Mirjana Z. Radović*

Pregledni naučni članak
UDK: 343.53: 004.738.2
doi: https://doi.org/10.56461/SPZ_25305KJ
Primljeno: 25. 4. 2025.
Prihvaćeno: 6. 9. 2025.

RASPODELA GUBITKA ZBOG PREVARE KOMPROMITOVANJEM POSLOVNOG MEJLA U ODNOSU IZMEĐU POVERIOCA I DUŽNIKA NOVČANE OBAVEZE**

Sažetak

U ovom radu autor istražuje privatnopravne posledice prevare usled kompromitovanja poslovnog mejla u odnosu između poverioca i dužnika novčane obaveze. Reč je o situaciji u kojoj privredni subjekt (dužnik novčane obaveze iz osnovnog posla) dobija mejl koji naizgled potiče od poverioca, a zapravo je poslat od trećeg lica – prevaranta, u kome se od njega traži da hitno izvrši plaćanje u skladu sa novim instrukcijama – na određeni račun, po pravilu u inostranoj banci. Prvi deo rada je uvodnog karaktera i sadrži objašnjenja karakteristika, uzroka i vrsta navedenih prevara. Potom je pružena pravno-dogmatska analiza raspodele gubitka između dužnika kao žrtve prevare i poverioca novčane obaveze. U tom pogledu, autor analizira mogućnost pripisivanja izjave volje sadržane u prevarnom mejlu poveriocu, ispunjenje primarnog ugovornog zahteva plaćanjem u skladu sa instrukcijama iz prevarnog mejla i pravo dužnika na naknadu štete od poverioca zbog izazivanja pravnog privida da je sporni mejl autentičan. Na kraju su izložena shvatanja ove problematike u domaćoj sudskoj praksi. Na osnovu teorijske i praktične analize navedenih pitanja autor zaključuje da će gubitak zbog prevare usled kompromitovanja poslovnog mejla po pravilu snositi dužnik.

Ključne reči: komunikacija elektronskom poštom, kompromitovanje poslovnog mejla, zloupotreba identiteta, pravni privid, phishing, prevara.

* Doktor pravnih nauka, redovni profesor Pravnog fakulteta Univerziteta u Beogradu, Srbija.
E-mail: *mirjanam@ius.bg.ac.rs*
ORCID: *https://orcid.org/0000-0003-1700-6495*

** Istraživanje u okviru rada podstaknuto je brojnim otvorenim pitanjima u okviru diskusije na okruglom stolu „Pažnja dobrog privrednika u digitalno doba (*phishing emails*)“ održanom na II godišnjoj konferenciji Udruženja za stečajno pravo, 19. juna 2024. godine u Beogradu (moderator: doc. dr Milena Đorđević, panelisti: prof. dr Miloš Živković, Senka Mihaj, Boško Kaćanski i Nevena Krivokapić Martinović) i izlaganjem Senke Mihaj na temu „Internet prevare u poslovanju“, na Kopaoničkoj školi prirodnog prava – Slobodan Perović, 15. decembra 2024. godine.

ALLOCATION OF LOSS CAUSED BY BUSINESS EMAIL COMPROMISE SCAM IN THE RELATIONSHIP BETWEEN CREDITOR AND DEBTOR OF A MONETARY OBLIGATION

Summary

In this paper, the author examines the private law consequences of business email compromise scam (fraud) in the relationship between a creditor and a debtor of a monetary obligation. The situation involves a business entity (the debtor of the monetary obligation from the underlying transaction) receiving an email that appears to originate from the creditor but is actually sent by a third party – a fraudster – requesting urgent payment according to new instructions, typically to a foreign bank account. The first part of the paper serves as an introduction and provides explanations of the characteristics, causes, and types of such fraud. It then offers a legal-dogmatic analysis of the allocation of loss between the debtor, as the fraud victim, and the creditor of the monetary obligation. The author examines: attributing the will in a fraudulent email to the creditor, fulfilling the contract by paying as instructed in the fraudulent email, and the debtor's right to seek damages from the creditor for making the email appear authentic. The final part of the paper includes an overview of domestic court practices on this issue. Based on theoretical and practical analyses, the author concludes that the loss from fraud due to the compromise of a business email will, as a rule, be borne by the debtor.

Keywords: business email compromise, email account compromise, identity theft, legal appearance, phishing, fraud, scam.

1. Uvod

Poslovne odnose između privrednih subjekata karakteriše značajno oslanjanje na komunikaciju putem mejla, odnosno elektronske pošte. Međutim, iskustvo pokazuje da je takav vid komunikacije daleko od sigurnog i pouzdanog. Iako u najvećem broju slučajeva mejl koji privredni subjekt dobije zaista potiče od lica koje je u njemu naznačeno kao pošiljalac, prevare u ovoj oblasti sve su češća pojava. Otuda se neretko dešava da mejl koji privredni subjekt primi samo na prvi pogled deluje kao da potiče od naznačenog pošiljaoca, dok ga je u stvari poslalo treće,

neovlašćeno lice (prevarant). U slučaju da primalac mejla ne prepozna da je reč o prevari i, na primer, izvrši plaćanje u skladu sa instrukcijama prevaranta, misleći da time ispunjava svoju novčanu obavezu prema poveriocu iz osnovnog posla u čije ime je neovlašćeno poslat mejl, za njega može da nastane veliki gubitak koji bi želeo da prevali na drugoga.

U praksi, opisane vrste prevare predstavljaju ozbiljan problem. Prema nekim istraživanjima, u periodu od juna 2016. do jula 2019. godine širom sveta prevare usled kompromitovanja poslovnog mejla izazvale su gubitke u vrednosti od najmanje 26 milijardi američkih dolara (Cross & Gillett, 2020, p. 872).[1] Iako je u pitanju delo koje je protivzakonito i kažnjivo, zbog čega bi trebalo da prevarant u krajnjem ishodu naknadi gubitak i štetu žrtvama, problem je u tome što učinioci retko kada budu pronađeni. Iz tog razloga, u realnosti gubitak jedino može da se raspodeli između poznatih učesnika, a to su: platilac (na primer dužnik novčane obaveze u osnovnom poslu), nameravani primalac plaćanja (na primer poverilac iz osnovnog posla), kao i banke platioca i (stvarnog) primaoca plaćanja. Cilj redova koji slede je da pruže privatnopravnu analizu posledica prevare usled kompromitovanja poslovnog mejla u odnosu između dva privredna subjekta – poverioca i dužnika novčane obaveze iz određenog osnovnog posla – kako bi se iz toga izveo zaključak o raspodeli prouzrokovanog gubitka između njih.

2. Postavljanje problema

U slučaju prevare putem kompromitovanja poslovnog mejla (*business email compromise scam/fraud*, skr. *BEC scam/fraud*) privredni subjekt (žrtva prevare) dobija mejl koji naizgled potiče od pouzdanog pošiljaoca (na primer poslovnog partnera iz aktuelnog ugovornog odnosa), a zapravo je poslat od trećeg lica (učinioca prevare, odnosno prevaranta), u kome se od njega traži da hitno izvrši plaćanje određenog iznosa novca na određeni račun, po pravilu u inostranoj banci (upor. Koza, Öztürk & Willer, 2024, p. 131; Walker, 2023, p. 35; Freedman, 2020; Jones, 2024, p. 225). Uveren da je mejl autentičan i da potiče od pošiljaoca u koga ima poverenje, privredni subjekt izvršava plaćanje u skladu sa datim instrukcijama. Međutim, naknadno se ispostavlja da nameravani primalac plaćanja nije dobio novčana sredstva, već da su ona preneta na račun nepoznatog trećeg lica (prevaranta).

[1] U SAD je ova vrsta prevare 2022. godine bila na prvom mestu po veličini finansijskih gubitaka u iznosu od 2,4 milijarde američkih dolara (vid. Walker, 2023, p. 35). Prema Kanadskom centru za borbu protiv prevara (*Canadian Anti-Fraud Centre*), prevara putem kompromitovanja poslovnog mejla je drugi najveći uzrok novčanih gubitaka od preko četrdeset prijavljenih vrsta prevara (vid. Freedman, 2020).

Kompromitovanje poslovnog mejla je vrsta prevare usmerena ka konkretnoj žrtvi, te je u tom smislu „skrojena po meri" datog privrednog subjekta (UK National Cyber Security Centre, 2020).[2] Da bi prevarni mejl ostvario svoju svrhu, potrebno je da bude što uverljiviji, a to se postiže uvidom u funkcionisanje i poslovanje, odnosno konkretan poslovni odnos datog privrednog subjekta, kako bi se zahtev sa instrukcijama za plaćanje ispostavio u pravo vreme i naizgled u skladu sa postojećim odnosom (Jones, 2024, p. 226). Načini na koje treće (neovlašćeno) lice može da dođe do potrebnih informacija za uspešnu prevaru putem kompromitovanja poslovnog mejla su mnogobrojni i najčešće uključuju fišing (engl. *phishing*) i/ili malver (engl. *malware*) napade.

Primera radi, putem fišinga treće lice može da prevari zaposlenog u privrednom subjektu da mu otkrije podatke neophodne za pristup poslovnom mejlu ili računarskom sistemu (Schmidt & Pruß, 2019, Rn. 274; Weber, 2024; Deusch & Eggendorfer, 2024, Rn. 154; Borges, 2005, p. 3313; Maihold, 2022, Rn. 49) kako bi proučavanjem poslovne korespondencije saznao detalje aktuelnih poslovnih odnosa, predstojeće obaveze plaćanja prema poslovnim partnerima i dr. (Eckhardt, 2023, Rn. 70; Zahrte, 2023, Rn. 130c; UK National Cyber Security Centre, 2020). Važno je napomenuti da fišing napad, koji prethodi prevari putem kompromitovanja poslovnog mejla, može da se dogodi bilo kod žrtve prevare (platioca ili dužnika novčane obaveze), bilo kod njegovog poslovnog partnera (nameravanog primaoca plaćanja ili poverioca novčane obaveze). Isto važi i za malver napade, kod kojih štetan program (na primer trojanac ili virus) biva potajno instaliran u računarskoj mreži žrtve prevare ili njegovog poslovnog partnera da bi omogućio prikupljanje potrebnih informacija i eventualno manipulisanje relevantnom komunikacijom putem poslovnog mejla. Takođe, moguće je da sadržina komunikacije putem poslovnog mejla bude izmenjena u procesu slanja od legitimnog pošiljaoca primaocu od strane trećeg lica koje se umeće između te dve strane tako što presretne autentičan mejl pošiljaoca na putu ka primaocu, kada je reč o tzv. napadu „čoveka u sredini" (engl. *man-in-the-middle attack*) (Borges, 2005, p. 3314; Jungmann, 2023, Rn. 44).

Prevarni mejl koji sadrži instrukcije za plaćanje na račun trećeg lica – prevaranta može da bude upućen sa različite adrese elektronske pošte u odnosu na adresu pošiljaoca u koga primalac ima poverenje (na primer *matija.ilic@kompanija.rs* umesto *mateja.ilic@kompanija.rs*) ili zaista sa adrese elektronske pošte koju pošiljalac redovno koristi u svom poslovanju. U prvonavedenom slučaju korišćenje različite mejl-adrese u odnosu na adresu pošiljaoca od poverenja može da se prikrije lažnom oznakom pošiljaoca mejla ili upotrebom slova ćiriličkog pisma

[2] Za razliku od standardnog fišinga, koji je usmeren bez razlike ka milionima ljudi, napadi kompromitovanjem poslovnog mejla su usmereni ka određenim pojedincima i često ih je teže otkriti.

u mejl-adresi,[3] uz očekivanje da primalac mejla neće proveriti ili neće primetiti odstupanje od ispravne mejl-adrese pošiljaoca. U drugonavedenom slučaju može da postoji neovlašćeni pristup mejl nalogu pošiljaoca od strane trećeg lica (prevaranta), koji mu omogućava slanje poslovnih mejlova sa legitimne adrese elektronske pošte pošiljaoca, pa se takva vrsta kompromitovanja poslovnog mejla označava kao kompromitovanje mejl naloga (engl. *email account compromise*) (Koza, Öztürk & Willer, 2024, p. 131).[4] U oba navedena slučaja treće lice falsifikuje, odnosno preuzima identitet pošiljaoca, predstavljajući se kao on u nadi da primalac mejla neće posumnjati u autentičnost mejla niti prepoznati da je reč o prevari.

Komunikacija putem elektronske pošte naročito je pogodna za zloupotrebu identiteta pošiljaoca mejla, budući da u redovnim okolnostima nije moguće pouzdano utvrditi od koga potiče konkretna poruka (Maihold, 2022, Rn. 50-51). Otuda, da bi se sa sigurnošću znalo da li je određeni mejl autentičan, neophodno je sprovesti dodatnu proveru izvan razmene mejlova, poput telefonskog ili video-poziva. Upravo u cilju izbegavanja eventualnih dodatnih provera, prevarni mejl po pravilu sadrži zahtev za hitnim postupanjem, uverljivo obrazloženje zbog čega plaćanje treba izvršiti na račun u inostranstvu, iskorišćava period kada je nadređeni (na primer šef ili direktor) zaposlenog koji primi mejl nedostupan, upućuje se na samom kraju radnog dana i slično (Cross & Gillett, 2020, p. 875). Ovi i drugi mehanizmi socijalnog inženjeringa obezbeđuju da se primalac mejla isključivo osloni na komunikaciju elektronskom poštom (Freedman, 2020; Walker, 2023, p. 35), te u tom smislu iskorišćavaju „čoveka kao slabu tačku" u organizaciji privrednog subjekta (Jungmann, 2023, Rn. 46; Cross & Gillett, 2020, pp. 873-874).

U konkretnim pojavnim oblicima prevare putem kompromitovanja poslovnog mejla prevarant može da falsifikuje, odnosno preuzme identitet saugovarača (na primer poslovnog partnera, pružaoca usluga, klijenta) ili direktora kompanije primaoca mejla (Cross & Gillett, 2020, p. 873). S jedne strane, kada prevarni mejl deluje kao da potiče od saugovarača, u njemu se od primaoca mejla traži da izvrši plaćanje na drugi račun u odnosu na onaj koji je izričito ili prećutno ugovoren. Reč je o situaciji u kojoj se dva privredna subjekta nalaze u poslovnom odnosu iz koga proizlazi novčana obaveza primaoca mejla, pri čemu je ugovoreno ili postoji ustaljena praksa da dužnik plaćanje vrši na određeni račun druge strane. Nakon

[3] Kada se u mejl-adresi upotrebe slova ćiriličkog pisma koja se u latiničkom pismu isto pišu, tako da je ljudskom oku neprepoznatljiva razlika (na primer slovo „a" na ćirilici umesto latiničkog slova „a"), mejl adresa sa koje je poslat prevarni mejl primaocu izgleda identično mejl adresi lica u koje ima poverenje, iako je u računarskom smislu reč o dve različite adrese, jer su slova „a", „e" ili „o" napisana različitim pismima.

[4] U domaćoj sudskoj praksi navedena vrsta kompromitovanja poslovnog mejla označava se kao „zloupotreba *e-mail* adrese". Vid. Presuda PAS, 2020.

što dužnik izvrši plaćanje u skladu sa novim instrukcijama, poverilac kao nameravani primalac plaćanja tvrdi da nije dobio novac niti je poslao sporni mejl sa novim brojem računa. Nasuprot tome, dužnik smatra da je ispunio novčanu obavezu u skladu sa instrukcijama iz mejla poverioca,[5] odnosno iz mejla koji je bio ubedljivo nalik na mejl poverioca.

S druge strane, kada je prevarni mejl upućen zaposlenom pod prividom da ga je poslao njegov nadređeni kod poslodavca (na primer direktor), takav vid prevare počiva na „preuzimanju identiteta direktora" (engl. *executive impersonation*), pa se pod tim nazivom izučava kao specifična varijanta kompromitovanja poslovnog mejla (Zweighaft, 2017, p. 1). Ovde direktor navodno zahteva od zaposlenog da hitno izvrši plaćanje na određeni račun u inostranstvu za potrebe izmirenja obaveze prema poslovnom partneru, finansiranja rada ogranka, pomoći zavisnom društvu i sl. (Zweighaft, 2017, pp. 1-2). Ključna specifičnost takvog slučaja preuzimanja tuđeg identiteta ogleda se u tome što nastali gubitak predstavlja interni problem za privrednog subjekta, koji nikako ne može da se prevali na poslovnog partnera ili zavisno društvo, već eventualno jedino na zaposlenog koji je izvršio plaćanje ili direktora čiji je identitet falsifikovan. S obzirom na specifičnost problematike odgovornosti zaposlenog, odnosno direktora u privrednom subjektu, predstojeća analiza neće obuhvatiti ta pitanja, već će se isključivo baviti raspodelom gubitka u slučaju prevare putem kompromitovanja poslovnog mejla falsifikovanjem identiteta saugovarača privrednog subjekta.

Nesporno je da gubitak usled opisane prevare u krajnjem ishodu treba da snosi treće lice (učinilac prevare) koje je na taj način ostvarilo protivpravnu imovinsku korist. Međutim, problem je u tome što žrtvi prevare i njegovom saugovaraču najčešće nije poznat identitet tog lica ili se ono ne može pronaći. Osim toga, do momenta kada platilac shvati da je bio žrtva prevare, novčana sredstva su po pravilu već podignuta ili preneta sa računa primaoca – prevaranta, te ne mogu da budu jednostavno „vraćena" platiocu. Iz tih razloga, gubitak usled prevare putem kompromitovanja poslovnog mejla u praksi po pravilu jedino može da se raspodeli između poznatih učesnika, i to: dužnika novčane obaveze (platioca), poverioca novčane obaveze (nameravanog primaoca plaćanja), banke platioca ili banke primaoca plaćanja. Predstojeća analiza privatnopravnih odnosa između navedenih lica ograničena je na pravni odnos između poverioca i dužnika novčane obaveze, dok će pravni odnosi između učesnika u izvršenju bankarske platne transakcije podstaknute prevarnim mejlom biti predmet posebnog rada.

[5] Reč je o kompromitovanju mejl naloga, kada je poruka poslata sa adrese elektronske pošte poverioca.

3. Pravno-dogmatska analiza raspodele gubitka između poverioca i dužnika novčane obaveze

Poverilac i dužnik novčane obaveze nalaze se u takozvanom valutnom odnosu ili odnosu iz osnovnog posla koji je po pravilu ugovorne prirode (na primer ugovor o prodaji u kome je poverilac novčane obaveze prodavac, a dužnik novčane obaveze kupac). U tom odnosu je izričito ili prećutno ugovoreno da dužnik treba da izvrši plaćanje novčane obaveze žiralnim novcem na određeni račun poverioca.[6] Naknadno, međutim, dužnik dobija mejl za koji veruje da potiče od poverioca, u kome dobija nove instrukcije za plaćanje sa drugim brojem računa primaoca plaćanja. Kada dužnik izvrši plaćanje u skladu sa uputstvima iz prevarnog mejla, raspodela gubitka u njegovom odnosu sa poveriocem zavisi od odgovora na sledeća pitanja: a) da li izjava volje koja je sadržana u prevarnom mejlu može da se pripiše poveriocu; b) da li je plaćanjem ispunjena ugovorna obaveza dužnika (primarni ugovorni zahtev) i c) da li kompromitovanje poslovnog mejla izaziva odgovornost za štetu između ugovornih strana. U slučaju spora između poverioca i dužnika, za svako od navedenih pitanja značajno je utvrditi ko snosi teret dokaza relevantnih spornih činjenica. Štaviše, za ishod spora između dužnika i poverioca biće često od presudne važnosti upravo pitanje tereta dokazivanja, budući da relevantne činjenice u vezi sa kompromitovanjem poslovnog mejla nije uvek jednostavno dokazati.[7]

3.1. Pripisivanje izjave volje iz prevarnog mejla poveriocu

S obzirom na to da prevarni mejl sadrži novi broj računa za prijem ispunjenja obaveze dužnika, on predstavlja izjavu volje u pravcu ugovaranja novih instrukcija za plaćanje između poverioca i dužnika. Da bi ta izjava volje proizvodila pravna dejstva u odnosu između poverioca i dužnika, neophodno je da ona može da se pripiše poveriocu u čije ime je poslata dužniku. U analizi ovog pitanja nadalje treba praviti razliku između dve situacije u kojima je: 1) izjava poslata sa adrese elektronske pošte poverioca ili 2) izjava poslata sa mejl-adrese koja nije adresa elektronske pošte poverioca.

3.1.1. Izjava volje poslata sa mejl-adrese poverioca

Činjenica da su nove instrukcije za plaćanje poslate sa mejl-adrese kojom se poverilac inače služi u svom poslovanju sama po sebi nije dokaz autentičnosti izjave volje poverioca. Naime, poznato je da mejlovi nisu siguran i pouzdan način

[6] O žiralnom novcu kao ugovorenom sredstvu plaćanja više vid. Radović, 2016, pp. 28 *et seq.*

[7] Primera radi, nekada nije moguće utvrditi čiji je računarski sistem kompromitovan i kako je treće lice došlo do informacija o poslovnom odnosu između stranaka da bi moglo da uputi kredibilan prevarni mejl.

identifikacije pošiljaoca, budući da je za njihovo slanje dovoljno poznavanje određenih parametara za pristup mejl nalogu (na primer adrese elektronske pošte i odgovarajuće lozinke), koji mogu da dođu u posed neovlašćenih trećih lica. Uz to, postoji mogućnost presretanja i falsifikovanja, odnosno neovlašćene izmene autentičnog mejla pošiljaoca na njegovom putu do primaoca u slučaju takozvanog napada „čoveka u sredini", te u tom smislu takođe nema potpune sigurnosti da je mejl sa sadržinom koju dužnik primi sa adrese poverioca stvarno poslao poverilac. Iz navedenih razloga se ne može neoborivo smatrati da je svaka izjava volje poslata sa mejl-adrese poverioca autentična, tj. da je zaista potekla od poverioca.

Imajući u vidu da je u sporu oko autentičnosti izjave volje sa novim instrukcijama za plaćanje dužnik taj koji tvrdi da je konkretnu izjavu volje dao poverilac ili od njega ovlašćeno lice, iz čega dalje izvodi zaključak da je punovažno ugovoren novi račun za prijem ispunjenja novčane obaveze, na njemu je teret dokazivanja navedene činjenice (Borges, 2005, p. 3316). Naime, osnovno pravilo parničnog postupka je da svaka strana treba da predloži dokaze za činjenice koje tvrdi i na kojima zasniva svoj zahtev ili osporava zahtev suprotne strane (Zakon o parničnom postupku, 2011, čl. 7 i 228). Budući da dužnik u sporu tvrdi da je izvršio obavezu plaćanja (prigovor ispunjenja ugovora), on treba da dokaže da je platio saglasno punovažnim instrukcijama poverioca. Međutim, kao što je objašnjeno, slanje mejla sa određenog naloga elektronske pošte samo po sebi nije nesporan dokaz da je izjavu sadržanu u mejlu dao poverilac. Otuda je opšte pravilo o teretu dokazivanja veoma strogo za dužnika u slučaju kompromitovanog mejl naloga poverioca, imajući u vidu da se korišćenje računarskog sistema i mejl naloga poverioca ne nalaze u njegovoj sferi uticaja. Pošto je pružanje direktnog dokaza da je upravo poverilac poslao mejl određene sadržine *probatio diabolica* za dužnika, opravdano se postavlja pitanje da li je u ovom slučaju moguće prihvatiti dokaz na prvi pogled (*prima facie* dokaz), kako bi se olakšao procesni položaj dužnika (Borges, 2005, p. 3316).

Dokaz na prvi pogled postoji kada određene dokazane činjenice po iskustvu redovno omogućavaju zaključak o drugim, sa njima povezanim, nedokazanim činjenicama (Marković, 2007, p. 230; Hofmann, 2005, p. 445; Eggers & Goerth, 2005, p. 493; Borges, 2005, p. 3317). Prihvatanje dokaza na prvi pogled značilo bi da dužnik samo treba da dokaže da je primio mejl sa adrese elektronske pošte poverioca, iz čega bi sud posredno izveo zaključak da, u skladu sa iskustvom, mejlovi poslati sa mejl naloga određenog lica redovno potiču upravo od tog lica. U slučaju da poverilac osporava autentičnost mejla poslatog sa njegove adrese, on bi morao da dokaže činjenice koje bi stvorile ozbiljnu sumnju u pretpostavljeni redovan tok stvari u datom slučaju (Borges, 2005, p. 3317). Drugim rečima, na poveriocu bi bilo da obori pretpostavku da je on poslao mejl dokazivanjem činjenica koje bi u dovoljnoj meri učinile verovatnim

da se konkretan slučaj razlikuje od redovnog ili uobičajenog.[8] Sledstveno tome, ovde bi primena dokaza na prvi pogled dovela do sličnog efekta kao prebacivanje tereta dokazivanja autentičnosti izjave volje sa dužnika na poverioca.

Primena shvatanja o *prima facie* dokazu mogla bi da ima veliki značaj u sporovima povodom kompromitovanog mejl naloga. Međutim, sud može da prihvati dokaz na prvi pogled samo ako ne postoji sumnja u sigurnost, odnosno nepovredivost mejl naloga. U tom smislu bi bilo neophodno utvrditi da li je parametre za pristup mejl nalogu uopšte moguće otkriti bez „pomoći" poverioca. Ako je mejl nalog tako siguran da je verovatnoća otkrivanja parametara za pristup izrazito mala, sud bi morao da prihvati *prima facie* dokaz da je poverilac poslao sporni mejl (Borges, 2005, p. 3317). Ipak, iskustvo pokazuje da mejl nalozi nisu u toj meri sigurni da bi „garantovali" nemogućnost pristupa od strane trećih neovlašćenih lica. To je glavni razlog koji se u uporednom pravu ističe protiv prihvatanja dokaza na prvi pogled (upor. Borges, 2005, p. 3317). Smatra se da dokaz na prvi pogled ne može da se prihvati kod autentifikacije putem jednostavne lozinke za pristup mejl nalogu, jer postoje brojni načini da treće neovlašćeno lice sazna tu lozinku (na primer uz pomoć fišinga, farminga /engl. *pharming/* ili trojanca) (Borges, 2005, p. 3317).

Važno je istaći da u nedostatku zakonskog prebacivanja tereta dokazivanja autentičnosti izjave volje poverioca, odbacivanje dokaza na prvi pogled dovodi dužnika u izrazito nepovoljan položaj. Od njega se očekuje da dokaže da je upravo poverilac poslao određeni mejl, pri čemu ne bi bilo dovoljno samo dokazati da je mejl poslat sa adrese elektronske pošte koju poverilac inače koristi. Otuda se postavlja pitanje da li je dozvoljeno da poverilac i dužnik unapred ugovore da će se slanje mejlova sa određene adrese elektronske pošte poverioca neoborivo smatrati njegovom izjavom volje.[9] U slučaju da je takva ugovorna odredba bila sastavni deo opštih uslova poslovanja dužnika, njeno dejstvo bi moglo da se ospori kao nepravično i preterano strogo prema poveriocu (Zakon o obligacionim odnosima, 1978 – ZOO, čl. 143).[10] Nasuprot

[8] U praksi povodom zloupotreba platnih kartica „bi često tek dokazivanje masovnih prevara pod sličnim okolnostima slučaja bilo dovoljno da poljulja zaključak suda na prvi pogled", vid. Marković, 2007, p. 231. Vid. i: Borges, 2005, p. 3317. Dokaz na prvi pogled moglo bi da obori i pružanje konkretnog dokaza da je poverilac bio žrtva fišing napada. S druge strane, poverilac neće moći da dokaže da je bio žrtva farminga ili trojanca pomoću kojih mu je treće lice uzelo podatke za pristup mejl nalogu.

[9] U kanadskoj sudskoj praksi smatra se dozvoljenim ugovaranje da će poverilac davati instrukcije za plaćanje dužniku sa određene mejl-adrese i da će dužnik moći da se osloni na instrukcije koje deluju da su potekle od poverioca, pod uslovom da je bio savestan, te da je u dobroj veri smatrao da su date instrukcije autentične. Vid. Ontario SCJ, 2017. U tom slučaju, poverilac snosi gubitak zbog prevare putem kompromitovanja poslovnog mejla (vid. Ontario SCJ, 2019; Moosajee, Munga & Nxumalo, 2024).

[10] O pojmu opštih uslova poslovanja više vid. Radović, 2019, p. 339. O kontroli opštih uslova

tome, ako je takva odredba posledica individualnog pregovaranja i važi obostrano, i za izjave sa mejl naloga poverioca i za izjave sa mejl naloga dužnika, ona bi načelno mogla da bude punovažna. Ipak, preporučljivo je da se i tada za važna pitanja, poput izmene instrukcija za plaćanje, predvidi obaveza primaoca mejla da izvrši dodatnu proveru kod saugovarača mimo korespondencije elektronskom poštom (na primer putem telefona ili video-poziva).

U nemačkom pravu, čak i ako dužnik ne uspe da dokaže da je izjavu volje sa novim instrukcijama za plaćanje dao poverilac, ona bi svejedno mogla da se pripiše poveriocu ako bi bili ispunjeni uslovi za odgovornost zbog izazivanja pravnog privida da je sporni mejl potekao od njega. Zaštita poverenja u pravni privid moguća je samo ako je dužnik bio savestan, što znači da nije znao niti je zanemario očigledne indicije da je reč o prevari (Rieder, 2004, pp. 93-94). Prema tome, ako je prevarni mejl poslat u neuobičajeno vreme (na primer van radnog vremena poverioca), a sadržao je neuverljiva obrazloženja za plaćanje na račun u zemlji u kojoj poverilac ne obavlja delatnost, uz korišćenje reči i izraza koji uopšte nisu svojstveni poveriocu i sl. (upor. Zahrte, 2023, Rn. 130d), treba smatrati da nije ispunjen zahtev savesnosti budući da je dužnik ignorisao očigledne signale da poruku nije zaista poslao poverilac.[11] Nasuprot tome, ako je dužnik bio savestan, zaštita njegovog poverenja u pravni privid bila bi moguća samo ako se utvrdi da je poverilac „izazvao", odnosno stvorio pravni privid svojim skrivljenim radnjama ili propuštanjem.[12] Ovde treba naglasiti da zloupotreba identiteta poverioca i falsifikovanje izjave volje u njegovo ime od trećeg neovlašćenog lica samo po sebi ne znači da je poverilac izazvao pravni privid.[13] Otuda bi trebalo da dužnik koji se poziva na zaštitu poverenja u pravni privid dokaže konkretne okolnosti slučaja koje ukazuju na to da je poverilac skrivljeno omogućio trećem licu izradu prevarnog mejla u njegovo ime.

Za razliku od nemačkog prava, sporno je da li bi u srpskom pravu zaštita poverenja u pravni privid mogla da dovede do toga da se izjava volje trećeg neovlašćenog lica, koje je falsifikovalo, odnosno preuzelo identitet poverioca, tretira kao izjava volje poverioca. S jedne strane, takva mogućnost nije predviđena Zakonom

poslovanja u nemačkom i francuskom pravu više vid. Vukadinović, 2021, pp. 354 *et seq*.; Vukadinović, 2020, pp. 10 *et seq*.

[11] Međutim, u poslednje vreme prevarni mejlovi postaju sve profesionalniji, tako da nije lako na prvi pogled prepoznati da je reč o prevari (Zahrte, 2023, Rn. 130d; upor. Maihold, 2022, Rn. 51).

[12] Više vid. Rieder, 2004, pp. 96-97. Iako nemačka sudska praksa i jedan deo pravne teorije stoji na stanovištu da je za izazivanje pravnog privida potrebno utvrditi krivicu štetnika, postoji i mišljenje da njegova odgovornost treba da bude nezavisna od krivice, već zasnovana na izazivanju povećanog rizika koji on može bolje da savlada nego druga strana – oštećeni.

[13] Izazivanje pravnog privida ne postoji ako poverilac nije znao da treće neovlašćeno lice zloupotrebljava njegov identitet, te samim tim nije mogao ni da spreči nastanak pravnog privida (Borges, 2005, p. 3314).

o obligacionim odnosima, a mogla bi da se smatra i suprotnom raciju pojedinih njegovih pravila.[14] S druge strane, postoje trgovačke uzanse iz Opštih uzansi za promet robom koje su dozvoljavale pripisivanje izjave volje neovlašćenog lica trgovcu u slučaju zaključenja ugovora preko memoranduma (poslovnog papira), pa tako i dovele do razvoja sudske prakse koja to potvrđuje. Međutim, sporno je da li bi ista praksa bila nastavljena i danas, nakon skoro pola veka važenja Zakona o obligacionim odnosima, koji je u velikoj meri potisnuo značaj Opštih uzansi u savremenom srpskom pravu.

3.1.2. Izjava volje poslata sa druge mejl-adrese različite od adrese poverioca

Kada su nove instrukcije za plaćanje poslate sa druge mejl-adrese u odnosu na onu koju poverilac inače koristi, dužnik koji tvrdi da je reč o izjavi volje poverioca treba da dokaže da je izjava potekla od poverioca. U tom pogledu nije dovoljno pokazati da poruka iz mejla na prvi pogled deluje autentično. Sama činjenica da se mejl pošiljaoca razlikuje od mejla poverioca, makar i najmanje (na primer *aol@org.rs* i *aoI@org.rs*), zahteva pružanje dodatnih konkretnih dokaza da je izjava potekla upravo od poverioca ili drugog lica po njegovom nalogu, a ne od trećeg neovlašćenog lica. U suprotnom, smatraće se da konkretan mejl nije poslao poverilac. Sledstveno tome, nove instrukcije za plaćanje iz takvog mejla ne bi proizvodile dejstvo u odnosu između poverioca i dužnika. Drugim rečima, dužnik bi i dalje bio obavezan da izvrši plaćanje u skladu sa instrukcijama koje su bile ugovorene i na snazi nezavisno od prevarnog mejla.

Međutim, dužnik bi i ovde mogao da se poziva na zaštitu poverenja u pravni privid, pod uslovom da uspe da dokaže svoju savesnost i da je poverilac odgovoran za izazivanje pravnog privida. Ipak, čini se da takva mogućnost u ovom slučaju ostaje samo teorijska ako se ima u vidu da upotreba očigledno različite mejl-adrese u odnosu na adresu poverioca čini dužnika nesavesnim, dok istovremeno nije jednostavno utvrditi da je poverilac izazvao pravni privid budući da treće lice nije koristilo njegov mejl nalog, a moglo je da sazna podatke iz poslovnog odnosa sa dužnikom i iz računarskog sistema žrtve prevare. Pošto dužnik snosi teret dokazivanja uslova za odgovornost poverioca zbog izazivanja pravnog privida, odatle proizlazi da pripisivanje prevarne izjave volje poveriocu po navedenom osnovu najčešće neće biti moguće.

[14] Primera radi, neovlašćeni zastupnik ne može da zaključi ugovor u ime neovlašćeno zastupanog protiv njegove volje (ZOO, čl. 88), pa bi po istoj logici trebalo smatrati da neovlašćeno treće lice koje falsifikuje identitet poverioca ne može da izjavi volju umesto njega.

3.2. Primarni ugovorni zahtev – (ne)ispunjenje dužnikove novčane obaveze

Izričit ili prećutan sporazum poverioca i dužnika da novčana obaveza mora da se izvrši prenosom određenog iznosa novčanih sredstava na određeni račun predstavlja ugovaranje posebnog sredstva i načina plaćanja.[15] Otuda se prevarna izjava volje koja sadrži nove instrukcije za plaćanje u odnosu između poverioca i dužnika tretira kao predlog za izmenu navedenog ugovorenog načina plaćanja. U slučaju da ta izjava može da se pripiše poveriocu, tako što dužnik uspe da dokaže da ju je poslao poverilac ili lice ovlašćeno od poverioca, plaćanje u skladu sa novim instrukcijama značilo bi prihvatanje izmene ugovora, pa bi sledstveno tome dužnikova novčana obaveza bila ispunjena u skladu sa ugovorom. U suprotnom, ako ta izjava ne može da se pripiše poveriocu, smatraće se da ugovoren način plaćanja nije izmenjen jer ne postoji saglasnost druge ugovorne strane (poverioca), zbog čega dužnik ne bi mogao da ispuni svoju novčanu obavezu plaćanjem na novi broj računa iz osporenog mejla.[16] Iz izloženog proizlazi da ispunjenje primarnog ugovornog zahteva, odnosno dužnikove ugovorene novčane obaveze (na primer obaveze plaćanja cene iz ugovora o prodaji) zavisi od toga da li izjava volje sa novim instrukcijama za plaćanje može da se pripiše poveriocu kao drugoj ugovornoj strani.

3.3. Pravo na naknadu štete

Mogućnost ostvarenja prava na naknadu štete aktuelna je samo u situaciji kada se utvrdi da primarni ugovorni zahtev nije ispunjen. To je logično jer dužnik koji je ispunio svoju novčanu obavezu onako kako je ugovoreno ne može biti odgovoran za štetu koja bi bila prouzrokovana poveriocu time što je postupio po instrukcijama iz mejla koji se pripisuje poveriocu. Nasuprot tome, ako se dođe do zaključka da dužnikova novčana obaveza nije ispunjena plaćanjem u skladu sa novim instrukcijama iz prevarnog mejla, poverilac ima pravo da zahteva ispunjenje primarnog ugovornog zahteva, kao i naknadu štete zbog docnje, u vidu zatezne kamate i eventualno ostale (predvidljive) štete (ZOO, čl. 266, st. 1).[17] Jasno je da u tom slučaju dužnik trpi gubitak budući da će morati ponovo da plati dugovani iznos uvećan za kamatu, a možda i dodatnu naknadu štete poveriocu. Stoga se postavlja

[15] Ugovoreno sredstvo plaćanja u ovom slučaju je žiralni novac ili sredstva na računu, dok se način plaćanja sastoji u prenosu novčanih sredstava posredstvom banaka, a ne direktno poveriocu.

[16] Vid. Radović, 2016, p. 31: „...ako između poverioca i dužnika postoji dogovor o plaćanju na tačno određeni platni račun, onda se žiralni novac smatra ugovorenim sredstvom plaćanja samo u slučaju plaćanja na taj račun, ali ne i u slučaju plaćanja na neki drugi platni račun poverioca."

[17] Pravo na potpunu naknadu štete postoji ako je dužnik poverovao u autentičnost prevarnog mejla i, stoga, nije ispunio svoju obavezu zbog krajnje nepažnje.

pitanje da li dužnik može da prevali gubitak zbog prevare usled kompromitovanja poslovnog mejla na poverioca pozivanjem na njegovu odgovornost za štetu. Takvo dužnikovo pravo na naknadu štete predstavlja dospelo uzajamno istovrsno (novčano) potraživanje prema poveriocu, pa bi moglo da se kompenzuje (prebije) sa poveriočevim potraživanjima prema njemu, čime se gubitak zbog prevare u potpunosti ili delimično prevaljuje na poverioca.

Poveriočeva odgovornost za štetu može da bude zasnovana na izazivanju poverenja u pravni privid da je prevarni mejl autentičan, odnosno potekao upravo od njega, ili na povredi drugih, sporednih ugovornih obaveza (na primer opšte obaveze obaveštavanja ili obaveze neprouzrokovanja štete saugovaraču). U nemačkom pravu, dužnik koji uspe da dokaže odgovornost poverioca za izazivanje pravnog privida ima pravo izbora da li će se osloniti na fikciju da stvarno stanje odgovara prividnom, tj. da se izjava volje trećeg lica tretira kao izjava poverioca, ili će zahtevati naknadu štete prouzrokovane stvorenim poverenjem u pravni privid (više vid. Rieder, 2004, pp. 100-101). Za razliku od toga, čini se da u srpskom pravu nema mesta primeni pomenute fikcije, te bi dužnik po osnovu zaštite poverenja u pravni privid mogao da zahteva jedino naknadu štete od poverioca. Preduslov za to je, naravno, dužnikova savesnost i pružanje dokaza da je poverilac određenim radnjama ili propuštanjima stvorio pravni privid. Međutim, kao što je već objašnjeno, pružanje takvih dokaza u konkretnom slučaju može da bude vrlo problematično, pri čemu i ovde teret dokazivanja snosi dužnik.

Smatraće se da dužnik nije bio savestan ako su okolnosti u vezi sa prijemom prevarnog mejla očigledno ukazivale na to da ga nije poslao poverilac (upor. Schmalenbach, 2024, Rn. 13e). S druge strane, neće se smatrati da je poverilac izazvao pravni privid ako nije kriv za falsifikovanje njegovog identiteta putem komunikacije elektronskom poštom. Od poverioca se u svakom slučaju očekuje da se uzdrži od postupaka kojima se saugovaraču može prouzrokovati šteta, pa stoga treba da uloži dužnu pažnju kako bi sprečio kompromitovanje svog naloga elektronske pošte (na primer odgovarajućim čuvanjem lozinke za pristup mejl nalogu), da u razumnoj meri čuva svoj računarski sistem od pristupa neovlašćenih trećih lica, kao i da obavesti dužnika čim sazna da treće neovlašćeno lice šalje prevarne mejlove poslovnim partnerima u njegovo ime. Naime, u slučaju da je poveriočeva adresa elektronske pošte kompromitovana, tako da treće neovlašćeno lice ima pristup njegovom legitimnom mejl nalogu, treba smatrati da je poverilac izazvao pravni privid nečinjenjem ako od dana saznanja za mogućnost neovlašćenog pristupa mejl nalogu nije o toj činjenici obavestio dužnika.[18] Međutim, poverilac nije dužan da na

[18] ZOO, čl. 268: „Ugovorna strana koja je dužna da obavesti drugu stranu o činjenicama koje su od uticaja na njihov međusobni odnos, odgovara za štetu koju pretrpi druga strana zbog toga što nije bila na vreme obaveštena." (vid. i: Borges, 2005, pp. 3314 i 3315).

svojim računarima instalira najjači sistem zaštite od fišing i malver napada (upor. Schmalenbach, 2024, Rn. 13a), a nije dužan ni da zna da je treće lice hakovalo njegov računarski sistem ili da presreće njegovu elektronsku poštu na putu ka primaocu.

Najzad, čak i kada bi dužnik uspeo da dokaže činjenice na kojima zasniva zahtev za naknadu štete, ostaje mogućnost umanjenja njegovog prava na naknadu na osnovu pravila o doprinosu oštećenika šteti. Sledstveno tome, dužnik koji je doprineo da šteta nastane ili da bude veća nego što bi inače bila imaće pravo na srazmerno smanjenu naknadu (ZOO, čl. 192). Važno je naglasiti da doprinos šteti ovde ne može da se ogleda u tome što je dužnik poverovao u autentičnost prevarnog mejla i izvršio plaćanje u skladu sa tamo navedenim instrukcijama, budući da je već prethodno utvrđena odgovornost poverioca za izazivanje pravnog privida, tako da navedene posledice poverenja dužnika u principu padaju poveriocu na teret. Međutim, postavlja se pitanje da li tako prevaljeni gubitak na poverioca može ponovo da se potpuno ili delimično „vrati" na dužnika preko instituta doprinosa oštećenika šteti.[19]

Kao što je objašnjeno, jedan od uslova za postojanje odgovornosti poverioca za izazivanje pravnog privida sastoji se u tome da dužnik nije zanemario „očigledne signale" da je reč o prevarnom mejlu. U tom pogledu, zaštitu ne treba da uživa jedino preterano lakoverni dužnik, koji je sa grubom nepažnjom poverovao u autentičnost mejla (upor. Schmalenbach, 2024, Rn. 13e). Nasuprot tome, za primenu pravila o doprinosu oštećenika šteti dolazi u obzir ne samo gruba (krajnja) nego i obična nepažnja dužnika.[20] Otuda bi poverilac mogao da dokazuje da dužnik, iako nije bio krajnje nepažljiv kada je poverovao da su nove instrukcije za plaćanje zaista potekle od poverioca, ipak jeste bio nepažljiv, jer se prilikom izvršavanja svoje obaveze nije ponašao sa pažnjom koja se u pravnom prometu zahteva od privrednih subjekata – sa pažnjom dobrog privrednika.[21] Kao argument u prilog običnoj nepažnji dužnika moglo bi da se istakne, primera radi, da dužnik nije primetio neobične aspekte mejla, poput gramatičkih i sintaksnih grešaka, načina obraćanja ili drugačijeg načina „potpisivanja", da se plaćanje traži na račun u zemlji različitoj od zemlje poverioca, kao i da nije proverio sa poveriocem telefonskim pozivom ili na drugi način, iako je posumnjao

[19] Otuda se u američkoj sudskoj praksi ispituje da li je bilo koja strana svojom običnom nepažnjom doprinela prevari, tako da se gubitak raspodeljuje na osnovu upoređivanja krivice dužnika i poverioca u datom slučaju (vid. U.S. Court of Appeals, 2018).

[20] Iako u pravnoj teoriji postoje shvatanja da se pravilo Zakona o obligacionim odnosima o doprinosu oštećenika šteti zasniva isključivo na uzročno-posledičnoj vezi između radnje ili propuštanja oštećenika i nastale štete, sudska praksa stoji na stanovištu da je u tom pogledu ipak relevantno utvrditi krivicu dužnika, te da li je „njegovo ponašanje bilo drukčije od redovnog, uobičajenog, standardnog ponašanja drugih osoba u takvoj situaciji" (Karanikić Mirić, 2024, pp. 669-670).

[21] Reč je o primeni čl. 18, st. 1 ZOO: „Strana u obligacionom odnosu dužna je da u izvršavanju svoje obaveze postupa sa pažnjom koja se u pravnom prometu zahteva u odgovarajućoj vrsti obligacionih odnosa (pažnja dobrog privrednika, odnosno pažnja dobrog domaćina)."

da mejl možda nije autentičan (upor. Borges, 2005, p. 3314). Za razliku od uslova za odgovornost poverioca za izazivanje pravnog privida, teret dokazivanja uslova za srazmerno smanjenje naknade štete snosi poverilac, a ne dužnik.

4. Raspodela gubitka u sudskoj praksi

U Srbiji se pitanje raspodele gubitka usled kompromitovanja poslovnog mejla postavilo u sporu pred Privrednim sudom u Beogradu (Presuda PS u Beogradu, 2018), nakon čega je po žalbi o istom pitanju odlučivao Privredni apelacioni sud (Presuda PAS, 2020), a zatim po reviziji i Vrhovni kasacioni sud (Presuda VKS, 2021). U konkretnom slučaju, dva privredna subjekta zaključila su ugovor o prodaji, po osnovu koga je prodavac isporučio robu, a kupac bio dužan da plati cenu. Iako je kupac dve fakture uredno platio, treću fakturu je primio mejlom sa izmenjenim instrukcijama za plaćanje. Mejl je poslat sa adrese elektronske pošte koju je prodavac redovno koristio u svom poslovanju i dotadašnjoj korespondenciji sa kupcem, a stigao je kupcu van radnog vremena, oko 8 sati uveče. Nakon sprovođenja dokaznog postupka, koji je uključivao i pribavljanje nalaza veštaka za informacione tehnologije, prvostepeni sud je zaključio da nema dokaza da je tužilac poslao sporni mejl, kao i da se ne može utvrditi ko je stvarni pošiljalac novih instrukcija za plaćanje (Presuda PS u Beogradu, 2018).

U postupku po žalbi, a potom i po reviziji, sudovi su nedvosmisleno stali na stanovište da činjenica prijema novih instrukcija za plaćanje (izjave volje) sa mejl-adrese prodavca (poverioca) sama po sebi nije dovoljan dokaz da je te instrukcije zaista poslao prodavac. Privredni apelacioni sud u tom smislu naglašava sledeće: „opštepoznata stvar je da se *e-mail* adrese presreću i da je moguća zloupotreba te vrste komunikacije" (Presuda PAS, 2020). Slično tome, Vrhovni kasacioni sud ističe da se „kod zaključenja ugovora o međunarodnoj prodaji robe gde se komunikacija obavlja pretežno u elektronskom obliku, moraju uzeti u obzir svi rizici takvog posla, računajući i mogućnost zloupotrebe elektronskih naloga preko kojih se obavlja ta komunikacija, budući da u svetu savremene informacione tehnologije, tzv. hakerski napadi nisu retkost" (Presuda VKS, 2021). Iako to nije izričito pomenuto, jasno je da takvim stavom sudovi odbijaju mogućnost primene dokaza na prvi pogled (*prima facie* dokaza) da je sporni mejl poslalo lice sa čije adrese elektronske pošte je upućen.

Pošto u datom sporu dužnik nije dokazao da je poverilac izazvao pravni privid, te da su ispunjeni i svi ostali uslovi da bi on odgovarao za štetu koja je nastala zbog dužnikovog pouzdanja u autentičnost prevarne mejl poruke, na osnovu analize pružene u ovom radu trebalo je zaključiti da dužnik kao žrtva prevare u celosti snosi gubitak izazvan kompromitovanjem poslovnog mejla. Međutim, sudovi su se svejedno upustili u ispitivanje stepena pažnje koju je dužnik uložio

kada je poverovao da prevarne instrukcije za plaćanje potiču od poverioca. U tom pogledu Vrhovni kasacioni sud ističe: „Elektronska poruka koja je sadržala izmenjene instrukcije za plaćanje odstupala je od uobičajene poslovne prakse koja se do tada odvijala između stranaka, i to kako proizlazi iz utvrđenih činjenica, iz najmanje dva razloga: poslata je van radnog vremena (u 20:11 časova) i sadržala je instrukciju za plaćanja koja pre toga nikada nije bila izdata od strane tužioca..." (Presuda VKS, 2021). Iz toga se, nadalje, izvodi zaključak da su navedene okolnosti iziskivale „pojačanu pažnju tuženog prilikom ispunjenja svoje obaveze" (Presuda VKS, 2021). Pa ipak, „tuženi je postupio po datoj instrukciji ne proveravajući njenu autentičnost, što znači da tuženi nije pristupio sa dovoljno pažnje jer je navedenu smetnju blagovremenim delovanjem (proverom kod tužioca da li je predmetni mejl autentičan i da li je to zaista njegova instrukcija), bilo moguće otkloniti i savladati" (Presuda VKS, 2021). Na isti način je rezonovao i Privredni apelacioni sud, navodeći da je kupac „bio dužan da racionalno postupi, što podrazumeva da pre plaćanja po izmenjenim instrukcijama, izvrši proveru u komunikaciji sa tužiocem, telefonskim putem ili na drugi način, obzirom da se radi o dispoziciji plaćanja koja se razlikuje od uobičajenog načina poslovanja" (Presuda PAS, 2020).

Na osnovu svega izloženog Privredni apelacioni sud i Vrhovni kasacioni sud zaključuju da gubitak usled kompromitovanja poslovnog mejla treba u celosti da snosi dužnik (kupac), jer nije uložio dužnu pažnju prilikom izvršenja svoje novčane obaveze.[22] Iz toga proizlazi da u sudskoj praksi obična nepažnja dužnika prilikom plaćanja u skladu sa prevarnim instrukcijama dovodi do potpune nemogućnosti prevaljivanja gubitka na poverioca, a ne do srazmernog smanjenja naknade u skladu sa već objašnjenim pravilima o doprinosu oštećenika šteti. Iz citiranih delova presuda čini se da sudovi pretpostavljaju postojanje obaveze dužnika da proveri sa poveriocem ispravnost dobijenih instrukcija čim postoje razlozi za sumnju u autentičnost mejla. Ako je tako, onda zaista svako dužnikovo postupanje suprotno navedenoj obavezi dovodi do njegovog stoprocentnog doprinosa šteti, jer da je proverio kod poverioca, sigurno ne bi izvršio plaćanje na račun prevaranta. Konačno, važno je napomenuti da su sudovi pribegli utvrđivanju obične nepažnje dužnika, nezavisno od pitanja da li je uopšte poverilac odgovoran za izazivanje pravnog privida zbog koga je dužniku pričinjena šteta.[23] Otuda ostaje otvoreno

[22] Slično tome, u američkoj sudskoj praksi gubitak zbog prevare snosi dužnik ako nije uložio razuman stepen pažnje, odnosno nije proverio sa poveriocem koje od različitih instrukcija za plaćanje treba da primeni (vid. The United States District Court, M. D. Florida, *Arrow Truck Sales, Inc. v. Top Quality Truck & Equipment, Inc.* (8:14-cv-02052), 2015 (nav. prema: Harrison, 2024); Walker, 2023, p. 36).

[23] U kanadskoj sudskoj praksi, u nedostatku ugovornih odredbi o raspodeli rizika zbog prevare putem kompromitovanja poslovnog mejla, prevaljivanje gubitka na poverioca bilo bi moguće samo ako se dokaže njegova krivica u prouzrokovanju štete dužniku (vid. Ontario SCJ, 2019.

pitanje kako bi sudovi raspodelili gubitak zbog kompromitovanja poslovnog mejla u slučaju da je dužnik u svemu postupio u skladu sa pažnjom dobrog privrednika. Reč je o situacijama u kojima nije bilo razloga za sumnju u autentičnost mejla, pa samim tim nije ni postojala dužnikova obaveza provere kod poverioca.

5. Zaključak

Prethodna analiza je pokazala da će u preovlađujućem broju slučajeva gubitak zbog prevare usled kompromitovanja poslovnog mejla snositi dužnik, bilo zato što će se smatrati da nije ispunio novčanu obavezu prema poveriocu, bilo zato što je svojim radnjama doprineo sopstvenoj šteti jer nije uložio dužnu pažnju kada je poverovao u autentičnost mejl poruke. Pritom je dužnik u lošijem procesnom položaju, budući da snosi teret dokazivanja relevantnih činjenica na kojima zasniva svoja prava da gubitak prevali na poverioca. U situaciji kada poverilac ospori da je dao nove instrukcije za plaćanje putem mejla, ne može se prihvatiti dokaz na prvi pogled da je mejl autentičan, čak ni kada je poslat sa adrese elektronske pošte koju poverilac inače koristi. Otuda bi dužnik morao da pruži druge, dodatne dokaze da je mejl zaista poslao poverilac, iako su u pitanju okolnosti izvan njegove sfere uticaja. Kao posledica nemogućnosti pružanja takvog dokaza smatraće se da nove instrukcije za plaćanje nije poslao poverilac, te da dužnik nije ispunio svoju novčanu obavezu, zbog čega će morati „ponovo" da plati, kao i da poveriocu naknadi štetu zbog docnje.

Druga mogućnost da dužnik prevali navedeni gubitak na poverioca postoji na osnovu odgovornosti poverioca za štetu zbog izazivanja pravnog privida da je mejl potekao od njega. Pritom i ovde dužnik snosi teret dokazivanja da je poverilac izazvao pravni privid u datom slučaju. Međutim, čak i kada bi uspeo to da dokaže, poverilac može da gubitak potpuno ili delimično ponovo prevali na dužnika dokazivanjem da je on kao oštećeni doprineo svojoj šteti tako što nije uložio pažnju dobrog privrednika prilikom provere autentičnosti mejla. Prevaljivanje gubitka zbog prevare usled kompromitovanja poslovnog mejla na dužnika opravdava se argumentom da je on u boljoj poziciji da upravlja navedenim rizikom, s obzirom na to da poverilac u konkretnom slučaju po pravilu i ne zna da je treće neovlašćeno lice poslalo prevarni mejl u njegovo ime (Harrison, 2024).[24] Osim toga, dužnik ima mogućnost da pod određenim uslovima ostvari povraćaj plaćenog iznosa od banke primaoca, za razliku od poverioca koji ni po kom osnovu to ne bi mogao da zahteva.

Vid. i: Freedman, 2020).

[24] Reč je o pravilu po kome lice koje je u najboljoj poziciji da spreči prevaru primenom razumnog stepena pažnje treba da snosi skrivljeno izazvani gubitak zbog prevare. (vid. i: Walker, 2023, p. 35; U.S. Court of Appeals, 2018).

Literatura

Borges, G. 2005. Rechtsfragen des Phishing – Ein Überblick. *Neue Juristische Wochenschrift – NJW*, 46/2005, pp. 3313-3317.

Cross, C. & Gillett, R. 2020. Exploiting trust for financial gain: an overview of business email compromise (BEC) fraud. *Journal of Financial Crime*, 27(3), pp. 871-884.

Deusch, F. & Eggendorfer, T. 2024. IT-Sicherheit. In: Taeger, J. & Pohle, J. (Hrsg.), *Computerrechts-Handbuch*. Werkstand: 39. München: C. H. Beck.

Eckhardt, J. 2023. TKG § 174 Manuelles Auskunftsverfahren. In: Geppert, M. & Schütz, R. (Hrsg.), *Beck'scher TKG-Kommentar*. 5. Auflage. München: C. H. Beck.

Eggers, C. & Goerth, A. 2005. Die Haftung des Bankkunden für unbefugte Abhebungen mittels ec-Karte und PIN. *Juristische Schulung – JuS*, 6/2005, pp. 492-495.

Freedman, B. 2020. Managing the risks of email compromise fraud. Borden Ladner Gervais LLP. Dostupno na: https://www.lexology.com/library/detail.aspx?g=e5ec24d4-a720-43dc-a4be-26454518bb6d, 22. 7. 2025.

Harrison, M. E. M. 2024. Business Email Compromise Fraud: Should the Party Best Positioned to Avoid the Fraud Bear the Loss? Arnall Golden Gregory LLP. Dostupno na: https://www.agg.com/news-insights/publications/business-email-compromise-fraud-should-the-party-best-positioned-to-avoid-the-fraud-bear-the-loss/, 22. 7. 2025.

Hofmann, C. 2005. Schadensverteilung bei Missbrauch der ec-Karte – Zugleich Besprechung des Urteils des BGH vom 5. Oktober 2004 = WM 2004, 2309. *WertpapierMitteilungen (Zeitschrift für Wirtschafts- und Bankrecht) – WM*, 10/2005, pp. 441-450.

Jones, N. 2024. *Understanding Payments*. Oxon – New York: Routledge.

Jungmann, C. 2023. BGB § 675l Pflichten des Zahlungsdienstnutzers in Bezug auf Zahlungsinstrumente. In: Säcker, F. J. *et al.* (Hrsg.), *Münchener Kommentar zum BGB*. 9. Auflage. München: C. H. Beck.

Karanikić Mirić, M. 2024. *Obligaciono pravo*. Beograd: JP „Službeni glasnik".

Koza, E., Öztürk, A. & Willer, M. 2024. *Social Engineering und Human Hacking – Strategien zur Prävention und Abwehr von Manipulationstechniken in der IT*. Berlin – Heidelberg: Springer.

Maihold, D. 2022. Bankgeschäfte online. In: Ellenberger, J. & Bunte, H.-J. (Hrsg.), *Bankrechts-Handbuch*. Band I. 6. Auflage. München: C. H. Beck.

Marković, M. 2007. Odnos banke i korisnika u slučaju zloupotrebe platnih kartica. *Pravni život*, 13, pp. 217-238.

Moosajee, A., Munga, S. & Nxumalo, O. 2024. *Business email compromise: Who bears the risk of liability?* International Bar Association. Dostupno na: https://www.ibanet.org/business-email-compromise-who-bears-risk-liability, 22. 7. 2025.

Radović, M. 2016. *Platni promet – Pravo bankarskih platnih usluga*. Beograd: Univerzitet u Beogradu – Pravni fakultet.

Radović, M. 2019. Smisao i domen primene regulative opštih uslova poslovanja. *Pravo i privreda*, 7-9/2019, pp. 332-347.

Rieder, M. S. 2004. *Die Rechtsscheinhaftung im elektronischen Geschäftsverkehr*. Berlin: Duncker & Humblot.

Schmalenbach, D. 2024. BGB § 675v Haftung des Zahlers bei missbräuchlicher Nutzung eines Zahlungsinstruments. In: Hau, W. & Poseck, R., *BeckOK BGB*. 72. Edition. München: C. H. Beck.

Schmidt, M. & Pruß, M. 2019. Technische Grundlagen des Internets. In: Auer-Reinsdorff, A. & Conrad, I. (Hrsg.), *Handbuch IT- und Datenschutzrecht*. 3. Auflage. München: C. H. Beck.

U.S. Court of Appeals, 2018. The U.S. Court of Appeals, *Beau Townsend Ford Lincoln v. Don Hinds Ford*, 6th Cir. 2018. Dostupno na: https://law.justia.com/cases/federal/appellate-courts/ca6/17-4177/17-4177-2018-11-27.html, 22. 7. 2025.

UK National Cyber Security Centre. 2020. Business email compromise – Dealing with targeted phishing emails. Dostupno na: https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf, 22. 7. 2025.

Vukadinović, S. G. 2020. Adhezioni ugovori u francuskom pravu. *Strani pravni život*, 1/2020, pp. 5-15.

Vukadinović, S. G. 2021. Pravnoteorijske karakteristike i pravnodogmatski razvoj nemačkog prava opštih uslova poslovanja. *Strani pravni život*, 3/2021, pp. 343-359.

Walker, L. 2023. Who Bears the Risk of Loss When Your Business Email Is Hacked? An Overview of Business Email Compromise Scams and the Potential Risks. *Commercial Law World*, 37(1), pp. 34-37.

Weber, K. 2024. Phishing. In: Weber, K. (Hrsg.), *Weber kompakt, Rechtswörterbuch*. 11. Edition. München: C. H. Beck.

Zahrte, K. 2023. Sonderbedingungen für das Online-Banking. In: Bunte, H.-J. & Zahrte, K. (Hrsg.), *AGB-Banken, AGB-Sparkassen, Sonderbedingungen*. 6. Auflage. München: C. H. Beck.

Zweighaft, D. 2017. Business email compromise and executive impersonation: Are financial institutions exposed?. *Journal of Investment Compliance*, 18(1), pp. 1-7.

Pravni izvori

Zakon o obligacionim odnosima 1978 – ZOO. *Službeni list SFRJ*, br. 29/78, 39/85, 45/89 i 57/89, *Službeni list SRJ*, br. 31/93, *Službeni list SCG*, br. 1/2003 i *Službeni glasnik RS*, br. 18/2020.

Zakon o parničnom postupku 2011. *Službeni glasnik RS*, br. 72/2011, 49/2013, 74/2013, 55/2014, 87/2018, 18/2020 i 10/2023.

Sudska praksa

Ontario SCJ, 2017. Ontario Superior Court of Justice, *Du v. Jameson Bank*, 2017 ONSC 2422 (CanLII). Dostupno na: https://www.canlii.org/en/on/onsc/doc/2017/2017onsc2422/2017onsc2422.html, 22. 7. 2025.

Ontario SCJ, 2019. Ontario Superior Court of Justice (Small Claims Court), *St. Lawrence Testing & Inspection Co. Ltd. v. Lanark Leeds Distribution Ltd.*, 2019 CanLII 69697 (ON SCSM). Dostupno na: https://www.canlii.org/en/on/onscsm/doc/2019/2019canlii69697/2019canlii69697.html, 22. 7. 2025.

Presuda PAS, 2020. Presuda Privrednog apelacionog suda, 4 Pž 1629/19 od 11. 6. 2020. godine.

Presuda PS u Beogradu, 2018. Presuda Privrednog suda u Beogradu, P 5132/18 od 4. 12. 2018. godine.

Presuda VKS, 2021. Presuda Vrhovnog kasacionog suda, Prev 135/2021 od 22. 4. 2021. godine.