. Po kilku nieudanych próbach zrezygnowała z dalszego logowania. Około godziny 13:00 ponownie próbowała wejść do systemu bankowości elektronicznej, zalogowała się, kontynuowała procedurę, po włożeniu karty i wpisaniu PIN, została „wyrzucona" ze strony banku. Po raz trzeci taka sytuacja powtórzyła się o godzinie 14:00. Ostatecznie inny pracownik wykonał przelewy. Około 14:30 jeden z pracowników urzędu wszedł na konto bankowe i odkrył przelewy, które nie były zlecane przez pracowników Powiatowego Urzędu Pracy w K. (zeznania świadków: U. W., k. 398-400 – od 00:11:13 do 01:13:42 i k. 402v. – 02:11:54, E. D., k. 400-401 – od 01:16:44 do 01:27:15, A. R., k. 401-402v. -01:33:37-02:02:35).

Każdy z 9 spornych przelewów był zlecony, zaakceptowany i wysłany z konta pracownika powoda - U. W. – Głównej Księgowej Powiatowego Urzędu Pracy w K.. Do wykonania tych przelewów użytkownik zalogował się z komputera o IP, z którego najczęściej korzystał. Użytkownik ten wpisał odpowiednie części hasła. Dnia 15 października 2013 tych logowań było około 9-10. Podczas tych logowań dokonywano transakcji w schemacie jednoosobowym. Do zatwierdzenia tych przelewów podano odpowiednie narzędzie autoryzacyjne. W przypadku tego zdarzenia karta została włożona do czytnika, został wpisany poprawny PIN i klucz prawidłowo został sczytany i te transakcje zostały nim podpisane. Zgadzały się wszystkie czynności i narzędzia autoryzacyjne służące dokonaniu przelewu. Po stronie banku nie wykryto w tym procesie anomalii (historia operacji, k. 17-18; oświadczenie, k. 19-21; zeznania świadka M. S., k. 404-405 – od 03:07:44 do 03:24:23 i k. 405v. – od 03:31:34).

W przypadku gdy zostały spełnione wszystkie wymagane do uwierzytelnienia operacji warunki (np. autoryzacja kartą), system bankowy traktował to jako prawidłowe zlecenie (opinia biegłego informatyka, k. 432-445).

Powiatowy Urząd Pracy w K. tego samego dnia – 15 października 2013 r. (około godziny 14:30), w którym dokonano przelewów, zawiadomił Bank (...) S.A. (...) Oddział w K. o zaistniałym zdarzeniu oraz złożył reklamacje. Jednocześnie w siedzibie (...) Oddziału Banku (...) S.A. w K. odbyło się spotkanie, w którym wieli udział: U. W. i A. R. — ze strony powoda oraz M. S. - dyrektor w/w oddziału i A. B. - ze strony pozwanego. Zablokowano konto użytkownika przypisane U. W. (reklamacje, k. 22-29; korespondencja, k. 87-96; zeznania świadków: M. S., k. 404-405 – od 03:07:44 i k. 405v.

– od 03:31:34, A. B., k. 403v.-404v. – od 02:41:07, U. W., k. 398-400 – od 00:11:13 do 01:13:42 i k. 402v. – 02:11:54, E. D., k. 400-401 – od 01:16:44 do 01:27:15, A. R., k. 401-402v. -01:33:37-02:02:35).

W dniu 16 października 2013 r. Powiatowy Urząd Pracy w K. zawiadomił o podejrzeniu popełnienia przestępstwa w zakresie wyłudzenia środków z jego rachunku bankowego. Na powyższą okoliczność prowadzone było postępowanie karne przez Prokuraturę Rejonową w Kutnie pod sygn. akt: Ds. 1983/13 (Ds. 1122/15).

Z wydanego w dniu 3 lutego 2014 r. postanowienia Policji Republiki Czeskiej wynika, że zgodnie z informacją przekazaną przez I. W., do dokonania przelewów doszło, ponieważ „sprawca złamał zabezpieczenie internetowe urzędu".

Komenda Powiatowa Policji w K. za nr PG 780/17 pod nadzorem Prokuratury Rejonowej w Kutnie, sygn. akt DS. 1817/2017 prowadzi postępowanie w sprawie niedopełnienia obowiązków przez Dyrektora Powiatowego Urzędu Pracy w K. oraz Głównego Księgowego Powiatowego Urzędu Pracy w K. polegających na niedostatecznym nadzorze nad bezpieczeństwem środków pieniężnych znajdujących się na rachunku bankowym Powiatowego Urzędu Pracy w K. czym wyrządzili szkodę PUP w K. w wysokości 89.538,96 zł tj. o czyn określony w art. 231 § 1 k.k. (zawiadomienie, k. 30-31; pismo, k. 32; kserokopia akt, k. 126-326; kserokopia akt, k. 327-384; pismo, k. 462).

Pismem z dnia 14 stycznia 2014 r. Bank poinformował powoda o zwróceniu na rachunek łącznej kwoty 71.074,58 zł.

W Republice Czeskiej ujawniono, że ustalone osoby pobrały z tamtejszego banku środki finansowe przekazane z rachunku bankowego Powiatowego Urzędu Pracy w K.. W związku z tym PUP w K. pismami z dnia 8 maja 2015 r., 12 czerwca 2015 r. i 17 lipca 2015 r. zwracał się do policji w Czechach o przekazanie zajętych środków. W dniu 17 sierpnia 2015 r. Na rachunek bankowy urzędu wpłynęła przekazana z Czech kwota 21.982,08 zł (tj. 147.510,68 koron czeskich) (pismo, k. 33; pisma, k. 34-36; przetłumaczona kserokopia postanowienia, k. 37-43; potwierdzenie wykonania operacji, k. 47)

W Powiatowym Urzędzie Pracy w K. monitorowano pracowników w zakresie korzystania przez nich z komputerów służbowych. Większość pracowników miała zablokowany dostęp do internetu, w tym do prywatnej poczty elektronicznej. Jedynie: dyrektor, zastępca dyrektora, główny księgowy i informatyk mieli możliwość korzystania z prywatnej poczty elektronicznej, a także nie mieli zablokowanego dostępu do internetu. Natomiast pozostali pracownicy mieli zablokowany dostęp do większości stron.

W urzędzie korzystano z płyt CD i pendrive'ów. Nie podlegały one kontroli pod kątem obecności złośliwego oprogramowania. Można było korzystać też z prywatnych nośników danych. Dyrekcja uznała, że skoro są zabezpieczenia, to one udaremnią zainstalowanie niewłaściwego oprogramowania. Pracownicy korzystali z prywatnych nośników danych (pendrive), chociaż przekazano im służbowe nośniki danych.

Na komputerach pracowników było zainstalowane oprogramowanie antywirusowe, które było co jakiś czas sprawdzane (tj. czy się nie wyłączyło, czy ściąga aktualne sygnatury). W Urzędzie znajduje się około 120 komputerów, pod kątem zainfekowania wirusami, informatyk sprawdzał w tygodniu około 5 komputerów.

Pracownicy zostali przeszkoleni jak mają dokonywać przelewów (zeznania świadków: U. W., k. 398-400 – od 00:11:13 do 01:13:42 i k. 402v. – 02:11:54, E. D., k. 400-401 – od 01:16:44 do 01:27:15, A. R., k. 401-402v. -01:33:37-02:02:35, M. M., k. 482v.-484 – od 00:05:18).

W Powiatowym Urzędzie Pracy w K. uprawnienia do dokonywania przelewów miało kilka osób. Użytkownicy byli podzieleni na dwie grupy, jedni mogli przelewy dodawać, drudzy wykonywać przelewy, za wyjątkiem U. W., która mogła dodawać, edytować, akceptować/zatwierdzać i wykonywać/wysyłać przelewy (jako jedyna w Powiatowym Urzędzie Pracy w K.). By dokonać przelewu należało się zalogować się na stronę wpisać hasło, wypełnić dane przelewu, a podczas przelewu włożyć kartę, wpisać PIN. Liczba przelewów, które obsługiwała U. W. mogła wynosić nawet

700-800 dziennie. (zeznania świadków: U. W., k. 398-400 – od 00:11:13 do 01:13:42 i k. 402v. – 02:11:54, E. D., k. 400-401 – od 01:16:44 do 01:27:15, A. R., k. 401-402v. -01:33:37-02:02:35, M. M., k. 482v.-484 – od 00:05:18).

U. W. w 2013 roku pracowała w Powiatowym Urzędzie Pracy w K. na stanowisku głównego księgowego. Miała przekazany od pracodawcy indywidualny komputer, do którego nie miały dostępu inne osoby. U. W. korzystała w godzinach pracy z komputera do prywatnych celów. Sprawdzała prywatną pocztę, korzystała z internetu, wchodziła na strony internetowe nie związane z pracą ((...)). U. W. korzystała w pracy z prywatnych nośników danych (pendrive) (zeznania świadków: U. W., k. 398-400 – od 00:11:13 do 01:13:42 i k. 402v. – 02:11:54, E. D., k. 400-401 – od 01:16:44 do 01:27:15, A. R., k. 401-402v. -01:33:37-02:02:35).

Po wydarzeniu z 15 października 2013 r. w Powiatowym Urzędzie Pracy w K. zmieniono sposób autoryzacji przelewów, tj. podzielono użytkowników na trzy grupy. By przelew był dokonany potrzebne były podpisy trzech osób. Dodatkowo zablokowano przelewy w walucie Euro (zeznania świadka: M. M., k. 482v.-484 – od 00:05:18).

Na komputerze U. W. znajdowało się w dniu 15 października 2013 r. złośliwe oprogramowanie, które mogło posłużyć do wykonywania przelewów przez osoby trzecie (opinia biegłego informatyka, k. 432-445; pisemna uzupełniająca opinia biegłego informatyka, k. 476-477).

Zidentyfikowane złośliwe oprogramowanie, które znajdowało się na komputerze U. W., umożliwiało: - rejestrację naciskanych przez użytkownika przycisków myszki i klawiszy klawiatury wraz z informacją której aplikacji działania te dotyczą, celem uzyskania danych uwierzytelniających, autoryzujących oraz hasła do klucza, którym podpisywane są transakcje finansowe; - wywoływanie okien aplikacji, podmianę danych transakcji; - przesyłanie zarejestrowanych danych do serwerów kontrolowanych przez osoby trzecie; - sprawdzanie czy w czytniku kart znajduje się karta inteligentna; - zestawienie połączenia zdalnego dostępu do komputera; - pobieranie i instalowanie złośliwego oprogramowania, modyfikowanie ustawień systemowych.

Pliki tekstowe zawierające zarejestrowane dane (dane wpisywane przez użytkownika) mogły być, w ocenie informatycznej, wysyłane w określonych odstępach czasowych do „atakującego", tj. niepowołanej osoby trzeciej, sterującej ujawnionym złośliwym oprogramowaniem. Zapisywanie danych rozpoczęło się, na komputerze U. W., w dniu 7 października 2013 o godzinie 15:00 (data utworzenia pliku). Najpóźniejsza data modyfikacji ujawnionych plików wskazuje, na dzień 15 października 2013 o godzinie 14:27.

Złośliwe oprogramowanie posiadało możliwość obserwowania oraz przekazywania informacji dotyczących obecności karty inteligentnej. Może to wskazywać, iż wyłącznie wtedy gdy karta inteligentna była podłączona do komputera, nieuprawnione osoby mogły dokonywać przelewów (opinia biegłego informatyka, k. 432-445; pisemna uzupełniająca opinia biegłego informatyka, k. 476-477).

Na komputerze U. W. zainstalowano w dniu 6 kwietnia 2011 r. program antywirusowy (...). Program posiadał bazy wirusów aktualne na dzień 14 października 2013r. Zainstalowane oprogramowanie antywirusowe na komputerze Powiatowego Urzędu Pracy w K. dnia 8 października 2013 wykazało 45 plików zainfekowanych, natomiast dnia 15 października 2013, 500 plików zainfekowanych. Komputer był przez ten czas wciąż wykorzystywany do celów zawodowych.

Skanowanie dnia 8 października oraz 15 października 2013 roku, oprogramowaniem antywirusowym S. (...), ujawniło zagrożenie w części plików związanych z zainstalowanym oprogramowaniem szpiegowskim. Brak w plikach tekstowych logów jednoznacznej informacji co do wykonanych czynności wobec zainfekowanych plików. Jednakże, fakt iż oprogramowanie wykryło zagrożenie winno, w ocenie informatycznej, skutkować niezwłocznym zaprzestaniem użytkowania oraz wyłączeniem urządzenia, a następnie przekazaniem go specjaliście IT. Zgodnie z ogólnie przyjętymi dobrymi praktykami bezpieczeństwa, w obliczu wykrycia zagrożenia lub informacji mogących wskazywać na obecność zagrożenia, należy zapewnić pracownikowi komputer zastępczy, zainfekowaną maszynę niezwłocznie odłączyć od sieci Internet oraz sieci przedsiębiorstwa, a następnie specjalista IT winien dokonać analizy i likwidacji zagrożenia oraz sprawdzenia pozostałych elementów infrastruktury teleinformatycznej przedsiębiorstwa pod kątem ewentualnych

innych infekcji bądź przełamania zabezpieczeń (opinia biegłego informatyka, k. 432-445; pisemna uzupełniająca opinia biegłego informatyka, k. 476-477).

W ocenie informatycznej, fakt obecności złośliwego oprogramowania na komputerze pracownika implikuje iż ogólnie przyjęte dobre praktyki bezpieczeństwa zostały naruszone w Powiatowym Urzędzie Pracy w K.. Nie zostały one dostatecznie wdrożone lub pracownicy nie zostali przeszkoleni, w zakresie bezpiecznego korzystania z komputera, poczty elektronicznej (ze szczególnym naciskiem na wiadomości oraz załączniki pochodzące z nieznanych źródeł), sieci Internet, reagowania na ewentualne zagrożenia.

Zachowania użytkownika (U. W.) takie jak odwiedzanie witryn niezwiązanych z wykonywaną pracą, korzystanie z prywatnej poczty elektronicznej, użytkowanie komputera pomimo wykrycia przez zainstalowane oprogramowanie antywirusa zainfekowanych plików oraz zaobserwowania niestandardowego zachowania podczas korzystania z bankowości internetowej można zakwalifikować jako naruszenie ogólnie przyjętych dobrych praktyk bezpieczeństwa (opinia biegłego informatyka, k. 432-445; pisemna uzupełniająca opinia biegłego informatyka, k. 476-477).

W ocenie informatycznej korzystanie z prywatnych nośników danych w instytucjach, przedsiębiorstwach zwiększa ryzyko infekcji złośliwym oprogramowaniem. Dobrą i powszechną praktyką bezpieczeństwa jest stosowanie tylko firmowych, zarejestrowanych, dopuszczonych do użytku w miejscu pracy nośników danych (np. typu pendrive). Zachowania użytkownika takie jak między innymi: otwieranie wiadomości poczty elektronicznej i załączników z niepotwierdzonych źródeł, odwiedzanie witryn internetowych niezwiązanych z wykonywaną pracą, zawierających nielegalne treści, korzystanie z prywatnej poczty elektronicznej i innych usług w miejscu pracy, używanie prywatnych urządzeń w miejscu pracy, nieaktualizowanie przeglądarek internetowych, oprogramowania antywirusowego, wtyczek i innych aplikacji mogą wpłynąć na zwiększenie niebezpieczeństwa zarażenia komputera oprogramowaniem szpiegowskim (opinia biegłego informatyka, k. 432-445).

Z punktu widzenia informatycznego, nie ujawniono informacji dotyczących sposobu, w jaki mogło zostać zainstalowane złośliwe oprogramowanie na komputerze U. W.. Mógł być to atak sprofilowany, to znaczy wymierzony w konkretne przedsiębiorstwa, instytucje i organizacje, o konkretnym celu. W przypadku wykorzystania luki bezpieczeństwa przed jej załataniem przez producenta, zagrożenie mogło być niewykrywane przez oprogramowanie antywirusowe, ze względu na brak sygnatur służących jego identyfikacji. Jedną z najczęstszych dróg infekcji jest również poczta elektroniczna poprzez otwieranie załączników i wiadomości spreparowanych bądź od nieznanych nadawców (opinia biegłego informatyka, k. 432-445; pisemna uzupełniająca opinia biegłego informatyka, k. 476-477).

W ocenie informatycznej, przypuszczalnie atakujący, posiadał dane uwierzytelniające oraz autoryzacyjne, hasło do klucza. Zakładając, że większość funkcjonalności ujawnionego złośliwego oprogramowania zadziałała poprawnie, atakujący otrzymywał również informacje o tym kiedy komputer jest włączony, a karta inteligentna obecna w systemie. Po zestawieniu zdalnego połączenia z badanym komputerem z wykorzystaniem ukrytego oprogramowania do przesyłania obrazu, a więc bez wiedzy użytkownika, atakujący w odpowiednim momencie przejmował kontrolę oraz wykonywał przelewy (opinia biegłego informatyka, k. 432-445; pisemna uzupełniająca opinia biegłego informatyka, k. 476-477).

Pismem z dnia 2 września 2015 r., nadanym w dniu 3 września 2015r., PUP w K. skierował do pozwanego wezwanie do zapłaty kwoty 89.538,96 zł, zakreślając 14-dniowy termin od daty otrzymania wezwania.

Pozwany pismem z dnia 9 października 2015 r. odmówił zapłaty, oświadczając, iż wezwanie do zapłaty wpłynęło do Banku w dniu 4 września 2015 r.

Powód 14 października 2015 r. skierował do Sądu Rejonowego dla Warszawy-Woli w Warszawie wniosek o zawezwanie do próby ugodowej (wezwanie, k. 54; odpowiedź, k. 49; wniosek, k. 50-51).

Ustalając powyższy stan faktyczny, Sąd oparł się na dowodach z zeznań świadków, opinii biegłego informatyka oraz z przedłożonych dokumentów, których treść nie była kwestionowana. Opinia biegłego ds. informatyki ostatecznie nie była kwestionowana przez żadną ze stron.

Sąd Okręgowy zważył, co następuje:

Powództwo podlegało oddaleniu w całości.

Roszczenie powoda znajduje oparcie w przepisach ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (t. jedn. Dz. U. z 2014 r., poz. 873 ze zm.). Przywołana ustawa określa między innymi prawa i obowiązki stron wynikające z umów o świadczenie usług płatniczych, a także zakres odpowiedzialności dostawców z tytułu wykonywania usług płatniczych (art. 1 pkt 2 ustawy). Bank krajowy jest dostawcą usług płatniczych w rozumieniu ustawy (art. 4 ust. 1 i ust. 2 pkt 1). Przez usługi płatnicze rozumie się działalność polegającą w szczególności na wykonywaniu transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy przez wykonywanie usług polecenia przelewu (art. 3 pkt 2 lit. c).

Płatnikiem w rozumieniu ustawy jest osoba fizyczna, osoba prawna oraz jednostka organizacyjną niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, składającą zlecenie płatnicze, czyli oświadczenie skierowane do dostawcy zawierające polecenie wykonania transakcji płatniczej (art. 2 pkt 22 i pkt 36). Zlecenie płatnicze, zgodnie z art. 2 pkt 10 ustawy, płatnik składa przy użyciu instrumentu płatniczego, którym jest zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego (art. 2 pkt 10).

Strony niniejszego postępowania umówiły się, że zgoda na wykonanie transakcji płatniczych za pośrednictwem usług bankowości elektronicznej świadczonych przez pozwany Bank będzie przez stronę powodową udzielana – po zalogowaniu się do konta za pomocą danych autoryzacyjnych (indywidualnej karty przypisanej do konkretnego pracownika, oraz kodu PIN).

Na pozwanym Banku jako dostawcy wydającemu instrument płatniczy ciążył z mocy art. 43 pkt 1 ustawy obowiązek zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, na stronie powodowej zaś - jako użytkowniku instrumentu płatniczego – spoczywał obowiązek korzystania z instrumentu płatniczego zgodnie z umową ramową oraz zgłaszania niezwłocznie dostawcy utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu (art. 42 ust. 1 pkt 1 i 2). W celu spełnienia powyższego obowiązku 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 nieudostępniania go osobom nieuprawnionym (art. 42 ust. 2).

Nadto strony łączył regulamin Bankowości Internetowej (...) dla (...) Banku (...) S.A. zgodnie, z którym na stronie powodowej ciążył obowiązek aby chronić hasło startowe, hasło logowania, identyfikator, klucz oraz hasło podpisu elektronicznego, a także kody autoryzacyjne otrzymywane za pośrednictwem SMS i skutecznie zabezpieczać je przed dostępem osób trzecich (§ 18 ust 2). Dyspozycja złożona przez użytkownika za pośrednictwem Systemu (...) i prawidłowo uwierzytelniona była zaś traktowana jak pisemna dyspozycja osoby uprawnionej do dysponowania środkami zgromadzonymi na rachunku klienta (§ 21 ust. 1).

W myśl art. 45 ustawy o usługach płatniczych, ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika lub że została wykonana prawidłowo, spoczywa na dostawcy tego użytkownika. 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.

Zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych oraz postanowieniami regulaminu stanowiącego integralną część łączącej strony umowy rachunku bankowego, 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.

Jeżeli jednak płatnik doprowadził do nieautoryzowanej transakcji umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42, odpowiada on za nieautoryzowane transakcje płatnicze w pełnej wysokości (art. 46 ust. 3).

Jak wynika z poczynionych ustaleń, pozwany Bank wywiązywał się z obowiązku zapewnienia, że indywidualne zabezpieczenia instrumentu płatniczego nie są dostępne dla osób innych niż użytkownik uprawniony do korzystania z tego instrumentu, strona powodowa natomiast swoim obowiązkom wymienionym w art. 42 ust. 1 i 2 ustawy uchybiła. W szczególności naruszone zostały w Powiatowym Urzędzie Pracy w K. dobre praktyki bezpieczeństwa. Nie wdrożono mechanizmów bezpiecznego korzystania z komputerów przez pracowników, poczty elektronicznej (ze szczególnym naciskiem na wiadomości oraz załączniki pochodzące z nieznanych źródeł), sieci Internet, reagowania na ewentualne zagrożenia. Główna Księgowa w godzinach pracy, na służbowym komputerze, otwierała prywatną pocztę, odwiedzała strony internetowe niezwiązane z pracą, a także używała prywatnego nośnika danych. Jednocześnie była jedyną osobą w urzędzie, która mogła jednoosobowo dokonywać przelewów. Takie ustawienie uprawnień dla tego szczególnego pracownika, jest co najmniej nierozważne. Przede wszystkim zaś pomimo wykrycia przez program antywirusowy zainfekowanych plików (już dnia 8 października 2013 r. było 45 zainfekowanych plików, a 15 października 2013r. już 500) nie poczyniono żadnych kroków celem wyeliminowania zagrożenia. Zatrudniony w jednostce informatyk, nie zrobił z informacją o zainfekowaniu komputera Głównej Księgowej, nic. Należało zaś niezwłocznie zaprzestać użytkowania zainfekowanego komputera, zapewnić pracownikowi komputer zastępczy, zainfekowaną maszynę natychmiast odłączyć od sieci Internet oraz sieci przedsiębiorstwa, a następnie specjalista IT winien dokonać analizy i likwidacji zagrożenia oraz sprawdzenia pozostałych elementów infrastruktury teleinformatycznej przedsiębiorstwa pod kątem ewentualnych innych infekcji bądź przełamania zabezpieczeń. Nie dokonano zatem elementarnych procedur bezpieczeństwa. Powyższe zaś skutkowało tym, że osoby trzecie, wyprowadziły środki pieniężne z konta powódki. Nadto nawet 15 października 2013 r. pracownicy nie zachowali się w sposób prawidłowy. Winni bowiem już w momencie pierwszych problemów z logowaniem do konta – około godziny 8:30 – niezwłocznie zgłosić taką okoliczność pozwanemu Bankowi. Natomiast jak wynika z z ustaleń Sądu, komputer U. W. był aktywny aż do 14:27 tego dnia. Również i w tym momencie naruszono warunki umowy i ustawy po stronie powodowej.

W ocenie Sądu szereg nieprawidłowości jakie wykazało postępowanie, jakie ujawniły się po stronie powodowej, wykazują, że doszło rażącego niedbalstwa w Powiatowym Urzędzie Pracy w K..

Jednocześnie z punktu widzenia banku zostały spełnione wszystkie wymagania do uwierzytelnienia operacji, autoryzacja kartą, zalogowanie się z komputera z IP takim jak zazwyczaj. Reasumując, czynności, dokonane dnia 15 października 2013 r., były z punktu widzenia systemu informatycznego Banku, przeprowadzone poprawnie, przy wykorzystaniu właściwych narzędzi autoryzacyjnych. Podkreślenia bowiem wymaga, że na dostawcy usług płatniczych spoczywa jedynie obowiązek weryfikacji numeru rachunku, nie zaś danych posiadacza rachunku, na którego rzecz ma nastąpić wpłata. Oznacza to, że w świetle obowiązujących przepisów bankowi nie można zarzucić niedochowania należytej staranności poprzez niesprawdzenie personaliów beneficjenta przelewu z danymi posiadacza rachunku. Zgodnie z przepisem art. 143 ustawy o usługach płatniczych Bank nie miał, żadnych podstaw do odmowy realizacji zleconych przelewów. Mając na uwadze powyższe nie można przypisać działaniom Banku cechy bezprawności. Skoro

nie można przypisać Bankowi bezprawności działania, które stanowi przesłankę winy, to również nie można przypisać pozwanemu winy. Nie ma zatem podstaw do przypisania pozwanemu odpowiedzialności odszkodowawczej.

Mając na uwadze powyższe regulacje i rozważania, Sąd powództwo oddalił w całości.

Z uwagi na to, że żądanie powoda zostało oddalone w całości, sąd o kosztach procesu rozstrzygnął na podstawie art. 98 § 1 i 3 k.p.c. Koszty poniesione przez stronę pozwaną wyniosły łącznie 6.417 zł (wynagrodzenie dla pełnomocnika wraz z opłatą od pełnomocnictwa – 5.417; wykorzystana zaliczka na wynagrodzenie biegłego – 1.000 zł). Wynagrodzenie pełnomocnika pozwanego ustalone zostało przez sąd z uwzględnieniem rodzaju i stopnia zawiłości sprawy oraz nakładu pracy pełnomocnika na podstawie § 2 ust. 6 rozporządzenia Ministra Sprawiedliwości z dnia 22 października 2015 r. w sprawie opłat za czynności adwokackie. (Dz.U.2015.1800 z dnia 2015.11.05). Ponieważ strona powodowa przegrała proces w całości, sąd zasądził od niej na rzecz pozwanego kwotę 6.417 zł tytułem zwrotu kosztów procesu.

O nieuiszczonych kosztach (brakująca część zaliczki na wynagrodzenie biegłego w wysokości 3.018,40 zł) sąd orzekł na podstawie art. 113 ustawy z dnia 28 lipca 2005 r. o kosztach sądowych w sprawach cywilnych (Dz.U.2010.90.594 j.t. ze zm.) z zastosowaniem w/w art. 98 k.p.c., nakazując pobrać od Powiatu (...) - Powiatowego Urzędu Pracy w K. na rzecz Skarbu Państwa Sądu Okręgowego w Łodzi kwotę 3.018,40 zł, uchylając jednocześnie punkt 3 postanowienia z dnia 31 stycznia 2018 r.