II CSKP 1013/22

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

15 września 2023 r.

Sąd Najwyższy w Izbie Cywilnej w składzie:

SSN Agnieszka Piotrowska (przewodniczący)
SSN Władysław Pawlak
SSN Roman Trzaskowski (sprawozdawca)

po rozpoznaniu na posiedzeniu niejawnym 15 września 2023 r. w Warszawie,
skargi kasacyjnej Banku […] spółki akcyjnej w W.
od wyroku Sądu Apelacyjnego we Wrocławiu
z 14 października 2020 r., I AGa 248/20,
w sprawie z powództwa J. B.
przeciwko Bankowi […] spółce akcyjnej w W.
o zapłatę,

uchyla zaskarżony wyrok i przekazuje sprawę Sądowi Apelacyjnemu we Wrocławiu do ponownego rozpoznania i rozstrzygnięcia o kosztach postępowania kasacyjnego.

(K.L.)

UZASADNIENIE

Wyrokiem z dnia 14 października 2020 r. Sąd Apelacyjny we Wrocławiu oddalił apelację pozwanego Banku […] S.A. w W. (dalej – „Bank”) od wyroku Sądu Okręgowego we Wrocławiu z dnia 8 lipca 2020 r., zasądzającego od Banku na rzecz powoda J.B. kwotę 77.776 zł wraz z odsetkami ustawowymi za opóźnienie od dnia 16 marca 2018 r. z tytułu odszkodowania za utratę środków na rachunku bankowym, i orzekł o kosztach postępowania apelacyjnego.

W sprawie ustalono m.in., że strony zawarły w dniu 8 października 2015 r. umowę ramową o korzystanie z produktów bankowych („Umowa”), w tym z rachunków bankowych. Uzgodniły, że w sprawach nieuregulowanych w Umowie zastosowanie znajdą zapisy regulaminu otwierania i prowadzenia rachunków bankowych dla klientów instytucjonalnych („Regulamin”), taryfy opłat i prowizji bankowych Banku [...] S.A. dla klientów instytucjonalnych („Taryfa opłat i prowizji”) oraz przepisy powszechnie obowiązującego w Polsce prawa. Korzystając z kompetencji przewidzianej w art. 16 oraz art. 33 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (obecnie tekst jedn. Dz.U. z 2022 r., poz. 2360 ze zm.: dalej – „u.u.p.”) przyjęły, że odpowiedzialność z tytułu niewykonania lub nienależytego wykonania zobowiązania uregulowana została w sposób wyczerpujący w Umowie, Regulaminie oraz Taryfie opłat i prowizji. W całości wyłączyły zastosowanie art. 17-32, art. 34-37, art. 40 ust. 3 i 4, art. 44, art. 45, art. 46 ust. 2-5, art. 47, art. 48, art. 51 oraz art. 114-146 u.u.p.

W ramach umowy J.B. uzyskał dostęp do systemu bankowości internetowej, systemu bankowości mobilnej, systemu obsługi telefonicznej i usługi SMS Kontakt. Bank za pomocą systemu bankowości elektronicznej udostępniał: informacje o stanie środków pieniężnych zgromadzonych na rachunkach bankowych, wykonywanie transakcji płatniczych, otwieranie i zarządzanie lokatami terminowymi. Zgodnie z zapisami Regulaminu użytkownicy powinni korzystać ze sprawnego sprzętu komputerowego z dostępem do sieci Internet oraz przeglądarki internetowej umożliwiającej stosowanie protokołu szyfrującego SSL. Sprzęt komputerowy

użytkowników powinien mieć zainstalowane i działające aktualne wersje systemu operacyjnego, przeglądarki internetowej oraz programów antywirusowych i programów typu „firewall”.

Autoryzacja odbywała się przez: podanie hasła jednorazowego w przypadku transakcji płatniczych i innych dyspozycji, które wymagają autoryzowania, jednorazowe wyrażenie zgody za pomocą hasła jednorazowego w przypadku transakcji płatniczych wykonywanych w formie zleceń stałych, jednorazowe wyrażenie zgody za pomocą hasła jednorazowego w przypadku transakcji płatniczych wykonywanych z użyciem szablonu (przelewów zdefiniowanych) lub na rzecz odbiorców, którzy oznaczeni zostali jako niewymagający każdorazowych autoryzacji.

Na wniosek powoda Bank otworzył i prowadził mu rachunek bankowy w walucie polskiej „[...]” o bliżej oznaczonym numerze („Rachunek bankowy”). W dniu 11 sierpnia 2017 r. powód złożył wniosek o dostęp do systemu bankowości internetowej „[x]” dotyczący tego Rachunku bankowego oraz uzyskał dostęp do systemu bankowości elektronicznej. Wybraną przez powoda metodą autoryzacji w systemie był SMS otrzymywany na telefon komórkowy powoda o oznaczonym numerze. Bank wysyłał do swoich klientów korzystających z bankowości elektronicznej, w tym również do powoda, wiadomości ostrzegające przed atakami hakerów oraz przypominające o zachowaniu zasad bezpiecznego korzystania z bankowości internetowej i mobilnej.

W dniu 15 marca 2018 r. miało miejsce przechwycenie przez nieustaloną osobę loginu i hasła powoda do systemu bankowości elektronicznej [x] oraz dokonanie nieautoryzowanych przez powoda trzech transakcji płatniczych. Nieustalona osoba (haker) najpierw przechwyciła kod SMS wysłany powodowi i wpisany przezeń w celu autoryzacji logowania (na fałszywej stronie), co umożliwiło hakerowi autoryzację i zalogowanie się na prawdziwe konto powoda. Następnie powód otrzymał na telefon komórkowy następny kod SMS, który haker ponownie przechwycił i wykorzystał do zmodyfikowania na koncie powoda zaufanego odbiorcy krajowego. O godzinie 9:42:03 z konta powoda wypłynęła kwota 38.788 zł, o godzinie 11:38:07 wypłynęła kwota 39.988 zł i o godzinie 14:49:22 wypłynęła kwota 39.688 zł.

Powód nie otrzymał żadnej wiadomości w czasie, gdy przelewy były wykonywane i nie miał możliwości weryfikacji odbiorcy tych przelewów. O godzinie 15:36:30 powód zalogował się na swój rachunek elektroniczny, co spowodowało automatyczne wylogowanie hakera z konta powoda. Powód stwierdził, że z jego rachunku bankowego wykonano trzy przelewy, których nie wykonywał i nie autoryzował. Poinformował o tym fakcie telefonicznie pracownika Banku. Rachunek bankowy powoda został zablokowany i zabezpieczono do zwrotu kwotę ostatniego przelewu, tj. 39.688 zł.

W dniu 16 marca 2018 r. powód złożył w Banku pisemną reklamację dotyczącą kradzieży pieniędzy z jego konta firmowego, jednakże Bank nie uznał tej reklamacji, gdyż nie doszło do przełamania zabezpieczeń systemu bankowości internetowej.

W dniu 1 października 2018 r. powód wezwał pozwanego do zapłaty kwoty 77.776 zł stanowiącej środki, które wskutek nienależnego wykonania przez Bank zobowiązania wynikającego z Umowy wypłynęły z jego rachunku.

Prokuratura Rejonowa dla Wrocławia Krzyki Wschód wszczęła dochodzenie w sprawie przyjęcia w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru w okresie od 24 października 2017 r. do dnia 19 marca 2018 r. w nieustalonym miejscu przez posiadacza oznaczonych rachunków środków finansowych pochodzących z czynu zabronionego w kwocie nie mniejszej niż 125.307,41 zł, tj. o czyn z art. 291 § 1 w związku z art. 12 k.k. W postępowaniu tym uznano za dowód rzeczowy kwotę 39.694,57 zł i zwrócono ją poszkodowanemu.

Uznając żądanie powoda za uzasadnione, Sądy obu instancji były zgodne, że odpowiedzialność Banku wynika z przepisów kodeksu cywilnego oraz art. 46 ust. 1 u.u.p., którą implementowano do polskiego porządku prawnego Dyrektywę 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego („dyrektywa 2007/64”). Do dnia 20 czerwca 2018 r. przepis ten stanowił, że 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. W ocenie Sądu odwoławczego w dniu 15 marca 2018 r. miały miejsce trzy nieautoryzowane przez powoda transakcje przelewów na rachunek nieustalonego odbiorcy. Wprawdzie przekazując kody otrzymane SMS-em, powód umożliwił hakerowi zalogowanie się na jego rachunek, a następnie zmodyfikowanie odbiorcy zaufanego, jednak powód nie autoryzował kolejnych trzech przelewów ani nie posiadał wiedzy o ich dokonywaniu.

Sądy zgadzały się również co do tego, że działania powoda w dniu 15 marca 2018 r. nie stwarzały Bankowi podstawy do odmowy zwrotu kwoty dochodzonej pozwem. Oceniły, że użycie przez powoda do logowania kodu otrzymanego w wiadomości SMS na numer telefonu podany w Banku nie było wyrazem rażącego niedbalstwa. Sąd odwoławczy przyjął zarazem, że art. 46 ust. 3 u.u.p. wyłączający odpowiedzialność banku w razie winy umyślnej albo rażącego niedbalstwa płatnika w ogóle nie miał zastosowania w sprawie, gdyż został wyłączony przez strony w Umowie. Stwierdził również, że powód nie naruszył obowiązków przewidzianych w § 87 Regulaminu. Stwierdził ponadto – rozważając odpowiedzialność powoda na podstawie art. 471 w związku z art. 355 § 1 k.c. i negując zastosowanie profesjonalnej miary staranności (ze względu na specjalizację powoda, prowadzącego zakład świadczący usługi elektryczne) - że *in casu* powód zachował staranność ogólnie wymaganą w stosunkach danego rodzaju. Nie informował bowiem nikogo o swoim haśle oraz loginie do konta, przy obsłudze rachunku elektronicznego korzystał w własnego komputera - laptopa wyposażonego w legalne oprogramowanie oraz system antywirusowy. Do zdarzenia doszło w następstwie przekierowania powoda - przez nieustaloną osobę - na stronę do złudzenia przypominającą stronę internetową jego rachunku bankowego w Banku, oraz udostępnienia tej osobie kodów autoryzacyjnych umożliwiających zalogowanie się na właściwą stronę rachunku bankowego, jak również dokonanie określenia odbiorcy zaufanego. Wprawdzie powód posiadał ogólną świadomość działalności hakerów w bankowości internetowej, jednakże nie sposób przyjąć, aby mógł sobie wyobrazić skutek swoich działań w postaci nielegalnego pobrania środków z jego rachunku bankowego. W dniu 15 marca 2018 r. próbował w sposób nieudany zalogować się na swój rachunek bankowy, co przy bankowości internetowej z różnych przyczyn zdarza się

dość często. Otrzymany w związku z tym pierwszy SMS o dodatkowej autoryzacji logowania, na telefon komórkowy, którego numer udostępniono bankowi, mógł nie wzbudzić podejrzeń powoda, gdyż przeciętnie doświadczony płatnik obsługujący elektroniczny rachunek bankowy mógł dojść do przekonania, że otrzymany SMS umożliwi mu zalogowanie się do swojego rachunku bankowego. Również drugi SMS dotyczący modyfikacji bazy odbiorców mógł nie wywołać podejrzenia próby oszustwa. Z treści tej wiadomości bowiem nie wynikało wprost, że nastąpi dodanie odbiorcy do kategorii odbiorców zaufanych nie wymagających dodatkowej autoryzacji. Ponadto spółka E. uprzednio była już odbiorcą powoda, stąd jako uzasadnione należało przyjąć przypuszczenie powoda, że drugi SMS pochodzi również od Banku.

Sądy miały też na względzie, że środki zgromadzone na rachunku powoda stanowiły własność Banku, który mógł nimi swobodnie obracać we własnym imieniu i który ponosił ryzyko dokonania wypłaty z rachunku bankowego do rąk osoby nieuprawnionej oraz dokonania rozliczenia pieniężnego na podstawie dyspozycji wydanej przez osobę nieuprawnioną, bez względu na okoliczność czy utrata środków była przez Bank zawiniona (*damnum sensit dominus*). Zarazem Sąd Apelacyjny uznał, że Bank nie naruszył obowiązku szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych, a w szczególności nie zostały przełamane zabezpieczenia banku umożliwiające dostęp osobom nieuprawnionym do systemów informatycznych banku.

Skargę kasacyjną od wyroku Sądu Apelacyjnego wniósł pozwany, zaskarżając go w całości. Zarzucił naruszenie prawa materialnego, tj. art. 46 ust. 1 u.u.p. w związku z art. 72 ust. 1 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającej dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE (dalej „PSD2”), art. 40 u.u.p., art. 355 § 1 k.c. oraz art. 362 k.c. Wniósł o uchylenie zaskarżonego wyroku oraz wyroku Sądu Okręgowego we Wrocławiu w całości, oddalenie powództwa oraz zasądzenie od powoda zwrotu kosztów postępowania za wszystkie instancje oraz kosztów w postępowaniu kasacyjnym, ewentualnie – o uchylenie zaskarżonego wyroku oraz wyroku Sądu Okręgowego we Wrocławiu

w całości i przekazanie sprawy do ponownego rozpoznania sądowi Okręgowemu we Wrocławiu lub innemu równorzędnemu z pozostawieniem temu sądowi rozstrzygnięcia o kosztach postępowania kasacyjnego.

Sąd Najwyższy zważył, co następuje:

Naruszenia art. 46 ust. 1 u.u.p. w związku z art. 72 ust. 1 PSD2 pozwany dopatrzył się w przyjęciu, że w przypadku wystąpienia nieautoryzowanej transakcji płatniczej bank jest zobowiązany do udowodnienia autoryzacji transakcji płatniczej, a w przypadku braku takiego udowodnienia - do dokonania niezwłocznego zwrotu środków, podczas gdy z art. 72 ust 1 PSD2 wynika, iż do dostawcy usług płatniczych należy udowodnienie, że transakcja ta została uwierzytelniona, dokładnie zapisana, ujęta w księgach i że na transakcję nie miała wpływu awaria techniczna ani innego rodzaju usterka związana z usługą świadczoną przez danego dostawcę usług płatniczych, nie zaś fakt autoryzacji transakcji. Zdaniem skarżącego brzmienie art. 45 ust. 1 u.u.p., nakładającego na dostawcę użytkownika – w razie, gdy użytkownik kwestionuje autoryzację transakcji - ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika, nie oddaje prawidłowo treści art. 72 ust. 1 PSD2, który rozróżnia autoryzację oraz uwierzytelnienie i wskazuje na ciężar udowodnienia przez dostawcę „uwierzytelnienia” transakcji płatniczej. Różnica jest istotna: o ile bowiem autoryzacja to zgoda na wykonanie transakcji płatniczej wyrażona przez płatnika w sposób przewidziany w umowie, o tyle uwierzytelnienie to procedura umożliwiająca dostawcy usług (bankowi) na weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika. W ocenie pozwanego, w świetle art. 72 ust. 1 PSD2, w celu wykazania autoryzacji dostawca musi udowodnić uwierzytelnienie transakcji, które stanowi zewnętrzną formę (zewnętrzny przejaw) wyrażenia zgody. W tym kontekście skarżący wskazał, że *in casu* umożliwienie przez powoda zalogowania hakerowi w systemie przez udostępnienie danych służących do zalogowania w systemie bankowości elektronicznej Banku, tj. numeru klienta i hasła, jak również podanie kodów autoryzacyjnych otrzymanych SMS z Banku, służących do uwierzytelnienia transakcji do odbiorcy zaufanego, oznacza spełnienie kryteriów uwierzytelnienia (autoryzacji) transakcji w rozumieniu powyższych regulacji. Transakcje płatnicze były

zatem transakcjami autoryzowanymi. Powód wiedział też o dokonaniu uwierzytelnienia transakcji do odbiorcy zaufanego, gdyż otrzymując kod autoryzacyjny w formie SMS w treści wiadomości otrzymał informacje o tym, że posłuży on do zatwierdzenia modyfikacji odbiorcy zaufanego.

Rozpatrując przedstawiony zarzut, należy najpierw zwrócić uwagę – co skarżący pomija – że art. 46 ust. 1 u.u.p., którego naruszenie zarzuca, normuje konsekwencje braku autoryzacji w sposób odpowiadający treści dyrektywy PSD2. Natomiast kwestii dowodowych dotyczy art. 45 u.u.p., którego naruszenia pozwany nie zarzucił, a ponadto – jak wynika z ustaleń - zastosowanie tego przepisu zostało przez strony wyłączone na podstawie art. 33 u.u.p. Wbrew sugestii pozwanego trzeba też stwierdzić, że wykazanie uwierzytelnienia przez dostawcę usług nie jest równoznaczne z wykazaniem autoryzacji, co potwierdza art. 45 ust. 2 u.u.p., który stanowi, iż wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana (co do ciężaru dowodu por. wyrok Sądu Najwyższego z dnia 18 stycznia 2018 r., V CSK 141/17, niepubl.). Wprawdzie część doktryny zwraca uwagę, że wykazanie przez dostawcę uwierzytelnienia przenosi ciężar dowodu co do braku autoryzacji na użytkownika (płatnika), jednakże *in casu* jest to o pozbawione znaczenia, ponieważ Sąd odwoławczy ustalił jednoznacznie, iż powód nie udzielił zgody na przedmiotowe przelewy, a więc ich nie autoryzował. Rzecz bowiem w tym, że kod z obu SMS przesłanych przez Bank został użyty przez powoda z intencją zalogowania (był przezeń wpisywany na fałszywej stronie internetowej w celu zalogowania), a nie w celu autoryzacji przyszłych przelewów przez dodanie odbiorcy zaufanego.

Zarzucane przez skarżącego naruszenie art. 40 u.u.p. miało polegać na przyjęciu, że płatnik może wyrazić jednorazową zgodę na wykonanie kolejnych transakcji płatniczych do tzw. „zaufanego odbiorcy” tylko w przypadku, gdy zaufanym odbiorcą jest dostawca usług wody, prądu, abonamentu telefonicznego, itp., albo w zakresie transakcji o niedużych kwotach, podczas gdy art. 40 u.u.p. umożliwia wyrażenie przez płatnika jednorazowej zgody na wykonanie kolejnych transakcji płatniczych do danego odbiorcy bez ograniczeń w zakresie konkretnej kwoty lub wymogów co do branży w ramach której dany odbiorca świadczy usługi. Jednakże

wbrew sugestii pozwanego Sąd Apelacyjny nie ograniczył możliwości wyrażenia jednorazowej zgody na wykonanie kolejnych transakcji płatniczych do tzw. „zaufanego odbiorcy”, a jedynie zwrócił uwagę, że przyjęte w Banku rozwiązanie, zgodnie z którym przelewy wysyłane do tak zwanych odbiorców zaufanych nie wymagają dodatkowej autoryzacji, bez względu na wysokość tych przelewów, jest rozwiązaniem dla płatników niebezpiecznym. O ile bowiem umożliwia to prostsze i szybsze dokonywanie transakcji, zwłaszcza cyklicznych realizujących bieżące płatności – chodzi wówczas przeważnie o nieduże środki, których odbiorcami są zaufane przedsiębiorstwa – o tyle w przypadku powoda po fałszywym utworzeniu odbiorcy zaufanego w ciągu jednego dnia zdefraudowano kwotę 117.464 zł. Wymóg zaś dodatkowej autoryzacji lub chociażby telefonu czy SMS-a ze strony banku do płatnika uchroniłby posiadaczy rachunków bankowych od defraudacji na tak znaczną skalę. Wywód ten zatem miał nie tyle wskazać na samoistną podstawę odpowiedzialności Banku, ile wzmacniać argumentację na rzecz obciążenia Banku ryzykiem nieautoryzowanej transakcji.

Z kolei sformułowane w skardze kasacyjnej zarzuty naruszenia art. 355 § 1 i art. 362 k.c. zmierzają w istocie do wykazania, że udostępnienie przez powoda otrzymanego SMS-a zawierającego kod autoryzacyjny służący do autoryzacji transakcji do odbiorcy zaufanego, mimo że nie zamierzał on wykonać takiej operacji, stanowiło zachowanie naruszające miernik zwykłej staranności i rażąco niedbałe, a tym samym uzasadniało tezę o przyczynieniu się powoda do powstania szkody i zasadności zmniejszenia obowiązku naprawienia szkody przed Bank.

W tym kontekście trzeba przede wszystkim zauważyć, że jakkolwiek Sąd Apelacyjny oceniał zachowanie powoda w kontekście zastosowania art. 471 w związku z art. 355 § 1 k.c., jednakże nie określił jasno reżimu prawnego odpowiedzialności pozwanego ani nie wyjaśnił precyzyjnie, jakie znaczenie dla tej odpowiedzialności miała ewentualna zwykła niestaranność albo rażące niedbalstwo powoda. Jest to uchybienie, zwłaszcza w sytuacji, w której Sąd ten zauważył, że art. 46 ust. 3 u.u.p. nie miał tu zastosowania, gdyż został wyłączony przez strony w Umowie. Kwestia zastosowania w sprawie art. 362 k.c. w ogóle nie została przez Sąd rozważona, a jest to kwestia problematyczna już z tego względu, że część

doktryny kwestionuje odszkodowawczy charakter odpowiedzialności przewidzianej w art. 46 ust. 1 u.u.p. i tym samym dopuszczalność zastosowania art. 362 k.c.

Trzeba ponadto zgodzić się z zarzutem pozwanego o tyle, o ile ocena dochowania przez powoda staranności wymaganej w okolicznościach niniejszej sprawy miała rzeczywiście charakter zbyt powierzchowny. Dla tej oceny niezbędne było nie tylko uwzględnienie trudności powoda w zalogowaniu się do swojego konta w Banku w dniu 15 marca 2018 r. – związane rzecz jasna z przekierowaniem go na fałszywą stronę logowania – ale także treści wysyłanych przez Bank SMS, zawierających kody autoryzacyjne, a w szczególności sposobu zidentyfikowania w nich rodzaju autoryzowanej czynności. Skarżący trafnie zauważa, że z tego punktu widzenia szczególne wątpliwości budzi drugi SMS, który miał służyć autoryzacji dodania odbiorcy zaufanego, a został przez powoda wykorzystany w celu ponowienia próby zalogowania do konta. Stosownie bowiem do ustaleń Sądu pierwszej instancji – zaaprobowanych i przejętych za własne przez Sąd Apelacyjny, jakkolwiek w tej części pominiętych w uzasadnieniu zaskarżonego wyroku – SMS ten zawierał opis o treści „Modyfikacja bazy odbiorców: […], kod nr 2: […]. Pamiętaj, aby NIKOMU nie udostępniać kodu”. Wprawdzie Sąd odwoławczy zasadnie zwrócił uwagę, że „modyfikacja bazy odbiorców” nie jest wprost równoznaczna z dodaniem nowego odbiorcy zaufanego (do którego przelew nie wymagał dodatkowej autoryzacji), co przemawia na korzyść powoda, jednakże tym mniej kojarzy się z autoryzacją kolejnej próby logowania, do czego powód usiłował wykorzystać kod z tego SMS-a. Pełna ocena postępowania powoda nie jest też możliwa bez uwzględnienia informacji, które Bank udzielał powodowi. Przywołane przez Sąd odwoławczy ustalenia dotyczące tej kwestii są lakoniczne, wynika z nich bowiem jedynie, że Bank wysyłał m.in. do powoda wiadomości ostrzegające przed atakami hakerów oraz przypominające o zachowaniu zasad bezpiecznego korzystania z bankowości internetowej i mobilnej. Sąd drugiej instancji pominął przy tym fragment ustaleń Sądu Okręgowego, z których wynika, że Bank przypominał m.in. o potrzebie weryfikacji treści SMS-ów przez potwierdzeniem każdej transakcji. Tymczasem w rozpatrywanym kontekście nie bez znaczenia jest kwestia, czy i w jaki sposób (czy wystarczająco czytelny) Bank zwracał uwagę klientów (w tym powoda) na konieczność każdorazowego upewnienia się co do zgodności między autoryzowaną czynnością wskazaną w wiadomości SMS

a czynnością faktycznie dokonywaną przez klienta. Wskazane niedostatki argumentacji Sądu odwoławczego nie pozwalając odeprzeć zarzutu pozwanego.

Z tych względów, na podstawie art. 398^{15} § 1 k.p.c., Sąd Najwyższy orzekł, jak w sentencji.

(K.L.)

[ał]