Pregledni naučni rad

Bankarstvo, 2023, vol. 52, br. 4

Datum prijema: 02.02.2024. god.
Datum prihvatanja: 2024. god.

ODGOVORNOST BANKE PLATIOCA U SLUČAJU PREVARE SA AUTORIZOVANIM PLATNIM NALOGOM

Bojan Terzić
direktor Sektora za zaštitu korisnika finansijskih usluga
Narodna banka Srbije
bojan.terzic@nbs.rs

DOI: 10.5937/bankarstvo2304104T

Rezime: Prevara sa autorizovanim platnim nalogom predstavlja veliku opasnost za korisnike platnih usluga jer su iznosi tih transakcija često veći u odnosu na iznose kod neautorizovanih transakcija (zloupotreba platnih instrumenata), dok je povraćaj sredstava teže izvodljiv. Banke platioca za sada su uverene da u skladu sa propisima o platnim uslugama, u tim slučajevima ne mogu biti odgovorne za gubitak. Ipak, opšta pravila srpskog ugovornog prava koja bi se mogla supsidijarno primeniti, nalažu banci da upozori platioca koji je izdao platni nalog ako smatra da bi izvršenje takvog naloga bilo od štete za njega. Preduslov za aktiviranje ove dužnosti banke jeste da spram okolnosti konkretnog slučaja postoji razumno očekivanje da je uobičajeno razborit bankar mogao da posumnja u ispravnost (integritet) platnog naloga. Ako u takvoj situaciji banka nije upozorila platioca, u obzir dolazi primena instituta podeljene odgovornosti za nastanak, odnosno doprinos u nastanku štete iz Zakona o obligacionim odnosima.

Ključne reči: Prevara sa autorizovanim platnim nalogom; Presretnuta imejl komunikacija; Propisi o platnim uslugama; Dužnost pažnje; Odgovornost banke platioca.

JEL klasifikacija: G21, K12, K22, K42

Uvod

Internet i elektronska komunikacija pored ogromnih prednosti sa sobom nose i određene rizike kojih korisnici platnih usluga često nisu svesni ili ih prenebregavaju. Dok je rizik zloupotrebe platnih kartica usled gubitka, krađe kartice ili podataka sa kartice relativno dobro poznat korisnicima platnih usluga, prevara sa autorizovanim platnim nalogom (*Authorised Push Payments Fraud, APP*) nepoznata je širem krugu korisnika, iako njene posledice, u smislu iznosa gubitka, daleko nadilaze kartične zloupotrebe. Ovakav naziv (autorizovan nalog) proističe iz činjenice da platilac kao žrtva prevare sam daje instrukciju banci da prebaci novac na račun koji kontrolišu kriminalci, te je sa aspekta banke takva transakcija autorizovana.

Trenutno, najopasniji oblik *APP* prevare u Srbiji, jeste prevara usled presretnute (poslovne) imejl komunikacije (*Business Email Compromise, BEC*). Šema kod ove prevare se najčešće sastoji u tome što kriminalci pristupe komunikaciji između poslovnih partnera (tako što pristupe imejl nalogu jedne od strana u komunikaciji), a zatim imajući pred sobom sve podatke iz dotadašnje komunikacije, na uverljiv način navode jednog od njih da novac prenese na račun pod njihovom kontrolom.

Pored namere da ukaže stručnoj i široj zainteresovanoj javnosti na ovaj aktuelni izazov, cilj ovog rada je da na osnovu postojećih propisa, domaće i uporedne prakse razmotri pitanje odgovornosti klijenta i banke za gubitak (koji često iznosi nekoliko desetina, pa i stotina hiljada evra) nastao usled prevara sa autorizovanim platnim nalogom. Zbog toga što je transakcija nesumnjivo autorizovana od strane korisnika, banke su, čini se uverene, da na osnovu važećih propisa ne mogu biti odgovorne za gubitak korisnika. Međutim, da li je baš tako? U radu smo pokušali da damo odgovor na to pitanje, analizirajući domaće propise i dajući prikaz prakse Narodne banke Srbije, istovremeno ih dovodeći u vezu sa pojedinim institutima precedentnog prava (*common law*) i praksom u Ujedinjenom Kraljevstvu.

Podaci o prevarama usled presretnute imejl komunikacije

Prema podacima iz ankete Narodne banke Srbije ukupan iznos zloupotreba po platnim karticama u 2021. godini iznosi 93 miliona dinara (od toga 78,6 na internetu, 2,5 na fizičkim prodajnim mestima i 11,9 na bankomatima). Korisnicima je vraćeno 74,2 miliona dinara. U 2022. godini ukupan iznos zloupotreba po platnim karticama iznosi 179,7 miliona dinara (od toga 129,8 na internetu, 41,6 na fizičkim prodajnim mestima i 8,2 na bankomatu). Ukupno je vraćeno korisnicima 141 milion dinara.

Kada je reč o prevarama usled presretnute (poslovne) imejl komunikacije u 2021. godini izvršeno je 105 platnih naloga u ukupnom iznosu od 251,5 miliona dinara, dok je u 2022. godini izvršeno 108 naloga u ukupnom iznosu od 418 miliona dinara (99% od tog ukupnog iznosa odnosi se na plaćanja privrednih društava u međunarodnom platnom prometu). U 2021. godini izvršen je povraćaj za 22 transakcije u ukupnom iznosu od 54,2 miliona dinara, a u 2022. godini 22 transakcije u ukupnom iznosu od 68,8 miliona dinara.

Iz navedenih podatka najpre zaključujemo da je u slučaju zloupotreba platnih kartica (posmatrano za 2022. godinu) prosečan iznos transakcije oko 9.000 dinara, dok je prosečan iznos transakcije kod prevara sa presretnutom imejl komunikacijom oko 3.870.000 dinara. Dodatno, korisnicima kartica vraćeno je 78 - 80% zloupotrebljenih sredstava, dok je u slučaju BEC prevara banka platioca uspela da obezbedi povrat od 16 do 20% sredstava.

Pored ovog poređenja, a budući da su sve BEC transakcije izvršene u međunarodnom platnom prometu, korisno je dati poređenje između broja i vrednosti transakcija u domaćem i međunarodnom platnom prometu (ne uključujući kartične transakcije). Iz izveštaja Narodne banke Srbije (*Opšti pokazatelji RTGS sistema i Kliring sistema u 2022. godini:* https://nbs.rs/sr/ciljevi-i-funkcije/platni-sistem/statistika/) može se izvesti podatak da je prosečan dnevni broj plaćanja po učesniku u sistemu veći od 34.000, dok je prosečna vrednost transakcije u ovom platnom sistemu 473.210 dinara, odnosno oko 4.000 evra. S druge strane, primer jedne od banaka (sa znatnim tržišnim učešćem u međunarodnom platnom prometu) pokazuje da je u 2022. godini, u proseku dnevno izvršeno 1.206 međunarodnih transakcija čija je ukupna vrednost 45,9 miliona evra, a prosečan iznos takve transakcije je 38.000 evra.

Pravni režim u slučaju prevare sa autorizovanim platnim nalogom

Pravila koja uređuju alokaciju gubitaka su važna ne samo zbog njihovih posledica u smislu raspodele tog gubitka, već i zbog podsticaja koje stvaraju. Veća odgovornost strane za gubitak nastao prevarom, znači veći podsticaj za tu stranu da bude pažljivija kako bi izbegla prevaru. (Levitin, 2010). U slučaju prevara u platnom prometu, pitanje alokacije gubitka je regulisano nacionalnim pravilima kojima je implementiran režim odgovornosti za neautorizovane platne transakcije u skladu sa direktivom o platnim uslugama. Kod ostalih finansijskih usluga, ova pitanja se rešavaju u skladu sa opštim pravilima o obligacionim odnosima (Kjørven, 2020).

Ovo je samo donekle tačno (i za članice EU i za Srbiju), budući da je i pitanje odgovornosti u slučaju prevare sa autorizovanim platnim nalogom dotaknuto direktivama o platnim uslugama kroz odredbe koje regulišu situaciju u kojoj je transakcija nepravilno izvršena usled unosa pogrešnog broja računa od strane platioca. S druge strane, iako i kod prevare sa autorizovanim platnim nalogom platilac unosi, autorizuje pogrešan broj računa, pitanje je da li je kroz te odredbe evropski zakonodavac hteo da reguliše samo greške uzrokovane tehničkim ili drugim sličnim propustom platioca, ili je na isti način (na teret platioca) hteo da izvrši alokaciju rizika i u slučaju „greške" uzrokovane prevarom.

Zakon o platnim uslugama

Sa aspekata Zakona o platnim uslugama (Službeni glasnik RS, br. 139/2014, 44/2018, dalje: ZPU) pravni položaj izdavaoca platnog naloga (platioca) koji je posledica prevare, znatno je nepovoljniji u odnosu na vlasnika zloupotrebljene platne kartice. Naime, odgovornost za pravilno izvršenje autorizovanog platnog naloga uređuju odredbe člana 55. st. 1. i 2. ZPU, kojima su transponovane odredbe člana 74 st. 1 i 2 prve Direktive o platnim uslugama (*Directive 2007/64/EC, OJ L 319, 5.12.2007,* dalje: Direktiva 2007/64). Odredbe sa istom sadržinom postoje i u trenutno važećoj, drugoj Direktivi po platnim uslugama (*Directive (EU) 2015/2366, OJ L 337/35, 23.12.2015, dalje:* Direktiva 2015/2366). Te odredbe propisuju da, ako je platni nalog izvršen u skladu *s jedinstvenom identifikacionom oznakom* primaoca plaćanja iz tog naloga, smatra se da je taj nalog pravilno izvršen u delu koji se odnosi na određenje primaoca plaćanja, bez obzira na druge podatke dostavljene pružaocu platnih usluga, a da *u slučaju kada je jedinstvena identifikaciona oznaka koju je korisnik platnih usluga dostavio pružaocu platnih usluga netačna, pružalac platnih usluga nije odgovoran za neizvršenu ili nepravilno izvršenu platnu transakciju.*

U članu 2. stav 1. tač. 19) ZPU definisano je da jedinstvena identifikaciona *oznaka označava kombinaciju slova, brojeva i/ili simbola* koju pružalac platnih usluga utvrđuje korisniku platnih usluga i koja se u platnoj transakciji *upotrebljava za nedvosmislenu identifikaciju tog korisnika i/ili njegovog platnog računa.* U praksi je nedvosmisleno zauzet stav da je jedinstvena identifikaciona oznaka u slučaju domaćeg platnog prometa broj tekućeg računa kod banke, odnosno broj drugog platnog računa kod institucije elektronskog novca ili platne institucije, dok je u slučaju međunarodnog platnog prometa to međunarodni broj bankovnog računa (*International Bank Account Number; IBAN*).

Dakle, ZPU je ovde potpuno jasan i nedvosmislen. Ako banka prenese novac na račun naveden u platnom nalogu, koji je autorizovan od strane platioca (na način kako je određeno u ugovoru o platnim uslugama)[1], ne postoji odgovornost banke kao pružaoca platnih usluga platioca, za neizvršenu ili nepravilno izvršenu platnu transakciju. Drugim rečima, u skladu sa navedenim odredbama ZPU za banke je primalac lice koje je vlasnik računa koji je naveden u platnom nalogu, a ne lice čiji je naziv (ime i prezime), adresa i sl. naveden u tom nalogu. Banka platioca jeste dužna da proveri ispravnost računa navedenog u platnom nalogu u smislu njegove logičke kontrole (svih elemenata koji čine taj broj), ali banka u skladu sa pomenutim odredbama ZPU, nije dužna da „uparuje" broj računa i primaoca sredstava.

Ipak, od trenutka kada platilac prijavi da se radi o prevari, Banka je u skladu sa članom 55. stav 3. ZPU dužna da preduzme razumne mere radi povraćaja novčanih sredstava, odnosno kada povraćaj više nije moguć da utvrdi tok novčanih sredstava i o tome obavesti korisnika. Važno je pritom primetiti, da je radi ostvarivanja prethodno navedenog cilja (povraćaj, odnosno informacija o toku novčanih sredstava), ovom odredbom predviđena i obaveza banke primaoca sredstava da sarađuje (dostavlja određene podatke, npr. o primaocu sredstava) sa bankom platioca. Međutim, u međunarodnom platnom prometu, gde se trenutno ove vrste prevara najčešće dešavaju, tu saradnju nije moguće uvek obezbediti jer se radi o bankama u inostranstvu. Pribavljanje podatka o primaocu plaćanja koji je izvršio prevaru zavisi isključivo od volje njegove (inostrane) banke da sarađuje sa bankom platioca i njenom korespondentskom bankom. Pored kasne reakcije platioca (koji shvataju da su prevareni tek nakon nekoliko nedelja pa i meseci), nizak procenat povrata sredstava u ovim slučajevima uzrokovan je i pasivnošću banke primaoca sredstava. Zanimljivo je reći, da *SWIFT (Society for Worldwide Interbank Financial Telecommunication)*, za razliku od *SEPA (Single Euro Payments Area)* nema standardizovanu poruku za prevaru, što informacionim sistemima banaka primalaca sredstava ograničava mogućnost da automatski blokiraju sredstva ili generišu upozorenje. Banke platioca, trenutno, u slučaju ovakvih prevara, banke šalju dve standardizovane poruke, MT192 i MTn92 od kojih nijedna nužno ne ukazuje na prevaru. Prva označava zahtev za opoziv prethodne poruke kojom su sredstva transferisana, a druga predstavlja zahtev za povraćaj sredstava, ali uz saglasnost primaoca.

Prethodno navedeno pokazuje da ZPU, kao poseban zakon koji uređuje prava korisnika platnih usluga, propisuje da gubitak u slučaju prevare sa autorizovanim nalogom snosi platilac kao nalogodavac. Za razliku od zloupotreba platnih kartica gde se u skladu sa članom 51. ZPU ceni stepen nepažnje platioca, kod prevare sa autorizovanim platnim nalogom, stepen nepažnje korisnika sa aspekata ZPU nije od značaja. Čak i kada je platilac žrtva veoma vešte, sofisticirane, odnosno složene prevare, kojoj bi podlegao i korisnik koji je postupao sa pažnjom dobrog domaćina, odnosno dobrog privrednika, ZPU je neumoljiv - odgovornost za gubitak nastao usled ovakve prevare na strani je platioca, koji je popunio i izdao, autorizovao platni nalog. Za razliku od kartičnih transakcija (oblik direktnog zaduženja), gde nedostatak u monitoringu tih transakcija na strani banke izdavaoca kartice (član 59. ZPU) može biti poslednji argument korisnika koji otvara mogućnost eventualne podeljene odgovornosti banke i korisnika, izdavaocima klasičnog platnog naloga (transfera odobrenja) ZPU ne daje takvu priliku. ZPU njima garantuje samo obavezu banke da odmah nakon prijave prevare kontaktira banku primaoca sredstava, uglavnom preko korespondentske banke i zahteva povraćaj sredstava, nadajući se da će banka primalac reagovati na vreme.

[1] *Autorizacija naloga se može izvršiti svojeručnim potpisom na papirnom obrascu, kvalifikovanim potpisom u okviru elektronskog dokumenta ili dvofaktorskom autentifikacijom. Pored ZPU, pitanje (dvofaktorske) autentifikacije uređuje i Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije („Službeni glasnik RS", br. 23/2013, 113/2013, 2/2017, 88/2019 i 37/2021), kojom su implementirani određeni standardi autentifikacije utvrđeni Direktivom 2015/2366 i Delegiranom Uredbom Komisije 2018/389.*

Kada banka primalac i reaguje na vreme i spremna je da izvrši povraćaj sredstava (obično uz dokaz da je izvršena prijava prevare nadležnim organima) ona to često uslovljava pismenom garancijom banke platioca, da će izmiriti obaveze prema primaocu, ako na to bude obavezna *(letter of indemnity)*. S tim u vezi, postavlja se pitanje da li bi banka platilac bila dužna da pošalje takvu izjavu u kontekstu njene obaveze da preduzme sve razumne mere radi povraćaja sredstava. Na osnovu modela izjave u koju smo imali uvid, proizilazi da se tom izjavom[2] banka platioca obavezuje da izvrši povraćaj prethodno vraćenih sredstava, ne samo u slučaju odluke suda ili drugog nadležnog organa u zemlji banke primaoca sredstava, već i u slučaju zahteva primaoca sredstava bez takve odluke. Ipak, s obzirom da se radi o šemi prevare koja je dobro poznata bankama, teško je prihvatiti da bi banka primaoca sredstava koja je otvorila račun licu osumnjičenom za prevaru bila spremna da od banke platioca zahteva povraćaj sredstava, samo na osnovu zahteva tog lica bez procene osnovanosti takvog zahteva, odnosno bez pokretanja određenog postupka protiv banke od strane tog lica. Zbog toga bi se donekle ipak mogao izvesti zaključak, koji u određenim slučajevima zbog specifičnih okolnosti ne bi važio – da je banka platioca dužna, da u okviru razumnih aktivnosti s ciljem povraćaja sredstva (član 55. stav 3. ZPU), dostavi banci primaoca i takvu izjavu.

Supsidijarna primena opštih pravila ugovornog prava

Članom 14. stav 2. ZPU predviđeno je da se na sva pitanja koja nisu uređena tim zakonom primenjuju odredbe Zakona o obligacionim odnosima, (Sl. list SFRJ", br. 29/78, 39/85, 45/89 - odluka USJ i 57/89, „Sl. list SRJ", br. 31/93, Sl. list SCG, br. 1/2003 - Ustavna povelja i Sl. glasnik RS, br. 18/2020, dalje: ZOO)

ZPU uređuje pitanje odgovornosti za nepravilno izvršenje platne transakcije usled pogrešnog broja računa, ali kako je prethodno navedeno, ne može se sa sigurnošću uzeti da je prilikom formulisanja takvog pravila zakonodavac uzeo u obzir prevare sa autorizovanim platnim nalogom. Drugim rečima, moglo bi se postaviti pitanje je da li je član 55. ZPU sedes materiae za pitanje odgovornosti kod nepravilno izvršenih transakcije usled prevare sa autorizovanim nalogom ili u tom delu zapravo postoji pravna praznina, koju treba popuniti supsidijarnom primenom ZOO.

Dalje, jasno je da je primarna obaveza banke kao nalogoprimca da izvršava platne naloge kako glase u skladu sa ugovorenim rokovima. Drugim rečima, njena osnovna dužnost je da se novac sa računa njenog klijenta prenese na račun koji taj klijent naznači u platnom nalogu. S tim u vezi, član 36. ZPU izričito navodi da banka ne može odbiti izvršenje platnog naloga kada su ispunjeni svi uslovi utvrđeni ugovorom o platnim uslugama, osim ako je drugačije utvrđeno nekim propisom. Taj drugi propis bi mogao biti ZOO i to odredbe koje ustanovljavaju standarde u pogledu načina izvršavanja naloga, odnosno kada nalogoprimac može odbiti izvršenje tog naloga. S tim u vezi, članom 1057. stav 1. ZOO (koji uz ZPU reguliše ugovor o bankarskom tekućem računu) propisano je da banka odgovara za izvršenje naloga deponenta prema pravilima ugovora o nalogu. Međutim, (opštim) pravilima ugovora o nalogu nalaze se i odredbe člana 751. stav 1. i 2. ZOO. Prvom je propisana obaveza za nalogoprimca da nalog izvrši prema primljenim uputstvima, sa pažnjom dobrog privrednika, ostajući u njegovim granicama i u svemu pazeći na interese nalogodavca i rukovodeći se njima, dok je drugom precizirano da nalogoprimac ima obavezu da kada smatra da bi izvršenje naloga po dobijenim uputstvima bilo od štete za nalogodavca, skrene na to pažnju nalogodavcu i zatraži nova uputstva. Ova pravila bi se mogla shodno primeniti na banku, i to na način da bi za banku kao „profesionalnog nalogoprimca", morao da važi viši stepen pažnje iz stava 2. člana 18. ZOO – pažnja dobrog stručnjaka.

[2] *„Ovim pismom se saglašavamo da vas obeštetimo i da vas smatramo oslobođenim odgovornosti u vezi sa bilo kojim radnjama, postupcima, potraživanjima i zahtevima koji bi mogli biti usmereni prema vama, te da vam nadoknadimo sve gubitke, troškove i štetu koju možete da pretrpite - zbog toga što ste nam vratili iznos transakcije bez saglasnosti vašeg klijenta."*

Drugim rečima, „pošto je nalogoprimac stručnjak za poslove iz naloga čijeg se izvršenja prihvata, on je dužan da upozori na grešku postupajući sa pažnjom dobrog privrednika i dobrog domaćina. Pri tome se pod pažnjom dobrog privrednika podrazumeva pažnja dobrog stručnjaka" (Trajković, Perović (red), 1995, 1282).

S tim u vezi, razumno je očekivati da uz pažnju dobrog stručnjaka, a s obzirom na svoje znanje i iskustvo u vezi sa platnim prometom, banka u određenim slučajevima može da prepozna potencijalnu BEC prevaru i u skladu sa članom 751. stav 2. upozori svog klijenta.

Zapravo, ne bi trebalo dovoditi u pitanje postojanje uvek prisutne obaveze banke da kada sumnja na prevaru, odbije izvršenje naloga i upozori korisnika, već je ključno pitanje kada je banka dužna, odnosno kada kao profesionalni pružalac platnih usluga može, odnosno kada bi morala, da posumnja u ispravnost primljenih uputstava, čime bi se aktivirala njena obaveza iz člana 751. stav 2. ZOO.[3] U vezi sa ovim pitanjem treba primetiti da je članom 110. Zakona o bankama (Službeni glasnik RS, br. 107/2005, br. 91/2010 i 14/2015, dalje: Zakon o bankama) prepoznat standard opreznog bankarskog poslovanja. Iako je ovo pre svega standard koji se koristi kod kontrole boniteta banke, njegova primena se može ceniti i sa aspekta kontrole zakonitosti poslovanja banke u pružanju platnih usluga. S tim u vezi, može se uzeti da bi postojanje opreza na strani banke bilo opravdano i očekivano ako postoji određeno iskustvo ili saznanje na strani banke koje ukazuje da je kod pružanja određenih usluga takav oprez potreban, s tim da takav oprez ne remeti pružanje tih usluga.

U okolnostima kada postoji porast različitih oblika prevara sa autorizovanim platnim nalogom, može se uzeti da banke kao pružaoci platnih usluga imaju i saznanje i određeno iskustvo koje bi trebalo da ih navede da postupaju sa povećanim stepenom opreza kod izvršavanja, pre svega međunarodnih platnih transakcija. Uz to, a kako je prethodno prikazano, broj platnih naloga u međunarodnom platnom prometu nije tako veliki, dok je istovremeno pojedinačna vrednost tih naloga značajna i pritom postoji nizak stepen povraćaja sredstva u slučaju prevare. Sve to navodi na zaključak da pojačani oprez banke (koji vodi dodatnom administriranju), ne bi bio nesrazmeran potencijalnoj šteti koja se može izbeći i ne bi ugrozio pružanje ove vrste platnih usluga.

S tim u vezi i primera radi, „prema Američkom Jedinstvenom trgovačkom zakoniku *(Uniform Commercial Code)* generalno posmatrano, banka nije odgovorna za gubitak ako je primenila 'komercijalno razumne' *(commercially reasonable)* sigurnosne procedure" (Tang, 2015). Da bi odlučili šta je „ekonomski razumno" Američki trgovački zakonik upućuje sudove „da razmotre želje korisnika koje su iskazane prema banci, okolnosti u vezi sa korisnikom koje su poznate banci, uključujući vrednost, vrstu i učestalost platnih naloga koje korisnik redovno izdaje banci...i generalno sigurnosne procedure koje primenjuju korisnik i banke primalaca koje su u sličnoj poziciji" (Tang, 2015).

Ako se pogledaju slučajevi prevara usled presretnute imejl komunikacije u vezi sa kojima je pred Narodnom bankom Srbije vođen postupak po pritužbi, može se zaključiti da je prvi indikator ove prevare – podatak da sedište (fabrika, poslovnica i sl.) primaoca sredstava i sedište ili filijala banke u kojoj se nalazi račun iz naloga za plaćanje, nisu u istoj državi. Od ukupno 24 pritužbe u vezi sa *BEC* prevarama koje je Narodna banka Srbije rešila, u 18 slučajeva se razlikovala država sedišta, pravog primaoca sredstava i banke lažnog primaoca sredstava. Drugi, jednako važan pokazatelj jeste promena računa i banke prema kojoj se vrši plaćanje, u odnosu na račun (banku) na koji je klijent ranije vršio prenos istom primaocu sredstava. Ako su ova dva pokazatelja udružena, postoji veoma visok stepen verovatnoće da se radi o prevari. Pored navedenog, neuobičajeno visok iznos i/ili učestalost transakcija, kao i država banke primaoca mogu da predstavljaju dodatne pokazatelje.

[3] *Uporedno posmatrano, kao pandan ovom standardu iz ZOO u Ujedinjenom Kraljevstvu se primenjuje institut duty of care, odnosno u slučaju banaka quincecare duty. Više o tome u nastavku rada.*

Uz to, budući da banka ima saznanje o svakoj izvršenoj prevari prema njenim klijentima, pojavljivanje banke prema kojoj su prethodno vršena *BEC* plaćanja moralo bi uvek da bude dodatno provereno. Pritom, član 75. stav 2. ZPU daje mogućnost bankama da razmenjuju ove podatke, tako da mogu imati određenu sivu listu banaka prema kojima su vršena takva plaćanja.

Dakle, primena standarda opreznog bankarskog poslovanja kod izvršavanja (međunarodnih) platnih naloga u postojećim okolnostima bi između ostalog značila da banka treba da prikupi i objedini istorijske podatke i tako definiše indikatore prevara, te da te indikatore koristi prilikom kontrole platnog naloga. Ako se takvi indikatori pojave, Banka ima dužnost da prepozna da instrukcije mogu biti štetne po platioca, čime se aktivira njena obaveza iz člana 751. stav 2. ZOO da upozori nalogodavca. Ovde je važno primetiti da banke imaju različit stepen automatizacije u izvršavanju platnih naloga, različit broj i strukturu korisnika (stanovništvo/privredna društva) i platnih naloga, različit odnos broja domaćih i međunarodnih platnih transakcija, i uopšte različit obim i strukturu platnog prometa. Sve to treba uzeti u obzir kada se ceni ispunjenost standarda opreznog bankarskog poslovanja, te taj standard treba ceniti u odnosu na konkretnu banku.[4]

U svakom slučaju, u okolnostima kada se broj i vrednost *BEC* transakcija i drugih oblika prevara sa autorizovanim nalogom povećava, i kada je to banci poznato, banka se teško može sakriti iza isključive primene člana 55. stav 2. ZPU. Zapravo, i sama ta odredba navodi da Banka nije dužna da proverava ispravnost broja računa u platnom nalogu, što ne znači da nije dužna da upozori korisnika, ako ima određene sumnje u pogledu tog računa ili nekog drugog elementa iz platnog naloga.

Na osnovu prethodno navedenih razmatranja, moglo bi se zaključiti da u situaciji u kojoj je banci poznato postojanje ovih vrsta prevara, kao i pokazatelja koji mogu da signaliziraju prevaru, nije moguće ceniti odgovornost banke isključivo sa aspekata ZPU, već je neophodno primeniti standard dužne pažnje „profesionalnog nalogoprimca", a to je u smislu ZOO pažnja dobrog stručnjaka. To ne znači (osim u nekim izuzetnim slučajevima), da propust banke platioca da uoči prevaru i upozori korisnika može voditi zaključku da ona odgovara za celokupan iznos gubitka nastao prevarom, već bi se moralo uzeti da je banka platioca usled tog propusta doprinela nastanku, odnosno uvećanju štete. Drugim rečima, jasno je ko je prouzrokovač štete, ali svi ostali učesnici u platnoj transakciji: platilac, primalac plaćanja i njihove banke, mogu imati određeni (nekada ključni) doprinos u nastanku štete. Zato bi u konkretnom slučaju u kojem se utvrdi da je postojao propust banke platioca u pogledu njene obaveze iz člana 751. stav 2. ZOO, mogao da se primeni (uz neophodno prilagođavanje) institut podeljene odgovornosti iz člana 192. tog zakona.

Praksa NBS

Prema našim saznanjima, za sada nema domaće sudske prakse u vezi sa prevarama sa autorizovanim platnim nalogom, ali postoji praksa Narodne banke Srbije u postupcima po pritužbama korisnika platnih usluga (uglavnom pravnih lica). Narodna banka Srbije je u periodu od 2021., a zaključno sa decembrom 2023. godine rešila 24 pritužbe korisnika (uglavnom privrednih društava) u vezi sa nepravilnim izvršenjem platnih transakcija usled *BEC* prevara. U tim postupcima Narodna banka Srbije je ovlašćena da utvrđuje da li je banka postupala u skladu sa propisima kojima su uređene platne usluge. S tim u vezi, Narodna banka Srbije je u svojim nalazima pre svega cenila postupanje banke sa aspekata prethodno pomenutih odredbi ZPU, našavši da u smislu tih odredaba, ne postoji odgovornost banke za nepravilno izvršenu platnu transakciju. Ipak, Narodna banka Srbije je tim nalazima davala i mišljenje o postupanju banke sa aspekata člana 751. ZOO. S tim u vezi, slučajevi koji su razmatrani mogu se podeliti u nekoliko kategorija.

4 *Detaljnije o tome u slučaju Sjedinjenih Država, vid. Tang, 2015.*

Prvu čine oni slučajevi gde je banka, supsidijarnu obavezu iz člana 751. st. 1. i 2. ZOO u potpunosti ispunila, jer je nakon prijema platnog naloga sa spornim instrukcijama (u smislu sumnje na prevaru), upozorila korisnika i zahtevala da te instrukcije proveri, ali su i pored upozorenja korisnici takve instrukcije potvrđivali. U tim slučajevima, Narodna banka Srbije je jasno stavljala do znanja da se ne može postaviti pitanje odgovornosti banke za doprinos u nastanku štete ni sa aspekata pomenutih odredbi ZOO. Drugu kategoriju, čine slučajevi gde banka nije reagovala na određene indikatore, s tim da se radilo o pojedinačnim, a ne udruženim pokazateljima (npr. korisnik prvi put plaća određenom primaocu, te nema indikatora promene broja računa). U toj situaciji je Narodna banka Srbije iznosila mišljenje da i ako bi se moglo postaviti pitanje podeljene odgovornosti banke za doprinos u nastanku štete, taj doprinos bi bio mali. U treću kategoriju dolaze slučajevi gde su indikatori BEC prevara bili udruženi, a banka nije reagovala i upozorila korisnika. U takvim slučajevima Narodna banka Srbije je iznosila stav da u obzir dolazi primena instituta podeljene odgovornosti za štetu, sa potencijalno značajnijim stepenom odgovornosti banke za doprinos u nastanku štete. U svim slučajevima gde je NBS iznosila stav u vezi sa primenom tog instituta, taj stav je iznošen u formi mišljenja (u okviru obaveštenja o nalazu) jer prema važećim propisima NBS nema ovlašćenja da utvrđuje štetu.

Praksa u Ujedinjenom Kraljevstvu

Ni uporedno posmatrano, ne postoji bogata sudska praksa u vezi sa prevarama sa autorizovanim nalogom. Ipak, u julu 2023. godine, pred Vrhovnim sudom Ujedinjenog Kraljevstva (*United Kingdom Supreme Court,* Vrhovni sud) okončan je jedan veoma zanimljiv slučaj, gde su žrtve (penzionerki par koji je izgubio 700.000 funti uštedevine), veoma sofisticirane prevare sa autorizovanim platnim nalogom tužile banku. Presuda u ovom slučaju je precedent koji će imati izuzetno velike posledice po sudsku praksu u Ujedinjenom Kraljevstvu, a možda i šire, pa joj je zato u ovom radu dato mnogo prostora (Judgment, *Philipp v Barclays Bank* UK PLC, [2023], 25, 12/07/2023, dalje: SC Judgment). Dodatno, u Ujedinjenom Kraljevstvu postoji i praksa Finansijskog ombudsmana *(Financial Ombudsman Service)* koji je u nekoliko slučajeva prevara sa autorizovanim nalogom doneo odluke u korist oštećenih korisnika.

Još jedna zanimljiva presuda iz 2023. godine je iz Sjedinjenih Država, gde je Federalni sud u Virdžiniji našao da je banka primaoca sredstava odgovorna za štetu koju je pretrpeo platilac kao žrtva BEC prevare *(Studco Building Systems US, LLC v. 1st Advantage Federal Credit Union)*. Budući, da se tu radi o odgovornosti banke primaoca sredstava, a ne banke platioca, ovaj slučaj nećemo dalje razmatrati, već je naveden informativno.

Odgovornost banke platioca u slučaju Mrs Philipp v. Barclays

Nakon što je gospodin Filip *(Philipp)* kontaktiran od strane nepoznatog lica koje se predstavilo kao visoki službenik u Organu nadležnom za superviziju finansijskih institucija *(Financial Conduct Authority)* i nakon što je to lice primenjujući socijalni inženjering uspelo da zadobije njegovo poverenje, te da njega i njegovu suprugu *(Mrs Philipp)* ubedi da njihova sredstva nisu sigurna na računu g. Filipa u njegovoj banci i investicionom fondu, on uštedevinu od 950.000 funti najpre prebacuje na račun svoje supruge u drugoj banci *(Barclays)*, a ona odatle, u dve transakcije prenosi 700.000 funti na račune u Ujedinjenim Arapskim Emiratima. Treća transakcija od 250.000 funti nije izvršena, jer je banka *Barclays*, blokirala račune na osnovu informacija policije da su njeni klijenti žrtve prevare.[5] Engleski naziv za ovu vrstu prevare je *vishing*, a za ovaj konkretan oblik *'safe account fraud'*.

5 *Detaljnije o tome u slučaju Sjedinjenih Država, vid. Tang, 2015.*

Stav Apelacionog suda (The Court of Appeal)

Nakon što je prvostepeni sud doneo odluku u skraćenom postupku u kojem je odbio da utvrdi bilo kakvu odgovornost banke, apelacioni sud je usvojio žalbu tužilaca, našavši *da bi se mogla* utvrditi odgovornost banke zbog njenih propusta u vezi sa dužnošću pažnje *(quincecare duty)*. Ovaj institut ugovorne odgovornosti banke prema klijentu opisan je, ali nije primenjen, u slučaju *Barclays Bank plc v Quincecare Ltd.* I pre ovog slučaja bila je prepoznata dužnost pažnje *(duty of care)* banke prema klijentu. Tako je u presudi s početka sedamdesetih, sud u UK našao „da je banka povredila dužnost pažnje koju ima prema svom klijentu, tj. da sprovede ispitivanje pre nego što izvrši plaćanje po čeku, u situaciji gde su postojale razumne osnove za stav da su ovlašćeni potpisnici *zloupotrebili ovlašćenja* u cilju prevare njihovog vlastodavca, odnosno u cilju onemogućavanja njegovih istinskih namera" (*Karak Rubber Co Ltd v Burden,* No 2 [1972] 1 WLR 602, prema SC Judgment, para 41). Institut *quincecare duty* je primenjen u slučaju *Singularis* (Judgment, *Singularis Holdings Ltd v Daiwa Capital Markets Europe Ltd, UKSC 50,30/10/2019*), gde je ocenjeno da je broker, odnosno investiciona banka povredila dužnost pažnje prema klijentu (kompaniji), kada je bez dodatnog ispitivanja relevantnih okolnosti izvršila transakciju po nalogu zastupnika, (koji je istovremeno i jedini vlasnik), iako bi svaki razuman bankar shvatio da postoje očigledni znaci da vlasnik kompanije zloupotrebljava kompaniju kada daje instrukcije da se novac prenese na druge delove njegovih poslovnih operacija (Vid. SC Judgment, para 50).

Iz prethodno navedenog jasno proizilazi da je dotadašnja sudska praksa opisivala i primenjivala institut dužne pažnje banke isključivo u slučajevima gde je zastupnik pravnog lica pokušavao da zloupotrebi sredstva kompanije. S tim u vezi, Apelacioni sud je pokušao da institut qincecare duty reinterpretira na način da ga proširi i na slučaj kada fizičko lice usled prevare izdaje nalog svojoj banci. Analizirajući prethodno navedene (i druge) slučajeve gde je razmatrana primena instituta dužne pažnje, Apelacioni sud primećuje da ključno pitanje nije da li takva dužnost postoji nego kada se ona aktivira, odnosno koji (manji) nivo znanja aktivira za banku takvu obavezu. Pozivajući se na slučaj Singularis, ovaj sud zaključuje da su to situacije kada postoje okolnosti gde bi uobičajeno razborit bankar ispitao te okolnosti (Vid. The Court of Appeal, Approved Judgment [2022], EWCA Civ 116, 14/03/2022, para 28; dalje: CA Judgment). Sud prepoznaje da se obaveze, izvršavanje platnog naloga kako glasi (i u kratkom ugovorenom roku – kom. aut.) i primena razumne veštine i pažnje (u smislu sprečavanja nastanka štete za nalogodavca – kom. aut.) vrše u međusobnoj tenziji, a kako se u datom slučaju te tenzije rešavaju zavisi od konkretnih okolnosti (Vid. CA Judgment, para 34.).

Na argument banke da bi ovakav način primene instituta qincecare duty onemogućio normalno izvršavanje platnih naloga, sud odgovara da je pogrešno taj institut u kontekstu APP prevara razumeti kao obavezu banke da svaki nalog ispituje sa aspekata takve prevare, već obavezu banke da ne izvrši nalog bez dodatne provere samo kada postoje okolnosti koje bi uobičajenog razboritog bankara navele na dodatne provere. Zato sud ističe da je ključno koje su to okolnosti koje bi uobičajenog razboritog bankara navele da izvrši dodatne provere u vezi sa platnim nalogom, te s tim u vezi navodi da je neophodno utvrditi sve činjenice u konkretnom slučaju, odnosno da nije moguće doneti presudu u skraćenom postupku, kako je to učinio prvostepeni sud. U vezi sa tim okolnostima u konkretnom slučaju, Apelacioni sud navodi nekoliko: istorija računa gđe Filip; da je gđa Filip došla lično u poslovnicu banke koja nije njena uobičajena poslovnica; da je zahtevala prenos ogromne sume novca, u njenom slučaju bez presedana; da je samo nekoliko dana pre toga primila taj novac na svoj račun; kao i da se prenos vrši na račun firme Lambi Petroleum u UAE (Vid. CA Judgment, para 71.). Treba ukazati i da sud u pogledu objektivne ocene koje bi okolnosti vodile ka ispitivanju naloga klijenta, kao i u vezi sa administrativnim ograničenjima takvih ispitivanja, prepoznaje značaj određenih bankarskih standarda i dobre prakse, pre svega radi ocene šta je s tim u vezi, izvodljivo (Vid. CA Judgment, para 55.).

Kritički osvrt na presudu Vrhovnog suda

Ovom presudom Vrhovni sud ne samo da nije proširio dotadašnje shvatanje pravila qincecare duty, nego je i osporio njegovo postojanje, našavši da je to zapravo opšte pravilo o dužnoj pažnji banke kao nalogoprimca, koje je pritom suzio.

Sud je više paragrafa presude posvetio obrazloženju svog shvatanja dužne pažnje (duty of care), a znatno manje obrazloženju zbog čega takva dužnost nije postojala u konkretnom slučaju.

Vrhovni sud nije prihvatio stav Apelacionog suda da logika obrazloženja presuda u kojima je razmatran institut qincecare duty nije zasnovana na činjenici da je nalog banci izdao zastupnik klijenta banke, a ne klijent, te da je zato taj institut moguće proširiti i na slučaj kada nalog izdaje sam klijent, fizičko lice. Naprotiv, Vrhovni sud navodi da „kao što je primećeno, u slučaju Singularis, baronesa Hejl (Hale) shvata ovaj zajednički faktor kao definišuću karakteristiku instituta qincecare duty" (SC Judgment, para 53.).

Po mišljenju Vrhovnog suda, prva manjkavost u shvatanju Apelacionog suda (koju ovaj sledi iz presude u slučaju Quincecare), jeste ta što uzima da postoji tenzija između bančine dužnosti pažnje i njene obaveze da izvrši platni nalog klijenta, odnosno pokušava se doći do razumnog zaključka (do kog se već došlo u slučaju Selengor i Karak), polazeći od pogrešne pretpostavke (Vid. SC Judgment, para 62.). Vrhovni sud iznosi stav da je primarna obaveza banke kao platioca (kojoj su podređene sve ostale) da izvrši nalog korisnika kako glasi, a dužnost da se primeni razumna veština i pažnja se aktivira samo ako validnost ili sadržina naloga nije jasna ili ostavlja određeni izbor banci u pogledu načina izvršenja, te da nije moguće iz takve dužnosti kreirati dužnost da se nalog ne izvrši (Vid. SC Judgment, para 63. - 64.). Ovu tvrdnju pokušava da podrži pozivanjem na pravilo o dužnoj pažnji (važi za svaki ugovor o isporuci robe ili pružanju usluga), koje je propisano u zakonima (Statutory law), kao obaveza da se usluge pruže sa razumnom veštinom i pažnjom. Pozivajući se na neke presude (koje nisu u vezi sa presudama na liniji Quincecare) Vrhovni sud svodi dužnu pažnju banke na to da takva pažnja mora da se primeni ako instrukcija za plaćanje ostavlja slobodu banci u pogledu izbora metoda transfera ili u situaciji kada iz instrukcije nije jasno šta banka zapravo treba da uradi (navodeći da u takvoj situaciji dužnost pažnje znači da banka od korisnika zahteva pojašnjenje instrukcije; Vid. SC Judgment, para 34. - 37.).

Moglo bi se reći da Vrhovni sud ovde u potpunosti stavlja u stranu presude Selengor i Karak (iako prethodno tvrdi da se u tim presudama došlo do razumnih zaključaka) jer u ovim slučajevima dužna pažnja nije shvaćena samo kao obaveza da se zahteva preciziranje nepotpunih instrukcija, već kao obaveza da se banka uzdrži od izvršenja naloga dok ne izvrši dodatno ispitivanje, ako bi razuman i razborit bankar imao osnova da poveruje da zastupnik pokušava da prevari svog vlastodavca, klijenta banke. Vrhovni sud, ovo pokušava da „pokrije" tako što umesto zloupotrebe ovlašćenja zastupnika kompanije (misuse of authority), uvodi shvatanje po kojem u tim slučajevima ovlašćenje za izdavanje takvih naloga zapravo ne postoji (absence of authority), pa je tu sporna validnost tih naloga (Vid. SC Judgment, para 69. - 89.) Sud tako zaključuje da kada se načela u vezi sa pravom zastupanja primene na seriju Quincecare slučajeva (Selangor, Karak Rubber, Lipkin Gorman, Singularis), obrazloženje za pravne zaključke iznete u tim slučajevima postaje jasno. U situaciji u kojoj zastupnik pokušava da radi ostvarivanja sopstvenog interesa prevari kompaniju čiji je zastupnik, on nema stvarno ovlašćenje da izda platni nalog u ime kompanije (zastupnik i tada generalno ima pretpostavljeno ovlašćenje, kao predstavnik kompanije prema banci, da izdaje platne naloge, ali ne i ako okolnosti sugerišu nepoštenost koja je banci očigledna i koja bi razumnog bankara navela da pre izvršenja instrukcije proveri ovlašćenja zastupnika; Vid. SC Judgment, para 90.).

Drugim rečima, Vrhovni sud smatra da i kod slučajeva na liniji Quincecare nema nikakve posebne dužnosti banke da se uzdrži od izvršenja platnog naloga nego u tim slučajevima nalog nije zaista autorizovan od strane klijenta, tj. nije ni izdat, a banka je dužna da to prepozna u određenim okolnostima.

Vrhovni sud zaključuje, Qincecare duty nije nikakav specijalni institut već njegovo ispravno razumevanje znači primenu opšteg pravila dužne pažnje (duty of care) banke da tumači, utvrđuje i dela u skladu sa klijentovim instrukcijama. Kada banka ima razumne osnove da veruje da je platni nalog dat od strane zastupnika navodno u ime klijenta, zapravo pokušaj prevare klijenta, ova dužnost zahteva da banka odustane od izvršenja tog naloga, dok ne proveri da li je taj nalog zaista autorizovan od strane klijenta (SC Judgment, para 97.).

Ipak, ovako shvaćenu dužnost pažnje teško je primeniti npr. u slučaju Singularis, gde je sud utvrdio povredu dužnosti pažnje na strani banke, a gde je platni nalog kojim su oštećeni pre svega poverioci kompanije (a ne sama kompanija, drugi vlasnici, investitori i sl.) izdao zastupnik koji je istovremeno bio jedini akcionar, direktor, itd. Drugim rečima, Vrhovni sud očigledno stvara jednu fikciju kako bi izbegao konflikt dve dužnosti banke, a to je da kada prepozna u nalogu zastupnika potencijalnu zloupotrebu, banka zapravo prepoznaje da nema ovlašćenja za takav nalog, pa onda se i ne uzdržava od izvršenja naloga nego se uzima da nalog nije ni izdat.

Na osnovu rečenog, Vrhovni sud zaključuje da se ovakvi principi ne mogu primeniti na slučaj gde je klijent žrtva prevare, jer u toj situaciji nema sumnje u pogledu validnosti ovlašćenja, budući da sam klijent daje jasne instrukcije banci i nema potrebe da se nalog ispituje sa aspekta ovlašćenja da se on kao takav izda (Vid. SC Judgment, para 100.).

Iako zastupnik gđe Filip ukazuje da i u slučaju APP prevare, kao i u slučajevima gde zastupnici pokušavaju da prevare svoje vlastodavce, platni nalog ne odražava pravu nameru klijenta, Vrhovni sud odbacuje takav argument uz obrazloženje da to što su namere ili želje proistekle iz pogrešnih verovanja ne čini ih manje realnim ili zaista postojećim (Vid. SC Judgment, para 101.-102.). S tim u vezi, Vrhovni sud stavlja po strani činjenicu da je upravo u paragrafu 40. i 41. citirao presude Selengor i Karak u delu gde se navodi da ovlašćeni potpisnici zloupotrebljavaju njihova ovlašćenja u cilju prevare njihovog nalogodavca ili kako bi na drugi način izigrali njegove prave namere „poražavaju" prave namere klijenta (defeating his true intention).

Sud dalje navodi da u Engleskom pravu prevara ne uzrokuje ništavost ugovora ili drugog pravnog posla, već lice koje je pogođeno prevarom može zahtevati da se takav posao poništi, s tim da to poništenje utiče samo na odnos sa licem koje je učinilo prevaru, ali ne i u odnosu na treća lica, u ovom slučaju banku. Drugim rečima, sud zaključuje da je činjenica da je klijentov nalog uzrokovan prevarom ovlašćuje tog klijenta da zatraži povraćaj od lica koje je prevaru izvršilo, ali ne dovodi u pitanje punovažnost platnog naloga, niti daje osnova za potraživanje prema banci (Vid. SC Judgment, para 103.-105.).

Ipak, valja napomenuti da Vrhovni sud prihvata da dužnost pažnje u smislu dodatnog ispitivanja instrukcija postoji kada se radi o licu sa nedostatkom mentalnih kapaciteta (Vid. SC Judgment, para 99.). S tim u vezi, čudi da u tom delu nije povučena paralela sa licem koje je žrtva prevare, posebno u slučaju para Filip, koji su kao penzioneri bili pod tolikim uticajem prevaranta, odnosno u takvoj zabludi da su odbijali upozorenja svojih prijatelja i policije, a poslednja transakcija je sprečena upravo zahvaljujući njima, iako je gđa Filip insistirala da se platna transakcija izvrši. Drugim rečima, takav nivo zablude je svakako doveo do manjka mentalnih kapaciteta prilikom donošenja odluka, odnosno izdavanja platnog naloga.

Sud je ipak razmatrao ograničenja u pogledu izvršenja validnog naloga koji je izdalo zaista ovlašćeno lice. Kao primere navodi slučajeve gde bi prevoznik koji je preuzeo obavezu da odveze i istovari robu u neku fabriku, pa po dolasku na to mesto nađe fabriku u požaru delovao nerazumno ako bi se držao preuzete obaveze. Vrhovni sud nalazi da je logika ovde takva da je razumno uzdržati se od naloga kada je jasno da bi njegovo izvršenje štetilo nalogodavcu, pod uslovom da su okolnosti koje ukazuju na tu štetnost bile nepoznate nalogodavcu kada je izdao nalog. Primenjujući to na slučaj gđe Filip, Sud nalazi da bi ovakvo pravilo važilo u situaciji u kojoj banka dobije informaciju od policije da je njen klijent potencijalna žrtva zloupotrebe (što se u pogledu poslednje transakcije i dogodilo kada je banka i pored insistiranja gđe Filip odbila izvršenje naloga). Međutim, zaključuje sud, okolnosti koje ukazuju na prevaru bile su dobro poznate klijentu kada je izdala platne naloge, jer je kroz instrukcije za plaćanje potvrdio sve te okolnosti, i pritom je bio nepokolebljiv u nameri da se nalozi izvrše, pa banka nije imala razlog da sumnja da je klijent sa tim okolnostima nije upoznat (Vid. SC Judgment, para 107.-110.).

Sud je zapravo ovde kontradiktoran jer su okolnosti prevare bile dobro poznate klijentu i u pogledu poslednje transakcije koju je banka odbila da izvrši, a ona je to odbila ne zato što okolnosti koje ukazuju na prevaru nisu bile poznate klijentu, nego zato što je banka dobila informaciju od policije da se izvesno radi o prevari. Dakle, ovde se ne može primeniti logika na koju se sud poziva, već razlika postoji u stepenu saznanja na strani banke kao nalogoprimca.

Na kraju, Vrhovnom sudu je konflikt dve suprotstavljene dužnosti banke bio neprihvatljiv iz još jednog razloga koji nije vezan direktno za ovaj slučaj, pa ni samo za prevare sa autorizovanim platnim nalogom. Naime, taj sud smatra da sudija u slučaju Quincecare, uočivši konflikt (između dve dužnosti banke, koji u realnosti ne postoji) taj sukob nije mogao da reši na principijelan način, već je morao da se osloni na politička razmatranja (Vid. SC Judgment, para 65.-66.). Problem sa ovim metodom je što on nije adekvatan za utvrđivanje ugovornih obaveza. Koje pravilo bi predstavljalo „odgovarajući kompromis" ili „fer balans" između širokih političkih ciljeva je pitanje za zakonodavca. Prilikom odlučivanja da li postoji određena obaveza ugovorne strane koja nije izričito ugovorena, sud ima znatno skromniju ulogu da obezbedi primenu pretpostavljene volje ugovornih strana (SC Judgment, para 67.).

Ovaj stav zaslužuje poseban komentar. Naime, u odsustvu određenih pravila koja bi regulisala nove okolnosti, poput prevara sa autorizovanim nalogom, odnosno kada prilikom propisivanja tih pravila nisu uzete te specifične okolnosti, sud bi morao (posebno u common law sistemu) da odredi taj balans, kada za to postoji osnov u opštoj odredbi zakona ili sudskoj praksi, kao što je postojao u Quincecare slučajevima. Ovde treba citirati stav čuvenog Lona Fulera koji kaže: „Common law nije proizvod rada jednog sudije, već saradnje velikog broja sudija tokom dugog perioda vremena. Tokom njegove istorije primena njegovih pravila je unapređivana i oplemenjivana. Istovremeno, ta pravila su često revidirana kako bi se obezbedila njihova delotvornost. Šta je sud rekao u prethodnom slučaju uvek je predmet reinterpretacije u novoj situaciji pred sudom. Tada se polje primene precedenta ne određuje isključivo u svetlu ciljeva koje je imao na umu sud koji je doneo raniju odluku, već u svetlu novih ciljeva, koji proširuju značenje prethodnih, a koji nisu mogli biti artikulisani na osnovu ograničenog činjeničnog stanja koje je predstavljalo podlogu za donošenje precedenta" (prema Dević, 2007).

Dakle, prednost common law sistema u odnosu na kontinentalni, jeste upravo u tome što i sudovi stvaraju pravo i kroz reinterpretaciju precedenata mogu mnogo brže da prilagode pravo novim situacijama i konkretnim slučajevima, bez potrebe da (kao u kontinentalnom sistemu) čekaju zakonodavca koji po pravilu kaska za praksom (i realnošću), a i kada reaguje, neretko je potrebno vreme da se među sudovima uobliči šta je zakonodavac zapravo „rekao" ili „hteo da kaže". Ta prednost ovde nije iskorišćena.

Kodeks o povraćaju sredstava u slučaju prevara sa autorizovanim nalogom

Na stav Vrhovnog suda da treba sačekati zakonodavca, svakako je uticalo i to što su i same banke preduzele određenu inicijativu da ovu oblast samostalno i dobrovoljno regulišu (samoregulacija)[6] pod pokroviteljstvom Odbora za kreditne standarde (Lending Standards Board - organizacija u UK koje preduzima aktivnosti u vezi sa samoregulacijom banaka i drugih kreditora). Tako je jedan deo banaka (među kojima je i Barclays), dobrovoljno prihvatio primenu Kodeksa o postupanju u slučaju prevara sa autorizovanim platnim nalogom (Contingent Reimbursement Model Code for Authorised Push Payment Scams - Kodeks) koji je stupio na snagu maja 2019. godine, a kojim je određeno u kojim slučajevima su banka platioca, odnosno primaoca plaćanja dužne da nadoknade gubitak platiocu (https://www.lendingstandardsboard.org.uk/wp-content/). Kodeks se primenjuje samo u slučaju domaćih transakcija. Dodatno, treba ukazati na dva ključna standarda, instituta u tom kodeksu, od čijeg načina primene zavisi alokacija gubitka (korisnik ili banka/banke).

Prvi standard je krajnja nepažnja, gde pružalac platnih usluga nije obavezan da nadoknadi gubitak korisniku ako dokaže postojanje takve nepažnje. U Kodeksu je navedeno nekoliko izričitih primera takve nepažnje kao što su: 1) ignorisanje efektivnih upozorenja koja su data od pružaoca platnih usluga; 2) nepreduzimanje odgovarajuće aktivnosti od strane korisnika nakon jasnog negativnog rezultata potvrde primaoca plaćanja; 3) izdavanje naloga za prenos bez razumne osnove da korisnik veruje da je primalac lice kojem je on hteo da plati ili da se plaćanje vrši za pravu robu i usluge, itd. - uzimajući pritom u obzir karakteristike korisnika, kompleksnost i soficistiranost prevarne šeme. Pored ovih exempli causa slučajeva krajnje nepažnje u Kodeksu je dat i opšti pojam krajnje nepažnje. Izgleda da se bez ovog standarda ne može ni na Ostrvu, pa se može očekivati da će taj ili sličan standard i zakonodavac koristiti prilikom propisivanja pravila za alokaciju gubitaka, što će loptu iz parlamenta opet vratiti na teren suda.

Drugi standard od čije primene zavisi alokacija gubitka (banka platioca ako nije ispunila sve zahtevane standarde ili fond banaka ako banka jeste primenila sve standarde) jeste „scenario bez krivice“ (no - blame scenario), što bi opet u slučaju eventualnog spora, zahtevalo procenu suda, da li je banka u konkretnom slučaju ispunila sve standarde koji se od nje očekuju. [7]

Dakle, i sa zakonodavnom intervencijom sudovi će morati da se upuštaju u određena „politička“ razmatranja, odnosno da u svakom konkretnom slučaju daju određeno značenje pravnim standardima.

Praksa Finansijskog ombudsmana

Finansijski ombudsman (The Financial Ombudsman Service, FOS) je u Ujedinjenom Kraljevstvu uspostavljen od strane parlamenta u cilju rešavanja pritužbi korisnika na postupanje davalaca finansijskih usluga, na fer i nepristrasan način. Kada je reč o prevarama sa autorizovanim platnim nalogom, finansijski ombudmsan je imao različite odluke detaljno uzimajući u obzir sve okolnosti konkretnog slučaja.

Tako je u slučaju korisnice koja je bila žrtva prevare sa autorizovanim platnim nalogom, koja je izvršena preko telefona, a gde je ona od strane prevaranta navedena da izvrši plaćanje na siguran račun jer su joj sredstva ugrožena, Ombudsman zaključio da je u konkretnom slučaju banka (koja je potpisnica Kodeksa) nije dokazala da je u smislu Kodeksa korisnica postupala sa krajnjom nepažnjom te je banci naložio da izvrši povraćaj ukupnog iznosa spornih transakcija (Vid. FOS, DRN-3130787, 28 January 2022).

[6] *Detaljnije o pojmu samoregulacije vid. Jovanić, 2019.*

[7] *Detaljnije o Kodeksu i dosadašnjim efektima njegove primene vid. Maher, 2021, 140.-145.*

Takođe, Ombudsman je u slučaju jednog preduzetnika koji je bio žrtva BEC prevare odlučio da mu njegova banka izvrši povraćaj celokupnog iznosa sporne međunarodne transakcije od 24.235,97 funti (iako je korisnik zahtevao da mu banka nadoknadi 50%). Ombudsman je u svojoj odluci ukazao da je banka od te institucije dobila više mišljenja koja jasno kažu da banka ima obavezu da prepozna i reaguje u slučaju sumnjivih (u smislu rizika od prevare) transakcija, te da je u konkretnom slučaju korisnik iznenada promenio račun na koji plaća dugogodišnjem poslovnom partneru, kao i da se radi o transakciji koja je za korisnika neuobičajeno visoka. Ombudsman je analizirao i sa kojim stepenom pažnje je postupao oštećeni preduzetnik i zaključio da na njegovoj strani ipak nije bilo nepažnje, jer je ispravo posumnjao i zahtevao da poslovni partner sa kojim je verovao da komunicira, obrazloži razlog promene računa, ali je prevarant koji je hakovao imejl primaoca bio izuzetno uverljiv koristeći naloge više radnika primaoca sredstava koji su potvrđivali razloge promene instrukcija za plaćanje. Ovakva odluka je doneta nezavisno od Kodeksa koji se, kako smo rekli ne primenjuje na međunarodne platne transakcije (Vid. FOS, DRN-3087679, 6 May 2022.).

Nakon ovih odluka iz 2022. godine, navešćemo i jednu odluku iz novembra 2023. godine (nakon presude Vrhovnog suda) u vezi sa 'safe account' prevarom (korisnik je izgubio 50.000 funti), gde se takođe radilo o međunarodnim transakcijama (Vid. FOS, DRN-4453209). Ombudsman sada nije našao odgovornost Banke kao u prvom slučaju koji smo naveli. Zapravo je zaključio da je banka korisnika ispunila obavezu da prepozna i reaguje u slučaju sumnjivih transakcija jer je detaljno upozorila korisnika, pri čemu su ta upozorenja bila dovoljno konkretna da obuhvate upravo scenario prevare kojoj je korisnik bio izložen. Tačno je da za razliku od prvog slučaja, ovde Banka prilikom izvršenja druge transakcije (prva je bila u iznosu od svega 76 funti) upozorila korisnika, ali je teško oteti se utisku da je Ombudsman prilikom donošenja ove odluke uzeo u obzir i presudu Vrhovnog suda u slučaju gospođe Filip.

Odgovor Evropske komisije - Predlog uredbe o platnim uslugama

Opis pravnog režima odgovornosti banke platioca u slučaju prevara sa autorizovanim platnim nalogom, te nužda da se radi utvrđivanja te odgovornosti u pomoć pozivaju opšte odredbe civilnog zakonika jasan su dokaz da specijalni režim koji je uvezen iz direktiva o platnim uslugama ima pravne praznine. Očigledno svesna tih praznina, Evropska komisija u svom predlogu novih propisa o platnim uslugama, ovaj put u formi uredbe (Proposal for a Regulation of the European Parliament and of the Council on payment services in the Internal Market and amending Regulation (EU) No 1093/2010, Brussels, 28.6.2023), jednim delom popunjava te praznine. Pored ovog predloga, postoji i Predlog treće direktive o platnim uslugama, ali se on bavi isključivo statusnim pitanjima u vezi sa pružaocima platnih usluga, kao što su osnivanje, nadzor i slično (Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market[...], Brussels, 28.6.2023).

U poglavlju 4. Predloga uredbe koje je posvećeno autorizaciji platnih transakcija, u članu 49. predviđeno je da banka primaoca na zahtev banke platioca verifikuje da li račun na koji glasi platni nalog pripada licu koje je u tom nalogu navedeno kao primalac sredstava. Ako postoji neslaganje banka obaveštava o tome platioca, ali ako on i pored toga zahteva da se transakcija izvrši, takva transakcija će se smatrati odobrenom. Platioci će moći da isključe tu uslugu, ali će tada morati da budu upozoreni da sredstva mogu da završe na računu koji ne pripada primaocu iz naloga.

U svakom slučaju, platilac ne može snositi gubitke ako ga njegov pružalac platnih usluga nije obavestio o tome da postoji neslaganje, osim ako je optirao da ne koristi tu uslugu.

U slučaju prevare sa lažnim predstavljanjem (impersonation fraud, spoofing), gde je korisnik žrtva prevare nepoznatog lica koje se predstavljalo kao zaposleni njegovog pružaoca platnih usluga, taj pružalac bi u skladu sa članom 59. Predloga uredbe bio dužan da vrati korisniku celokupan iznos, na prevaru autorizovane transakcije, ako je korisnik prevaru odmah prijavio policiji i pod uslovom da pružalac platnih usluga ne može da dokaže da je korisnik postupao sa krajnjom nepažnjom ili da je eventualno i sam učesnik u toj prevari. Dakle, ovim se za razliku od Direktive 2015/2366 koja „pružaocu platnih usluga koji izvršava nalog u skladu sa jedinstvenom identifikacionom oznakom obezbeđuje široku zaštitu" (Benjamin, 2019), uvodi pretpostavka njegove odgovornosti, koju on može da obori dokazivanjem da je korisnik postupao sa krajnjom nepažnjom.

Kao što se vidi opet se primenjuje standard krajnje nepažnje kako je to bio slučaj i kod prve i druge direktive o platnim uslugama, s tim da je u slučaju tih propisa on korišćen samo kod zloupotrebe platnih instrumenata. Kada je reč o odgovornosti pružaoca platnih usluga u slučaju te vrste zloupotreba, Predlog uredbe je uglavnom u okvirima postojećih rešenja iz direktiva, uz dve razlike. Prva je ta, da nadležni organi (koji vrše nadzor nad primenom uredbe) mogu da umanje odgovornost platioca zbog toga što nije ispunio obaveze u pogledu korišćenja platnog instrumenta i njegove zaštite, ako nije postupao prevarno, tj. ako nije namerno odao određene podatke u vezi platnog instrumenta, uzimajući u obzir posebno prirodu sigurnosnih elementa i specifične okolnosti pod kojima je platni instrument izgubljen, ukraden ili zloupotrebljen. Druga razlika je ta, da ako nije primenjena tzv. jaka autentifikacija korisnika (strong customer authentication) nema odgovornosti platioca, osim ako je delao prevarno.

Pored navedenog poglavlja koje u pogledu zloupotreba i prevara uvodi strožija pravila (pretpostavke odgovornosti) za pružaoce platnih usluga, u 8. poglavlju Predloga uredbe daje se niz značajnih ovlašćenja organima država članica koji su nadležni za nadzor nad primenom tih pravila. Ta ovlašćenja uglavnom uključuju nadzor nad pružaocima platnih usluga na način koji se u Srbiji već sprovodi od strane Narodne banke Srbije (posredna i neposredna kontrola), a koji podrazumeva ovlašćenja da se tim pružaocima usluga nalažu određene mere radi otklanjanja nepravilnosti, kao i da im se izreknu administrativne novčane kazne. Ipak, usvajanje ovog predloga i njegova implementacija u srpsko zakonodavstvo donelo bi dodatne mogućnosti u toj kontroli poput mogućnosti da se od nadležnih organa pribavljaju podaci u vezi sa određenim krivičnim istragama i postupcima, kao i da se prema pružaocima platnih usluga koriste mere kao što su periodična kaznena plaćanja ili objavljivanje izrečenih mera i sankcija.

Zaključak

Kada se dakle analiziraju postojeći propisi, novi predlozi, kao i (kvazi) sudska domaća i uporedna praksa, može se izvesti zaključak da banke platioca nemaju razloga da budu ušuškane u uverenju da na njihovoj strani ne može postojati odgovornost za gubitak nastao usled prevare sa autorizovanim platnim nalogom. Bez obzira što je Vrhovni sud u UK suzio dosadašnje shvatanje dužne pažnje na strani banke, sve veći broj i obim zloupotreba u platnom prometu, pre ili kasnije dovešće do primene principa da rizik snosi onaj ko njime može bolje da upravlja. Da je to tako, potvrđuju između ostalog Kodeks, Predlog nove uredbe o platnim uslugama Evropske komisije, praksa Finansijskog ombudsmana u UK, pa i Narodne banke Srbije.

Do donošenja novih propisa ili određenih aktivnosti banaka u pravcu samoregulacije, sudovi, regulatori i supervizori bankarskog sektora, imaće presudnu ulogu u proceni postojanja eventualne odgovornosti banke platioca. Uostalom, i novi propisi će sigurno biti zasnovani na određenim pravnim standardima kako bi obuhvatili veliki broj različitih tipova prevara (sa autorizovanim i neautorizovanim transakcijama), što će opet značiti prilično široka diskreciona ovlašćenja za sudove i supervizore.

U svakom slučaju, prema postojećim domaćim propisima, eventualna odgovornost banke platioca u slučaju izvršenja autorizovanog platnog naloga koji je rezultat prevare, uglavnom ne bi trebalo da vodi ka njenoj isključivoj odgovornosti. Izostanak preduzimanja mera koje bi se u smislu domaćeg Zakona o bankama mogle shvatiti kao mere opreznog bankarskog poslovanja, odnosno izostanak upozorenja platiocu kada postoje pokazatelji potencijalne prevare, mogao bi u smislu srpskog civilnog zakonika voditi podeljenoj odgovornosti banke sa platiocem za nastalu štetu (shodnom, odnosno prilagođenom primenom člana 192. ZOO). S tim u vezi, u pogledu ispunjenosti uslova za aktiviranje obaveze banke platioca iz člana 751. stav 2. ZOO, najvažnije je utvrditi kako je banka postupala u konkretnom slučaju, u smislu postojanja odgovarajućih internih procedura za prepoznavanje i prevenciju prevara i načina njihove primene. Drugim rečima, važno je utvrditi da li je banka uspostavljanjem adekvatnih politika, procedura i softverskih alata, omogućila uobičajenom, razumnom bankaru da prepozna okolnosti koje zahtevaju proveru platnog naloga. Dakle, da bi se procenilo da li je u konkretnom slučaju razumni bankar mogao, odnosno morao da posumnja u ispravnost instrukcije, sud bi najpre morao da ceni ispunjenost standarda opreznog bankarskog poslovanja u izvršavanju predmetnih platnih transakcija. Da bi to cenio, sud bi trebalo da od stručnjaka u oblasti platnih usluga (ne od veštaka opšte ekonomske struke) ili institucija nadležnih za kontrolu banaka, pribavi mišljenje o postupanju banke u konkretnom slučaju.

Jer, „da bi banke ostvarile srazmernost između zaštite korisnika od internet prevara i troškova dodatne zaštite, sudovi bi prilikom odlučivanja o odgovornosti trebalo da prate jedinstvenu i objektivnu 'najbolju praksu' kako je određena od strane stručnjaka iz nadležnih institucija" (Tang, 2015). U suprotnom, nametanjem bezbednosnih zahteva u pružanju platnih usluga koji su izvan onoga što je ekonomski razumno i opravdano, moglo bi proizvesti negativne efekte za većinu korisnika tih usluga, jer bi se nesrazmerni troškovi bezbednosnih mehanizama prelili na cenu i/ili kvalitet usluga.[8] Osim toga, suviše rigorozni zahtevi prema banci mogli bi dovesti do moralnog hazarda na strani platioca.

Literatura

1. Burrow K. R., Increased Bank Liability for Online Fraud: The Effect of Patco Construction Co. v. People's United Bank, North Carolina Banking Institute, 2013.
2. Benjamin, G., Payment Transactions under the E.U. Second Payment Services Directive - An Outsider's View, Texas International Law Journal, vol. 54, no. 2, 2019.
3. Dević D., Kritika Fulerovog shvatanja prirodnog prava, Pravni fakultet Univerziteta u Beogradu, Beograd, 2007.
4. Jovanić T., Uvod u Ekonomsko pravo, Pravni fakultet Univerziteta u Beogradu, Beograd, 2019, 103.
5. Kjørven E. M., Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe, European Business Law Review, Issue 1, 2020.

[8] *Vidi više o tome: Burrow, 2013, 394-398.*

6. Levitin J. A., Private Disordering? Payment Card Fraud Liability Rules, Brooklyn Journal of Corporate, Financial & Commercial Law, Vol. 5, 2010.
7. Maher R., A Critical Analysis of Recent Efforts in the United Kingdom to Tackle, Authorised Push Payment Scams and the Impact on the Bank-Customer Relationship, Trinity College Law Review, Vol. 24, 2021.
8. Trajković M., Komentar uz član 751. ZOO, Perović S. (red.) (1995) Komentar Zakona o obligacionim odnosima, knjiga II, Beograd 1995.
9. Tang L. S., Increasing the Role of Agency Deference in Curbing Online Banking Fraud, North Dakota Law Review, Vol 91, 2015.
10. Presuda Vrhovnog suda Ujedinjenog Kraljevstva (The Supreme Court, Judgment, Philipp v Barclays Bank UK PLC, [2023], 25, 12/07/2023).
11. Presuda Apelacionog suda u Ujedinjenom Kraljevstvu, (The Court of Appeal, Approved Judgment [2022], EWCA Civ 116, 14/03/2022)
12. Presuda Visokog suda u Bristolu, Ujedinjeno Kraljevstvo, (The High Court of Justice, Business & Property Courts in Bristol, Approved Judgment, [2021] EWHC 10 (Comm), Judge Russen QC, Fiona Lorraine Philipp and Barclays Bank UK PLC, 18/01/2021)
13. Presuda Vrhovnog suda Ujedinjenog Kraljevstva (Judgment, Singularis Holdings Ltd v Daiwa Capital Markets Europe Ltd, UKSC 50,30/10/2019)
14. Presuda Federalnog suda Sjedinjenih Država, za istočni distrikt Virdžinije, (The United States District Court for the Eastern District of Virginia, Case 2:20-cv-00417, Studco Building Systems US, LLC v. 1st Advantage Federal Credit Union, Memorandum Opinion and Order, 12.1.2023.)
15. Odluke Finansijskog ombudsmana u Ujedinjenom Kraljevstvu, (The Financial Ombudsman Service Decisions: DRN-3130787, 28 January 2022; DRN-3087679, 6 May 2022; DRN-4453209, November 2023.)

Received: 02.02.2024.
Accepted: 08.02.2024.

THE LIABILITY OF THE PAYER'S BANK IN CASE OF AUTHORISED PUSH PAYMENTS FRAUD

Bojan Terzić
Head of Financial Consumer Protection Department,
National Bank of Serbia
bojan.terzic@nbs.rs

DOI: 10.5937/bankarstvo2304104T

Summary: The Authorised Push Payment (APP) fraud is a great danger for payers due to the fact that the value of these transactions is often significantly higher in comparison to unauthorised ones (misuse of payment instruments), while chargeback options are limited. Payers' banks are currently convinced that they cannot bear the losses in the case of APP fraud. Their assurance is based on special payment services regulations. Still, general rules of Serbian contract law, which should be applicable as additional rules, oblige the payer's bank to warn the payer if a bank finds that the payment order could be harmful for them. However, as a precondition for the activation of this bank's duty, a reasonable expectation that an ordinary prudent banker could notice something suspicious related to the payment order should arise. In this case, if the bank failed to warn the client, rules related to divided liability for damage from the Law on Contracts and Torts could be applied.

Key words : Authorised Push Payment fraud; Business Email Compromise; Payment service regulations; Quincecare Duty; Payer's bank's liability.

JEL classification: G21, K12, K22, K42

Introduction

The Internet and electronic communications, aside from vast benefits, also bring certain risks of which payment service users are often unaware, or which they overlook. While the risk of payment card fraud due to loss or theft of the card or its data is well known to payment service users, the Authorised Push Payments fraud is not familiar to the wider base of users, although the consequences of such fraud, in terms of losses, far surpass card fraud. The words authorised and push originate from the fact that the payer themself, as a fraud victim, instructs the bank to transfer the funds to an account controlled by criminals, making such a transaction authorised from the point of view of the bank.

The most dangerous form of APP fraud currently present in Serbia is the Business Email Compromise fraud. The scheme behind this fraud is usually based on the criminals gaining access to business correspondence (by accessing the email account of one of the parties in correspondence), and, by viewing all data from previous correspondences, convincingly lead one party to transfer funds into an account under their control.

Aside from the intent to warn the expert public and the greater audience of this ongoing challenge, this paper aims at considering existing regulation, local and comparative practices, and addressing the issue of a bank's and client's liability for losses (often amounting to several dozens, even hundreds of thousands of euros) caused by Authorised Push Payments frauds. Seeing as how such a transaction has been undoubtedly authorised by users, the banks are, seemingly, convinced that they cannot be responsible for the client's loss, based on existing regulation. However, is that truly the case? This paper tries to provide an answer to that question by analysing local regulations and providing an overview of the practice of the National Bank of Serbia, while relating them to certain rules of common law and

Data on Business Email Compromise Fraud

According to data from the National Bank of Serbia's questionnaire, the total amount lost in payment card frauds in 2021 is RSD 93 million (with 78.6 from online fraud, 2.5 from POS fraud, and 11.9 at ATMs). Users were refunded RSD 74.2 million. In 2022 the total amount lost in payment card fraud is RSD 179.7 million (with 129.8 from online fraud, 41.6 from POS fraud, and 8.2 at ATMs). A total of RSD 141 million was refunded to users.

When it comes to Business Email Compromise fraud in 2021, 105 transfers were completed, amounting to a total of RSD 251.5 million, while 2022 has seen 108 transactions amounting to RSD 418 million (99% of the total amount refers to legal entities' payments in international payment transactions). In 2021, 22 transactions were refunded, in the amount of RSD 54.2 million, while 22 transactions were also refunded in 2022, in the amount of RSD 68.8 million.

The aforementioned data indicates that, in the case of payment card fraud (in 2022), the average transaction amount is around RSD 9,000, while the average transaction amount in Business Email Compromise fraud is around RSD 3,870,000. Additionally, card users were refunded 78-80% of the misused funds, while payers' banks managed to refund 16-20% of funds in cases of BEC fraud.

Aside from this comparison and seeing as how all BEC transactions were done in international payment systems, it is also useful to compare the number and value of transactions in local and international payment systems (excluding card transactions). The Report of the National Bank of Serbia (Overall NBS RTGS System and Clearing System Indicators in 2022: https://nbs.rs/en/ciljevi-i-funkcije/platni-sistem/statistika/index.html) provides data from which we can extrapolate that the average number of daily payments per participant in the system exceeds 34,000, while the average value of transactions in this payment system is RSD 473,210, or around EUR 4,000. On the other hand, the example of one of the banks (with a significant share in international payment transactions) shows that in 2022 an average of 1,206 international transactions were completed daily, with a total value of EUR 45.9 million, and with an average transaction amount of EUR 38,000.

The Legal Framework Regarding Authorised Push Payment Fraud

The loss allocation rules are important not only because of their distributional consequences, but because of the incentives they create. The greater a party's liability for fraud losses, the greater incentive the party will have to take care to avoid fraud (Levitin, 2010). For payment-transaction fraud, questions of loss allocation are regulated by national rules implementing the liability regime for unauthorised payment transactions under the payment services directive. For other financial services, these questions are resolved according to general rules on contract and tort (Kjørven, 2020).

This is only partially factual (both for EU members and for Serbia), since the issue of liability in cases of Authorised Push Payment fraud was referred to in directives on payment services, through provisions regulating the situation where a transaction was done incorrectly, due to the payer entering an incorrect account number. On the other hand, although in APP fraud the payer enters and authorises an incorrect account number, it is unclear whether the provisions of European legislators were meant to regulate only technical errors and similar oversights of the payer, or if they were meant to allocate risk in the same manner (at the payer's expense) in cases of "error" caused by fraud.

Law on Payment Services

According to the Law on Payment Services (Official Gazette of the RS, no 139/2014, 44/2018, hereinafter: LPS), the legal position of an issuer of a payment order (payer) resulting from fraud is significantly less favourable than that of an owner of a misused payment card. Namely, the responsibility for the proper execution of an authorised payment order is governed by the provisions of Article 55, paragraph 1 and 2 of the LPS, which transposed the provisions of Article 74 paragraph 1 and 2 of the first Payment Services Directive (Directive 2007/64/EC, OJ L 319, 5.12.2007, hereinafter: PSD1). Provisions with the same content also exist in the currently valid, second Payment Services Directive (Directive (EU) 2015/2366, OJ L 337/35, 23.12.2015, hereinafter: PSD2). Those provisions stipulate that, if the payment order was executed in accordance with the unique identifier of the payee from that order, it is considered that the order was correctly executed in the part that refers to the determination of the payee, regardless of other data submitted to the payment service provider and that if the unique identifier provided by the payment service user to the payment service provider is incorrect, the payment service provider shall not be liable for the non-execution or incorrect execution of a payment transaction. In Article 2, paragraph 1, item 19) the LPS defines that the unique identifier is a combination of letters, numbers and/or symbols specified to the payment service user by the payment service provider to be used in a payment transaction to identify unambiguously the respective payment service user and/or its payment account.

The unanimously taken stance in practice is that the unique identifier in the local payment system in the number of a current account in a bank, that is, the number of some other payment account with an electronic money institution or a payment institution, while in the case of international payment systems, it is the International Bank Account Number (IBAN).

To summarise, the LPS is fully clear and unambiguous in this matter. If a bank transfers funds to an account listed in the payment order, authorised by the payer (in a way determined by the agreement on payment services)[1], the bank is not liable as a payer's payment service provider for the non-execution or incorrect execution in the payment transaction. In other words, in agreement with the mentioned provisions of the LPS, banks consider the owner of the account listed in the payment order as the payee, and not the person whose name, surname, address, etc. are listed in that payment order. The payer's bank must check the validity of the account listed in the payment order in terms of its logistical control (of all elements of the account number) but, in accordance with the mentioned provisions of the LPS, the bank is not obligated to "match" the account number and the recipient of the funds.

Nonetheless, from the moment when the payer reports a fraud, the bank is obligated, in accordance with Article 55, paragraph 3 of the LPS, to take all reasonable measures to return the funds, and, when the refund is no longer possible, to determine the flow of assets and notify the client. It is important to note that to accomplish the mentioned goal (refund, or information on the flow of assets), this provision defines the obligation of the recipient's bank to cooperate (submit certain information, i.e. on the recipient) with the payer's bank. However, in international transactions, where these kinds of frauds are most common, this cooperation in not always possible to ensure, as the banks are operating abroad. Acquiring data on the payment recipient who committed fraud depends solely on the willingness of their (foreign) bank to cooperate with the payer's bank and its correspondent bank. The low percentage of refunded assets in these cases is caused not only by the late reaction of the payer (who realises that they have been tricked only after several weeks, or even months), but also by the passivity of the recipient's bank. Interestingly, SWIFT (Society for Worldwide Interbank Financial Telecommunication), as opposed to SEPA (Single Euro Payments Area), has no standardised messages for fraud, which limits the possibility for the IT systems in banks to automatically block funds or generate warnings. Payers' banks currently send out two standardised messages in these cases, MT192 and MTn92, none of which necessarily points towards fraud. The first is a request for the recall of the previous message transferring the funds, and the second is a request for a return of funds, but with consent of the recipient.

The aforementioned points to the LPS, as a separate law defining the rights of payment service users, determining the loss in case of APP fraud is borne by the payer, as the submitter of the order. Unlike with payment card fraud, where Article 51 of the LPS weighs the payer's level of negligence, the LPS does not note the level of the user's negligence in cases of APP fraud. Even when the payer is a victim of a highly skilful, sophisticated, or complex fraud, which even a user acting with all due attention, as a good businessman, would fall victim to, the LPS is strict – the liability for the loss incurred as a consequence of such a fraud would fall to the payer, who had filled out, issued, and authorised the payment order. While in card transactions (a form of direct debit/pull payment) the lack of monitoring of such transactions by the card issuing bank (Article 59 of the LPS) may be the final argument of the user, opening the possibility of shared liability of the bank and the client, the LPS does not afford the same opportunity in case of push payments (credit transfer). The LPS only guarantees the obligation of the bank to contact the recipient's bank immediately following the report of fraud, mostly via a correspondent bank, and demand a return of funds, hoping that the recipient bank will react in a timely manner.

1 *Payment order authorisation can be done with a handwritten signature on a paper form, a qualified signature on an electronic document or via two-elements authentication. In addition to the LPS, the issue of (two-factor) authentication is also regulated by the Decision on Minimum Information System Management Standards for Financial Institutions ("Official Gazette of the RS", no. 23/2013, 113/2013, 2/2017, 88/2019 and 37/2021), which implemented certain authentication standards established by Directive 2015/2366 and Commission Delegated Reg-ulation 2018/389.*

Even when the recipient bank reacts in time, and with the willingness to refund the assets (usually with the evidence of fraud having been reported to the relevant authorities), it usually does so under the condition of a written guarantee of the payer's bank to settle its obligations to the recipient, if it is obliged to do so (letter of indemnity). With that in mind, the issue is whether the payer's bank would be obliged to send such a statement in the context of its obligation to take all reasonable measures to return the funds. Based on the model statement we have had access to[2] it can be seen that such a statement is an obligation of the payer's bank to refund the previously returned funds, not only in the case of a decision from a court or other competent authority in the recipient's bank's country, but also in the case of the recipient's demand without such a decision. Nonetheless, since the fraud at hand is well known to banks, it is difficult to accept that the recipient's bank, which had opened an account for an individual suspected of fraud, would be ready to demand a return of funds from the payer's bank solely based on the request from that individual, without an assessment of the validity of such a demand, i.e. without the individual initiating a procedure against the bank. Thus, it could be tentatively concluded, which would not hold true in certain cases and due to certain circumstances, that the payer's bank is obligated to submit such a statement to the recipient's bank, within the reasonable measures taken in order to return the funds (Art. 55, par. 3, LPS).

Application of the General Rules of Contract Law

Article 14, paragraph 2 of the LPS stipulates that the provisions of the Law on Contracts and Torts, (Official Gazette of the SFRY, No. 29/78, 39/85, 45/89 - Decision of the Supreme Court of Justice and 57/89, "Official Gazette of the FRY", No. 31/93, Official Gazette of Serbia and Montenegro, No. 1/2003 - Constitutional Charter and Official Gazette of the RS, No. 18/2020, hereinafter: the LCT) shall apply to all issues concerning the payment service contract which are not regulated by LPS.

The LPS governs the issue of liability for the improper execution of a payment transaction due to the wrong account number, but as previously stated, it cannot be assumed with certainty that when formulating such a rule, the legislator took into account APP fraud. In other words, the question could be raised as to whether Article 55 of the LPS is sedes materiae for the issue of liability for improperly executed transactions due to APP fraud, or whether there is actually a legal gap in that section, which should be filled by the application of the LCT.

Furthermore, it is clear that the primary obligation of the bank, as the order recipient, is to execute payment orders as they read in accordance with the agreed deadlines. In other words, its core duty is to transfer money from its client's account to the account indicated by that client in the payment order. In this regard, Article 36 of the LPS expressly states that the bank cannot refuse the execution of a payment order when all of the conditions set forth in the contract on payment services have been met, unless otherwise determined by some regulation. That other regulation could be the LCT and the provisions that establish standards regarding the manner of order execution, that is, when the order recipient can refuse the execution of that order. In this regard, Article 1057, paragraph 1 of the LCT (which in addition to the LPS regulates the contract on current bank accounts) stipulates that the bank is responsible for the execution of the depositor's order, according to the rules of the contract of order. However, among those rules of the contract of order are Article 751, paragraphs 1 and 2 of the LCT. The first stipulates the obligation for the client to execute the order according to the received instructions, with all the attention of a good businessman, staying within its limits and always looking after the interests of the client and being guided by them, while the second specifies that the client has the obligation to draw the orderer's attention and ask for new instructions when they believe that the execution of the order according to the received instructions is to the detriment of the orderer.

2 *"We hereby agree to indemnify you and hold you harmless against any actions, proceedings, claims and demands which may be brought against you and all losses, costs, charges, damages and expense which you may incur or sustain by reason of you having released the sum to us without the authority of your customer."*

These rules could accordingly be applied to the bank, as a "professional order receiver" in such a way that a higher level of attention should stand, from Article 18, paragraph 2 of the LCT – the standard of care of a good expert. In other words, "since the order recipient is an expert in the tasks from the order whose execution is accepted, they are obliged to warn of the error by acting with the standard of care of a good businessman and a good host. At the same time, the standard of care of a good businessman means the standard of care of a good expert" (Trajković, Perović (ed), 1995, 1282).

In this regard, it is reasonable to expect that with the standard of care of a good expert, and given its knowledge and experience in payment transactions, the bank in certain cases can recognise potential BEC fraud and, in accordance with Article 751, paragraph 2, warn its client.

In fact, one should not question the existence of the ever-present obligation of the bank to refuse the execution of the order and warn the user when it suspects fraud, but the key question is when the bank is obliged, i.e. when, as a professional provider of payment services, it can, i.e. should, doubt the correctness of the instructions received, which would activate its obligation from Article 751, paragraph 2 of the LCT.[3] In connection with this issue, it should be noted that Article 110 of the Law on Banks (Official Gazette of RS, No. 107/2005, No. 91/2010 and 14/2015, hereinafter: Law on Banks) recognizes the standard of prudent banking operations. Although this is primarily a standard that is used for prudential supervision, it can be used for banking conduct supervision as well, including the area of payment services. In this regard, it can be considered that caution on the part of the bank would be justified and expected if there is a certain experience or knowledge on the part of the bank that indicates that such caution is necessary when providing certain services, provided that such caution does not disrupt the provision of those services.

In circumstances where there is an increase in various forms of Authorised Push Payment fraud, it can be assumed that banks as providers of payment services have knowledge and certain experience that should lead them to act with an increased degree of caution when executing, above all, international payment transactions. In addition, and as previously shown, the number of payment orders in international payment traffic is not so large, while at the same time the individual value of those orders is significant and there is a low degree of refund in case of fraud. All this leads to the conclusion that the increased vigilance of the bank (which leads to additional administration) would not be disproportionate to the potential damage that can be avoided and would not jeopardise the provision of this type of payment services.

Related to abovementioned and as an example, "under the UCC, a bank is not liable for losses if it followed 'commercially reasonable' security procedures to verify the transactions" (Tang, 2015). To decide what is commercially reasonable, the US Commercial Code directs courts to consider "the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank... and security procedures in general use by customers and receiving banks similarly situated" (Tang, 2015).

If we look at the cases of Business Email Compromise fraud in connection with which a complaint procedure was conducted before the National Bank of Serbia, it can be concluded that the first indicator of this fraud is the information that the fund recipient's headquarters (factory, branch office, etc.) and the headquarters or branch of the bank where the account from the payment order is located is not in the same country.

3 *Comparatively speaking, the counterpart of this standard from the LCT in the United Kingdom is the duty of care rule, i.e. in the case of banks, Quincecare duty. More on that later.*

Out of a total of 24 complaints related to BEC frauds that the National Bank of Serbia resolved, in 18 cases the country of the headquarters of the payee and the fraudulent recipient's bank differed. Another equally important indicator is a change of the account and bank to which a payment is made, in relation to the account (bank) to which the client had previously transferred funds to the same recipient. If these two indicators are combined, there is a very high degree of probability that it is a fraud. In addition to the above, an unusually high amount and/or frequency of transactions, as well as an unusual country of the payee's bank can be additional indicators. Moreover, since the bank has knowledge of every fraud committed against its clients, the presence of a bank to which BEC payments had previously been made would always have to be additionally checked. At the same time, Article 75, paragraph 2 of the LPS gives banks the possibility to exchange this data, so that they can have a specific grey list of banks to which such payments were made.

Therefore, the application of prudent banking standards when executing (international) payment orders in the current circumstances would mean, among other things, that the bank should collect and consolidate historical data and, thus, define indicators of fraud, and use those indicators when controlling the payment order. Should such indicators appear, the bank has the duty to recognize that the instructions may be harmful to the payer, which activates its obligation from Article 751, paragraph 2 of the LCT to warn the orderer. It is important to note here that banks have different degrees of automation in the execution of payment orders, different number, and structure of clients (residents/businesses) and payment orders, different ratio of domestic and international payment transactions, and generally different volume and structure of payment transactions. All this should be considered when assessing the fulfilment of the standard of prudent banking operations, and that standard should be assessed in relation to a specific bank.[4]

In any case, in circumstances where the number and value of BEC transactions, and other forms of APP fraud, are increasing, and when the bank is aware of this, it can hardly hide behind the exclusive application of Article 55, paragraph 2 of the LPS. In fact, that provision itself states that the bank is not obliged to check the correctness of the account number in the payment order, which does not mean that it is not obliged to warn the user if it has certain doubts regarding that account, or some other element of the payment order.

Based on the mentioned considerations, it could be concluded that, in a situation where the bank is aware of the existence of these types of fraud, as well as indicators that can signal fraud, it is not possible to assess the bank's liability solely from the aspects of LPS, but it is necessary to apply the standard of due diligence of a "professional order receiver", which, in the sense of the LCT, is the standard of care of a good expert. This does not mean (except in some exceptional cases) that the failure of the payer's bank to spot the fraud and warn the user can lead to the conclusion that it is liable for the entire amount of the loss caused by the fraud, but it would have to be assumed that the payer's bank contributed to that occurrence, due to its failure, i.e. increasing the damage incurred. In other words, it is clear who caused the damage, but all other participants in the payment transaction: the payer, the payee, and their banks, may have a certain (sometimes key) contribution to the incurrence of the damage. Therefore, in a specific case in which a failure of the payer's bank with regard to its obligation from Article 751, paragraph 2 of the LCT was established, the rule of shared responsibility from Article 192 of that law could be applied (with necessary adjustments).

4 *More on this in the US case, see Tang, 2015.*

Practice of the NBS

According to our knowledge, there is currently no domestic court practice related to APP fraud, but there is a practice of the National Bank of Serbia in complaints procedures commenced mainly by legal entities. In the period from 2021 until the end of 2023, the National Bank of Serbia resolved 24 complaints from users (mainly businesses) regarding improper execution of payment transactions due to BEC fraud. In those procedures, the National Bank of Serbia is authorised to determine whether the bank acted in accordance with the regulations governing payment services. In this regard, in its findings, the National Bank of Serbia first assessed the bank's actions from the aspects of the previously mentioned provisions of the LPS, finding that, in terms of those provisions, there is no liability of the bank for an incorrectly executed payment transaction. Nevertheless, the National Bank of Serbia also gave an opinion on the bank's actions from the aspects of Article 751 of the LCT. In this regard, the cases considered can be divided into several categories.

The first category consists of those cases where the bank has a subsidiary obligation from Article 751 par. 1 and 2 of the LCT entirely fulfilled, because after receiving a payment order with questionable instructions (in the sense of suspected fraud), the bank warned the user and demanded from them to check those instructions, but despite the warning, the users confirmed the initial instructions. In those cases, the National Bank of Serbia made it clear that the question of the bank's liability for contributing to the occurrence of damage cannot be raised, even from the aspects of the aforementioned provisions of the LCT. The second category consists of cases where the bank did not react to certain indicators, as they were individual and not combined indicators (for example, the payer is transferring the funds to a specific payee for the first time, and there is no indicator of a change in the account number). In that situation, the National Bank of Serbia expressed the opinion that, even if the question of the bank's shared liability for contributing to the damage could be raised, that contribution would be small. The third category includes cases where BEC fraud indicators were combined, and the bank did not react and warn the payer. In such cases, the National Bank of Serbia expressed the view that the application of the rule of shared liability for damage comes into consideration, with a potentially more significant degree of the bank's liability for contributing to the incurrence of the damage. In all cases where the NBS expressed a position regarding the application of that rule, that position was expressed in the form of an opinion (within the notice of findings) because, according to the current regulations, the NBS does not have the authority to determine damages.

Practice in the United Kingdom

Even comparatively speaking there is no rich case law related to Authorised Push Payment fraud. However, in July 2023, a very interesting case was concluded before the United Kingdom Supreme Court, where the victims (a retired couple who lost £700,000 in savings) of a highly sophisticated APP fraud sued the bank. The judgment in this case is a precedent that will have extremely significant consequences for the judicial practice in the United Kingdom, and perhaps more widely, and for that reason it is given a lot of space in this paper (Judgment, Philipp v Barclays Bank UK PLC, [2023], 25, 12/07/2023, hereinafter: SC Judgment). In addition, the United Kingdom also has the practice of the Financial Ombudsman Service, which in several cases of APP fraud made decisions in favour of injured payers.

Another interesting ruling from 2023 comes from the United States, where the Federal Court in Virginia found the peyee's bank is liable for damages suffered by the payer as a victim of BEC fraud (Studco Building Systems US, LLC v. 1st Advantage Federal Credit Union). Since concerns the liability of the payee's bank, not the payer's bank, we will not consider this case further, but it is listed for informational purposes only.

Liability of the Payer's Bank in the Case of Mrs Philipp v. Barclays

After Mr Philipp was contacted by an unknown person who introduced himself as a high-rank-ing official in the Financial Conduct Authority, and after that person, using social engineering, succeeded in gaining his trust and convincing him and his wife (Mrs Philipp) that their funds are not safe in their bank and investment fund, Mr Philipp first transfers the savings of GBP 950,000 to his wife's account in another bank (Barclays), and from there, she transfers GBP 700,000 to accounts in the United Arab Emirates in two transactions. A third transaction of GBP 250,000 was not carried out, because Barclays blocked the accounts based on information from the police that its clients were victims of fraud.[5] The name of this type of fraud is vishing, and this specific form is called safe account fraud.

The Stance of the Court of Appeal

After the first-instance court granted summary judgment refusing to find any liability on the part of the bank, the appellate court allowed the plaintiffs' appeal, finding that the bank could be held liable for its failure to exercise Quincecare duty. This rule of law of contractual liability of the bank to the customer was described, but not applied, in the case of Barclays Bank plc v Quincecare Ltd. Even prior to this case, the bank's duty of care towards the client had been recognised. Thus, in a judgment from the early seventies, the UK court held "that the bank was in breach of a duty of care owed to its customer to make inquiries before paying the cheque in circumstances where there were reasonable grounds for believing that the authorised signatories were 'misusing their authority for the purpose of defrauding their principal or otherwise defeating his true intentions'" (Karak Rubber Co Ltd v Burden, No 2 [1972] 1 WLR 602, according to SC Judgment, para 41). The Quincecare duty rule was applied in the Singularis case (Judgment, Singularis Holdings Ltd v Daiwa Capital Markets Europe Ltd, UKSC 50, 30/10/2019), where it was judged that the broker, i.e. the investment bank, violated the duty of care towards the client (company), when, without further investigation of the relevant circumstances, the bank carried out a transaction at the behest of a representative, (who is also the sole owner), even though any reasonable banker would realize that there are obvious signs that the owner of the company is abusing the company by instructing funds to be transferred to other segments of their business operations (See SC Judgment, para. 50).

It clearly follows from the above that the previous judicial practice described and applied the rule of duty of care of the bank exclusively in cases where the representative of the legal entity tried to misuse the company's funds. In this regard, the Court of Appeal tried to reinterpret the Quincecare duty in such a way as to extend it to the cases when a natural person issues an order to their bank, as a result of fraud. Analysing the aforementioned (and other) cases where the application of the duty of care was considered, the Court of Appeal notes that the crucial question is not whether such a duty exists, but when it is activated, i.e., what (lower) level of knowledge activates such an obligation for the bank. Referring to the Singularis case, this Court concludes that these are situations where there are conditions where an ordinarily prudent banker would examine those circumstances (see: The Court of Appeal, Approved Judgment [2022], EWCA Civ 116, 14/03/2022, para. 28; hereinafter: CA Judgment).

[5] *For a detailed account of the facts, that is, for the manner in which the fraud was committed see The High Court of Justice, Business & Property Courts in Bristol, Approved Judgment, [2021] EWHC 10 (Comm), Judge Russen QC, Fiona Lorraine Philipp and Barclays Bank UK PLC, 18/01/2021, para 27 – 71.*

The court recognizes that the obligations, the execution of the payment order as it reads (and within the short, agreed to period – aut. comm.) and the application of reasonable skill and care (in the sense of preventing damage to the payer – aut. comm.) are performed in tension, and how, in a given case, resolving those tensions depends on the specific circumstances (see: CA Judgment, para. 34).

To the bank's argument that such a way of applying the Quincecare duty would prevent the normal execution of payment orders, the court replies that it is wrong to understand that rule in the context of APP fraud as the bank's obligation to examine each order from the aspects of such fraud, but rather the bank's obligation not to execute the order without additional checks only when there are circumstances that would lead an ordinary prudent banker to perform additional checks. Therefore, the court points out that the crucial information is what those circumstances are, that would lead an ordinary prudent banker to carry out additional checks in connection with the payment order, and in this connection the court states that it is necessary to determine all the facts in a specific case, i.e., it is not possible to pass a judgment in abbreviated procedure, as it was done by the first-instance court. In connection with those circumstances in this specific case, the Court of Appeal cites several: Ms Philipp's account history; that Ms Filip came in person to a bank branch that is not her usual branch; that she demanded the transfer of a huge sum of money, unprecedented in her case; that she had received that money in her account just a few days before; and that the transfer was made to the account of Lambi Petroleum in the UAE (see: CA Judgment, para. 71). It should also be pointed out that the court, with regard to the objective assessment of the circumstances that would lead to the examination of the client's order, as well as in relation to the administrative limitations of such examinations, recognises the importance of certain banking standards and good practice, primarily to assess what is feasible in this regard (see: CA Judgment, para 55).

A Critical Overview of the Supreme Court's Judgement

With this judgement, the Supreme Court not only refused to expand the previous understanding of the Quincecare duty, but also contested its existence, finding that it was actually a general rule on the duty of care of the bank as an order recipient, which it narrowed in the process. The court devoted several paragraphs of the judgment to the explanation of its understanding of the duty of care, and significantly less space to the explanation as to why such a duty did not exist in the specific case.

The Supreme Court did not accept the position of the Appellate Court that the logic behind the reasoning of the judgments in which the rule of Quincecare duty was considered is not based on the fact that the order to the bank was issued by the representative of the bank's client, and not the client themselves, and that it is therefore possible to extend that rule to the case when the order is issued by the client themselves, a natural person. On the contrary, the Supreme Court states that "as just noted, in Singularis Baroness Hale regarded this common factor as a defining characteristic of the 'Quincecare duty'" (SC Judgment, para 53.).

In the opinion of the Supreme Court, the first flaw in the understanding of the Court of Appeal (which it follows from the judgment in the Quincecare case), is that it assumes a tension between the bank's duty of care and its obligation to execute the client's payment order, i.e., it tries to reach a reasonable conclusion (which had already been reached in the case of Selengor and Karak), starting from a wrong assumption (see: SC Judgment, para 62). The Supreme Court expresses the view that the primary obligation of the bank as the payer (to which all others are subordinate) is to execute the user's order as it reads, and the duty to apply reasonable skill and care is activated only if the validity or content of the order is unclear or leaves a certain choice to the bank in regarding the manner of execution, and that from such a duty it is not possible to create a duty not to execute the order (see: SC Judgment, paragraphs 63 - 64). The Supreme Court tries to support this claim by referring to the rule of duty of care (applicable to any contract for the supply of goods or the provision of services), which is prescribed in the laws (Statutory Law), as an obligation to provide services with reasonable skill and care.

Referring to some judgments (not related to the Quincecare cases), the Supreme Court reduced the bank's duty of care to the fact that such diligence must be applied if the payment instruction leaves the bank free to choose the method of transfer, or in a situation where the instruction does not clearly inform what the bank should actually do (stating that, in such a situation, the duty of care means that the bank requires clarification of the instruction from the payer; See: SC Judgment, para. 34 - 37).

It could be said that the Supreme Court here completely sets aside the Selengor and Karak judgments (although it had previously claimed that reasonable conclusions had been reached in those judgments) because in these cases duty of care was not only understood as an obligation to demand clarification of incomplete instructions, but as an obligation for the bank to refrain from executing the order until it performs an additional investigation, if a reasonable and prudent banker would have reason to believe that the agent is trying to defraud his principal, the bank's client. The Supreme Court tries to "cover up" this stance by introducing, instead of the misuse of authority of the company's representative, the understanding that, in those cases, the authority to issue such orders does not actually exist (absence of authority), so the validity of those orders is disputed (see: SC Judgment, para. 69 - 89). The Court thus concludes that when the principles related to the right of representation are applied to the series of Quincecare cases (Selangor, Karak Rubber, Lipkin Gorman, Singularis), the rationale for the legal conclusions presented in those cases becomes clear. In a situation where the representative tries to pursue their own interest to defraud the company of which they represent, they do not have the actual authority to issue a payment order on behalf of the company (the representative generally has the presumed authority, as the company's representative to the bank, to issue payment orders, but not if the circumstances suggest a level of dishonesty which is obvious to the bank, and which would lead a reasonable banker to check the authority of the representative before executing the instruction; see SC Judgment, para. 90).

In other words, the Supreme Court considers that, even in cases on the Quincecare line, the bank does not have any special duty to refrain from executing the payment order, but, in those cases, the order has not really been authorised by the client, i.e. it has not even been issued, and the bank is obliged to recognize this in certain circumstances.

The Supreme Court concludes that "Quincecare duty is not, as that epithet might suggest, some special or idiosyncratic rule of law. Properly understood, it is simply an application of the general duty of care owed by a bank to interpret, ascertain and act in accordance with its customer's instructions. Where a bank is "put on inquiry" in the sense of having reasonable grounds for believing that a payment instruction given by an agent purportedly on behalf of the customer is an attempt to defraud the customer, this duty requires the bank to refrain from executing the instruction without first making inquiries to verify that the instruction has actually been authorised by the customer" (SC Judgment, para 97.).

However, the duty of care, defined in this way, is difficult to apply, e.g. in the case of Singularis, where the court found a violation of the duty of care on the part of the bank, and where the payment order which primarily harmed the company's creditors (and not the company itself, other owners, investors, etc.) was issued by a representative who was, simultaneously, the sole shareholder, director, etc. In other words, the Supreme Court obviously creates a sort of fiction in order to avoid conflict between the bank's two duties, namely that, when it recognizes potential abuse in the representative's order, the bank actually recognises that it does not have the authority to execute such an order, so it does not refrain from executing the order, but assumes that the order has not even been issued.

Based on the aforementioned, the Supreme Court concludes that such principles cannot be applied to a case where the client is a victim of fraud, because, in that situation, there is no doubt about the validity of the authorisation, since the client themselves give clear instructions to the bank, and there is no need to examine the order from the aspect of their authority to issue the instructions as such (see: SC Judgment, para. 100).

Although Ms Philipp's representative points out that, even in the case of APP fraud, as well as in cases where representatives try to defraud their orderers, the payment order does not reflect the true intention of the client, the Supreme Court rejects such an argument with the explanation that the fact that the intentions or wishes stemmed from incorrect beliefs does not make them less realistic or truly existing (see: SC Judgment, para. 101-102). In this regard, the Supreme Court sets aside the fact that in paragraphs 40 and 41 it cited the judgments of Selengor and Karak in the part where it is stated that the authorised signatories were "misusing their authority for the purpose of defrauding their principal or otherwise defeating his true intentions".

The Supreme Court further states that in the UK law, fraud does not cause the nullity of a contract or other legal transaction, but the person affected by the fraud can request such a transaction to be annulled, with that annulment affecting only the relationship with the person who committed the fraud, but not in relation to third parties, in this case the bank. In other words, the Supreme Court concludes that the fact that the client's order was caused by fraud authorises that client to request a refund from the person who committed the fraud, but does not call into question the validity of the payment order, nor does it provide a basis for a claim against the bank (see: SC Judgment, para. 103-105).

However, it should be noted that the Supreme Court accepts that the duty of care, in the sense of additional examination of instructions, exists when dealing with a person with a lack of mental capacity (see: SC Judgment, para. 99). In this regard, it is surprising that no parallel was drawn in that part with an individual who is a victim of fraud, especially in the case of the Philipp couple, who, as pensioners, had been so influenced by frauds, i.e. had been deluded in such a way that they were rejecting the warnings of their friends and the police, and the last transaction was prevented precisely thanks to their efforts, even though Mrs. Philipp insisted that the payment transaction be carried out. In other words, such a level of delusion certainly led to a lack of mental capacity when making decisions, i.e. issuing a payment order.

The Supreme Court did, however, consider limitations on the execution of a valid warrant issued by a genuinely authorised person. As examples, the Supreme Court cites cases where a transporter, who undertook the obligation to transport and unload goods to a factory, and who, upon arriving at that place, found the factory on fire, would have acted unreasonably if they had adhered to the assumed obligation. The Supreme Court finds that the logic here is such that it is reasonable to refrain from an order when it is clear that its execution would harm the orderer, provided that the circumstances indicating such harm had been unknown to the orderer when they issued the order. Applying this to the case of Ms Philipp, the Court finds that such a rule would be valid in a situation where the bank receives information from the police that its client is a potential victim of abuse (which is what happened for the last transaction, whereupon the bank refused to execute the order despite Ms Philipp's insistence). Nonetheless, as the Court concludes, the circumstances indicating fraud were well known to the client when she issued the payment orders, because she confirmed all those circumstances through the payment instructions, and at the same time she was unwavering in her intention to execute the orders, so the bank had no reason to suspects that the client is unfamiliar with those circumstances (see: SC Judgment, paras 107-110).

The Supreme Court actually contradicts itself here, because the circumstances of the fraud were also well known to the client with regard to the last transaction that the bank refused to perform, and the bank refused it not because the circumstances indicating the fraud were not known to the client, but because the bank received information from the police that it is definitely a fraud. Therefore, the logic referred to by the Court cannot be applied here, but the difference exists in the degree of knowledge on the part of the bank as the order recipient.

In the end, the Supreme Court found the conflict of two contradictory duties of the bank unacceptable for a different reason, that is not directly related to this case, nor indeed only to Authorised Push Payment frauds. Namely, the Court considers that the judge in the Quincecare case, having noticed a conflict (between two duties of the bank, which in reality does not exist), could not resolve that conflict in a principled way, but had to rely on political considerations (see: SC Judgment, para. 65-66). The problem with this approach is that it is not an appropriate method for identifying what duty is owed by a party pursuant to a contract. What rule would represent a "sensible compromise" or "fair balance" between broad policy goals is a matter for legislators and other policy-makers to consider. In deciding whether a party to a contract can be regarded as having undertaken an obligation to the other party without having done so expressly, the aim of the courts is the more modest one of seeking to give effect to the presumed common intention of the contracting parties (SC Judgment, para 67.).

This attitude deserves a special observation. Namely, in the absence of certain rules to regulate new circumstances, such as APP fraud, i.e., when those specific circumstances were not taken into account when prescribing those rules, the court would have to (especially in the common law system) determine that balance, when there is a reason for it in a general provision of law or case law, as there had been in the Quincecare cases. Here, the famous Lon L. Fuller should be quoted: "The common law is not the work of any one judge, but of many, collaborating through time. In the course of its history the implementation of its rules has been improved and refined. At the same time, the rules themselves have often been revised to make possible an effective implementation of them. Though the common law is said to be built- on precedent, there is no controlling verbal formulation of the meaning of any particular precedent. What the court said in a former case is always subject to reinterpretation as new situations arise. The scope of the precedent is determined not only in the light of the end-in-view pursued by the court that decided it, but in the light of ends then out of view because not stirred into active consciousness by the facts of the case being decided" (Fuller, 1958).

Therefore, the advantage of the common law system compared to the continental one, lies in the fact that the courts create law and, through the reinterpretation of precedents, they can adapt the law to new situations and concrete cases much faster, without having to (as is the case in the continental system) wait for the legislator who, as a rule, lags behind in practice (and reality), and even when they react, it often takes time for the courts to articulate what the legislator had actually "said" or "meant to say". That advantage was not used here.

Contingent Reimbursement Model Code for Authorised Push Payment Scams

The opinion of the Supreme Court that we should wait for the legislator was certainly influenced by the fact that the banks themselves took an initiative to independently and voluntarily regulate this area (through self-regulation)[6] under the auspices of the Lending Standards Board (a UK organization undertaking activities regarding the self-regulation of banks and other creditors). Thus, a part of the banks (including Barclays) voluntarily accepted the application of the Contingent Reimbursement Model Code for Authorized Push Payment Scams, which entered into force in May 2019, and which determines in which cases the payer's and payee's banks are obliged to compensate the payer for the loss (https://www.lendingstandardsboard.org.uk/wp-content/). The Code applies only to domestic transactions. In addition, two key standards, rules of law in that code, should be pointed out, the method of application of which depends on the allocation of loss (user's or bank'/banks').

The first standard is gross negligence, where the payment service provider is not obliged to compensate the user for the loss if they prove the existence of such negligence. The Code lists several explicit examples of such negligence, such as: 1) ignoring effective warnings given by the payment service provider; 2) failure to take appropriate action by the user after a clear negative result of the payee's confirmation; 3) issuing a transfer order without a reasonable basis for the user to believe that the recipient is the person to whom they wanted to transfer funds, or that the transfer is being made in return for real goods and services, etc. - while taking into account the characteristics of the user, and the complexity and sophistication of the fraud scheme. In addition to these exempli causa cases of gross negligence, the Code also includes the general concept of gross negligence. It would appear even in the UK this standard proves necessary, so it is to be expected that the legislator will use this, or a similar standard, when prescribing the rules for the allocation of losses, which will bring the ball back from the parliament's court to the court's.

Another standard, the application of which depends on the allocation of loss (the payer's bank, if it had not met all the required standards, or the bank's fund, if the bank had applied all the standards) is the "no-blame scenario", which again, in the event of a dispute, would require a court assessment on whether or not the bank, in that specific case, had met all the standards expected of it.[7]

Therefore, even with legislative intervention, the courts will have to engage in certain "political" considerations, i.e., give a certain meaning to legal standards in each specific case.

The Financial Ombudsman Service's Practice

The Financial Ombudsman Service (FOS) was established in the United Kingdom by the Parliament to resolve user complaints about the conduct of financial service providers in a fair and impartial manner. When it comes to Authorised Push Payment fraud, the Financial Ombudsman has made distinct decisions in detail, taking into account all the circumstances of a specific case.

Thus, in the case of a user who was a victim of APP fraud, which was carried out over the phone, and where she was instructed by the fraud to make a payment to a secure account, because her funds were at risk, the Ombudsman concluded that, in this particular case, the bank (which is a signatory to the Code) did not prove that, in terms of the Code, the beneficiary acted with extreme negligence, and ordered the bank to refund the total amount of the disputed transactions (see: FOS, DRN-3130787, 28 January 2022).

6 *For more on the definition of self-regulation see: Jovanić, 2019.*

7 *For more on the Code and the recent effects of its application see: Maher, 2021, 140-145.*

Similarly, in the case of an entrepreneur who was a victim of BEC fraud, the Ombudsman decided that his bank should reimburse him the entire amount of the disputed international transaction of GBP 24,235.97 (although the beneficiary demanded that the bank reimburse him 50%). In their decision, the Ombudsman pointed out that the bank had received several opinions from that institution, clearly stating that the bank has an obligation to identify and react in case of suspicious (in terms of fraud risk) transactions, and that, in this particular case, the user had suddenly changed the account to which they had been paying a long-term business partner, as well as that the transaction amount was unusually high for the user. The Ombudsman also analysed the level of attention the defrauded entrepreneur had used and concluded that there was no negligence on their part, because they had actually suspected and demanded that the business partner with whom they believed they were communicating explain the reason for changing the account, but the fraud who had hacked into the recipient's email was extremely convincing, using the accounts of multiple employees of the recipient of the funds who confirmed the reasons for the change in payment instructions. This decision was made independently of the Code, which, as stated, does not apply to international payment transactions (see: FOS, DRN-3087679, 6 May 2022).

After these decisions from 2022, one more decision from November 2023 (after the Supreme Court's judgement) is worth mentioning, where the user lost GBP 50,000 in a "safe account" fraud, which also involved international transactions (see: FOS, DRN-4453209). The Ombudsman did not find the bank liable now, as in the first case we mentioned. In fact, they concluded that the user's bank fulfilled the obligation to recognise and react in case of suspicious transactions, because it warned the user in detail, and those warnings were specific enough to include the very fraud scenario to which the user was exposed. It is true that, unlike the first case, here the bank warned the user during the execution of the second transaction (the first was in the amount of only GBP 76), but it is difficult to evade the impression that the Ombudsman also took into account the judgment of the Supreme Court in the case of Mrs Philipp when making this decision.

Response of the European Commission - Proposal for a Regulation on Payment Services

The description of the legal framework of the payer's bank's liability in case of Authorised Push Payment fraud, and the need to invoke the general provisions of the Civil Code for the purpose of determining this liability are clear evidence that the special framework imported from the payment services directives has legal gaps. Noticeably aware of these gaps, the European Commission in its proposal for new regulations on payment services, this time in the form of a regulation (Proposal for a Regulation of the European Parliament and of the Council on Payment Services in the Internal Market and Amending Regulation (EU) No 1093/ 2010, Brussels, 28.6.2023), partly fills those gaps. In addition to this proposal, there is also a Proposal for a third directive on payment services, but it deals exclusively with status issues related to payment service providers, such as the establishment, supervision, etc. (Proposal for a Directive of the European Parliament and of the Council on Payment Services and Electronic Money Services in the Internal Market [...], Brussels, 28 June 2023).

In Chapter 4 of the proposed regulation, which is dedicated to the authorisation of payment transactions, Article 49 stipulates that the payee's bank, at the request of the payer's bank, verifies whether the account on which the payment order is written belongs to the person named in that order as the recipient of the funds. If there is a discrepancy, the bank informs the payer about it, but if the payer still requests that the transaction be carried out, such a transaction will be considered approved. Payers will be able to turn off the service, but they will then have to be warned that the funds may end up in an account that does not belong to the intended recipient of the order. In any case, the payer cannot bear losses if their payment service provider did not inform them that there was a discrepancy, unless they had chosen not to use that service.

In the case of impersonation fraud (spoofing) where the user is a victim of fraud by an unknown person who presented themselves as an employee of their payment service provider, that provider would, in accordance with Article 59 of the draft regulation, be obliged to return the entire amount to the user, on fraud of an authorised transaction, if the user immediately reported the fraud to the police, and on the condition that the payment service provider cannot prove that the user acted with extreme negligence, or that they were possibly a participant in that fraud. Therefore, in contrast to Directive 2015/2366, which "provides the broad protection accorded to a payment service provider acting on a unique identifier" (Benjamin, 2019), this introduces a presumption of his responsibility, which can be refuted by proving that the payer acted with gross negligence.

Thus, the standard of gross negligence is applied again, as was the case with the first and second payment services directives, with the fact that, in the case of those regulations, it was used only in the case of misuse of payment instruments. When it comes to the liability of the payment service provider in case of this type of abuse, the Proposal for the Regulation is mostly within the framework of the existing solutions from the Directives, with two differences. The first is that the competent authorities (who supervise the implementation of the regulation) can reduce the liability of the payer, due to their not fulfilling their obligations regarding the use of the payment instrument and its protection, if they did not act fraudulently, i.e. if they have not intentionally disclosed certain data regarding the payment instrument, taking into account, in particular, the nature of the security elements and the specific circumstances under which the payment instrument was lost, stolen or misused. Another difference is that, if the so-called strong customer authentication is not applied, the payer is not held liable, unless they had acted fraudulently.

In addition to the aforementioned Chapter, which introduces stricter rules (assumptions of responsibility) for payment service providers in terms of abuse and fraud, Chapter 8 of the Draft Regulation gives a number of significant jurisdictions to the authorities of member states that are responsible for supervising the application of those rules. These jurisdictions mainly include the supervision of payment service providers in a way that is already carried out in Serbia, by the National Bank of Serbia (on - site and off - site supervision), which includes the authority to impose certain measures on these service providers in order to eliminate irregularities, as well as to impose administrative fines. Nevertheless, the adoption of this proposal and its implementation into the Serbian legislation would bring additional possibilities in that control, such as the possibility to obtain data from the competent authorities in connection with certain criminal investigations and procedures, as well as to use measures such as periodic penal payments or the publication of imposed measures and sanctions.

Conclusion

Therefore, when the existing regulations, new proposals, as well as (quasi)judicial domestic and comparative practices are analysed, it can be concluded that the payer's bank has no reason to be lulled into the belief that there can be no liability on their side for the loss caused by Authorised Push Payment fraud. Regardless of the fact that the Supreme Court in the UK has narrowed down the current understanding of duty of care on the part of the bank, the increasing number and scope of fraud in payment transactions will sooner or later lead to the application of the principle that the risk is borne by those who can better manage it. This is additionally confirmed, among other things, by the Code, the proposal for a new regulation on payment services by the European Commission, the practice of the Financial Ombudsman in the UK, and the National Bank of Serbia.

Until the adoption of new regulations or certain activities of banks in the direction of self-regulation, courts, regulators and supervisors of the banking sector will have a decisive role in assessing the existence of possible liability of the payer's bank. After all, the new regulations will certainly be based on certain legal standards to cover many different types of fraud (with authorised and unauthorised transactions), which will again mean fairly broad discretionary jurisdictions for courts and supervisors.

In any case, according to existing domestic regulations, the eventual liability of the payer's bank in the event of the execution of an authorised payment order resulting from fraud should generally not lead to its sole liability. Failure to take measures which, in terms of the domestic Law on Banks, could be understood as measures of prudent banking operations, i.e., failure to warn the payer when there are indicators of potential fraud, could, in terms of the Serbian Civil Code, lead to shared responsibility of the bank with the payer for the resulting damage (corresponding, i.e., adjusted by the application of Article 192 of the LCT). In this regard, regarding the fulfilment of the conditions for activating the obligation of the payer's bank from Article 751, paragraph 2 of the LCT, the most important thing is to determine how the bank acted in a specific case, in terms of the existence of appropriate internal procedures for the recognition and prevention of fraud and the manner of their application. In other words, it is important to determine whether the bank, by establishing adequate policies, procedures, and software tools, enabled a common, reasonable banker to recognise circumstances that require checking the payment order. Therefore, in order to assess whether, in a specific case a reasonable banker could, or had to, suspect the correctness of the instruction, the court would first have to assess the fulfilment of the standard of prudent banking operations in the execution of the payment transactions in question. In order to appreciate this, the court should obtain an opinion from an expert in the field of payment services (not from experts in the general economic profession) or institutions responsible for supervision of banks, on the bank's actions in a specific case. For the reason that "in order for banks to achieve a balance between protecting consumers against online banking fraud and the costs of additional safeguards, courts should follow uniform and objective "best practices" determined by agency experts when adjudicating liability" (Tang, 2015).Otherwise, by imposing security requirements in the provision of payment services that are beyond what is economically speaking reasonable and justified, negative effects could be produced for the majority of users of those services, as the disproportionate costs of security mechanisms would spill over into the price and/or quality of services.[8] In addition, overly rigorous requirements for the bank could lead to moral hazard on the part of the payer.

[8] *For more on this see: Burrow, 2013, 394-398.*

References

1. Burrow K. R., Increased Bank Liability for Online Fraud: The Effect of Patco Construction Co. v. People's United Bank, North Carolina Banking Institute, 2013.
2. Benjamin, G., Payment Transactions under the E.U. Second Payment Services Directive - An Outsider's View, Texas International Law Journal, vol. 54, no. 2, 2019.
3. Dević D., Kritika Fulerovog shvatanja prirodnog prava, Pravni fakultet Univerziteta u Beogradu, Beograd, 2007.
4. Jovanić T., Uvod u Ekonomsko pravo, Pravni fakultet Univerziteta u Beogradu, Beograd, 2019, 103.
5. Kjørven E. M., Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe, European Business Law Review, Issue 1, 2020.
6. Levitin J. A., Private Disordering? Payment Card Fraud Liability Rules, Brooklyn Journal of Corporate, Financial & Commercial Law, Vol. 5, 2010.
7. Maher R., A Critical Analysis of Recent Efforts in the United Kingdom to Tackle, Authorised Push Payment Scams and the Impact on the Bank-Customer Relationship, Trinity College Law Review, Vol. 24, 2021.
8. Trajković M., Komentar uz član 751. ZOO, Perović S. (red.) (1995) Komentar Zakona o obligacionim odnosima, knjiga II, Beograd 1995.
9. Tang L. S., Increasing the Role of Agency Deference in Curbing Online Banking Fraud, North Dakota Law Review, Vol 91, 2015.
10. Presuda Vrhovnog suda Ujedinjenog Kraljevstva (The Supreme Court, Judgment, Philipp v Barclays Bank UK PLC, [2023], 25, 12/07/2023).
11. Presuda Apelacionog suda u Ujedinjenom Kraljevstvu, (The Court of Appeal, Approved Judgment [2022], EWCA Civ 116, 14/03/2022)
12. Presuda Visokog suda u Bristolu, Ujedinjeno Kraljevstvo, (The High Court of Justice, Business & Property Courts in Bristol, Approved Judgment, [2021] EWHC 10 (Comm), Judge Russen QC, Fiona Lorraine Philipp and Barclays Bank UK PLC, 18/01/2021)
13. Presuda Vrhovnog suda Ujedinjenog Kraljevstva (Judgment, Singularis Holdings Ltd v Daiwa Capital Markets Europe Ltd, UKSC 50,30/10/2019)
14. Presuda Federalnog suda Sjedinjenih Država, za istočni distrikt Virdžinije, (The United States District Court for the Eastern District of Virginia, Case 2:20-cv-00417, Studco Building Systems US, LLC v. 1st Advantage Federal Credit Union, Memorandum Opinion and Order, 12.1.2023.)
15. Odluke Finansijskog ombudsmana u Ujedinjenom Kraljevstvu, (The Financial Ombudsman Service Decisions: DRN-3130787, 28 January 2022; DRN-3087679, 6 May 2022; DRN-4453209, November 2023.)