



LIETUVOS RESPUBLIKOS
SEIMAS

LIETUVOS RESPUBLIKOS SEIMO KANCELIARIJOS INFORMACIJOS IR KOMUNIKACIJOS DEPARTAMENTO TYRIMŲ SKYRIUS

Gedimino pr. 53, 01109 Vilnius Tel.: (0 5) 209 6170 / (0 5) 209 6185
El. p.: tyrimai@lrs.lt; info@lrs.lt; ikd@lrs.lt www.lrs.lt/info

**Analitinė apžvalga
25/144**

2025-12-11

Finansinis sukčiavimas ir jo prevencijos priemonės kai kuriose valstybėse

Darbe apžvelgiama finansinio sukčiavimo problema ir jo prevencijos priemonės 10 valstybių: Australijoje, Austrijoje, Danijoje, Ispanijoje, Jungtinėje Karalystėje, Nyderlanduose, Prancūzijoje, Suomijoje, Švedijoje ir Vokietijoje. Kai kuriose šalyse (ypač Australijoje, Jungtinėje Karalystėje ir Nyderlanduose), esant tam tikroms sąlygoms, yra galimybė nukentėjusiems nuo finansinių sukčių pretenduoti į kompensacijas.

Įvadas

Dažniausiai pasitaikantys finansinio sukčiavimo tipai yra šie: duomenų viliojimas, investicinis sukčiavimas, telefoninis sukčiavimas, romantinis sukčiavimas, avansiniai mokėjimai ir vadinamasis phishingas¹.

Reikėtų skirti neautorizuotus ir autorizuotus mokėjimus. Finansinio sukčiavimo atveju už neautorizuotą mokėjimą (pavyzdžiui, pasinaudojimą nukentėjusiojo kredito kortelės duomenimis) yra paprasčiau atgauti pinigus. Tuo tarpu autorizuoto mokėjimo atveju, kai asmuo sukčiams pats perveda pinigus, tai yra daug sudėtingiau ir dažnai tai priklauso nuo banko politikos. Kompensacijos išmokėjimas dažniausiai priklauso ir nuo to, ar finansinio sukčiavimo atvejis nebuvo susijęs su paties nukentėjusiojo „dideliu neatsargumu“.

Taip pat pažymėtina, kad finansų įstaigų pinigų pervedimai vyksta per tarpuskaitos arba kliringo sistemą. Tarpuskaitos operacijos užtrunka tam tikrą laiką ir yra vykdomos periodiškai, iš anksto nustatytu metu. Dėl to pervestos lėšos kartais matomos tik kitą dieną, pavedimai nevykdomi poilsio dienomis ir pan. Tarpuskaitos operacijos vyksta tik tarp atskirų rinkos dalyvių (šiuo atveju finansų institucijų), t. y. įskaitymai per mokėjimų namus vyksta tik pervedant lėšas iš vieno banko sąskaitos į kito banko sąskaitą. Tokia operacija nevyksta vykdant pavedimus tarp to paties banko sąskaitų².

Iš naujesnių Europos Sąjungos priemonių kovojant su finansiniu sukčiavimu paminėtina 2025 m. spalio 9 d. įsigaliojusi gavėjo tikrinimo paslauga³. Mokėjimai taps saugesni, kadangi, pagal Momentinių mokėjimų reglamentą, mokėjimo paslaugų teikėjai – bankai, kredito unijos, elektroninių pinigų ir mokėjimo įstaigos – prieš pervesdami lėšas, turės patikrinti, ar mokėjimo pavedime įrašytas lėšų gavėjo vardas, pavardė ar pavadinimas sutampa su nurodytos mokėjimo sąskaitos savininku. Tai kovos su sukčiavimu priemonė – ji skirta apsaugoti mokėtoją tais atvejais, kai sukčiai pateikia sąskaitos numerį su klaidingu vardu, pavyzdžiui, nurodo, kad tai pažįstamo žmogaus, institucijos ar žinomo pardavėjo sąskaita. Pranešimas apie gavėjo pavadinimo patikrinimą bus gautas kiekvieną kartą, kai elektroninės bankininkystės sistemoje ar mobiliuojoje programėlėje bus pradėtas mokėjimas

¹ Sukčiavimo prevencija gyventojams: <https://amlcenter.lt/sukciavimo-prevencija/sukciavimo-prevencija-gyventojams/>

² Tarpuskaita arba kliringas: <https://blog.swedbank.lt/zodynemis/tarpuskaita-arba-kliringas>

³ Gavėjo tikrinimo paslauga: <https://www.lb.lt/lt/gavejo-tikrinimo-paslauga>

eurais. Taip pat vartotojai bus informuojami apie patikrinimo rezultatai ir tuo atveju, jeigu mokėjimas bus atliekamas fiziniuose banko ar kito mokėjimo paslaugų teikėjo padaliniuose.

Kai kurios Europos Parlamento ir Tarybos direktyvos (ES) 2015/2366 2015 m. lapkričio 25 d. dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB⁴, dar vadinamos Antrąja mokėjimo paslaugų direktyva, nuostatos:

- 71 straipsnio (Pranešimas apie neautorizuotas ar netinkamai įvykdytas mokėjimo operacijas ir jų ištaisymas) 1 dalis: Mokėjimo paslaugų teikėjas neautorizuotų ar netinkamai įvykdytų mokėjimo operacijų ištaisymą mokėjimo paslaugų vartotojui atlieka tik tuo atveju, jei mokėjimo paslaugų vartotojas, sužinojęs apie visas tokias mokėjimo operacijas, dėl kurių gali būti pateikiami reikalavimai, įskaitant 89 straipsnyje nurodytus reikalavimus, praneša mokėjimo paslaugų teikėjui nepagrįstai nedelsdamas ir ne vėliau kaip per 13 mėn. nuo nurašymo iš sąskaitos datos;
- 72 straipsnio (Mokėjimo operacijų autentiškumo patvirtinimo ir įvykdymo įrodymas) 1 dalis: Valstybės narės reikalauja, kad jei mokėjimo paslaugų vartotojas neigia autorizavęs įvykdytą mokėjimo operaciją ar teigia, kad mokėjimo operacija buvo įvykdyta netinkamai, mokėjimo paslaugų teikėjas turi įrodyti, kad mokėjimo operacijos autentiškumas buvo patvirtintas, ji buvo tinkamai užregistruota, įrašyta į sąskaitas ir jos nepaveikė techninis sutrikimas arba kitas mokėjimo paslaugos teikėjo teikiamos paslaugos trūkumas. Jei mokėjimo operacija inicijuojama per mokėjimo inicijavimo paslaugų teikėją, mokėjimo inicijavimo paslaugų teikėjas turi įrodyti, kad pagal jo kompetenciją mokėjimo operacijos autentiškumas buvo patvirtintas, ji buvo tinkamai užregistruota ir jos nepaveikė techninis sutrikimas arba kitas trūkumas, susijęs su mokėjimo paslauga, už kurią jis atsako;
- 73 straipsnio (Mokėjimo paslaugų teikėjo atsakomybė už neautorizuotas mokėjimo operacijas) 1 dalis: Valstybės narės užtikrina, kad, nedarant poveikio 71 straipsniui, neautorizuotos mokėjimo operacijos atveju mokėtojo mokėjimo paslaugų teikėjas nedelsdamas ir bet kuriuo atveju ne vėliau kaip iki kitos darbo dienos pabaigos po to, kai sužino arba būna informuotas apie operaciją, mokėtojui sugrąžintų neautorizuotos mokėjimo operacijos sumą, išskyrus atvejus, kai mokėtojo mokėjimo paslaugų teikėjas turi pagrįstų priežasčių įtarti sukčiavimą ir tas priežastis raštu pateikia atitinkamai nacionalinei institucijai. Kai taikytina, mokėtojo mokėjimo paslaugų teikėjas atstato mokėjimo sąskaitos, iš kurios ta suma nurašyta, likutį, kuris būtų buvęs, jeigu neautorizuota mokėjimo operacija nebūtų buvusi įvykdyta. Tokiu būdu taip pat užtikrinama, kad sumos įskaitymo į mokėtojo mokėjimo sąskaitą data būtų ne vėlesnė nei data, kai ta suma nurašyta nuo sąskaitos;
- 74 straipsnio (Mokėtojo atsakomybė už neautorizuotas mokėjimo operacijas) 1 dalis: Nukrypstant nuo 73 straipsnio, mokėtojui gali tekti 50 eurų maksimalios sumos neviršijantys su neautorizuotomis mokėjimo operacijomis susiję nuostoliai, patirti dėl prarastos ar pavogtos mokėjimo priemonės panaudojimo arba dėl neteisėto jos pasisavinimo. Pirma pastraipa netaikoma, jei: a) mokėtojas negalėjo pastebėti mokėjimo priemonės praradimo, vagystės arba neteisėto pasisavinimo iki mokėjimo įvykdymo, išskyrus atvejus, kai mokėtojas veikė nesažiningai; arba b) nuostolis patirtas dėl mokėjimo paslaugų teikėjo ar išorės subjekto, kuriems perduodamas veiklos vykdymas, darbuotojo, tarpininko, filialo veiksmų ar neveikimo. Mokėtojui tenka visi su neautorizuotomis mokėjimo operacijomis susiję nuostoliai, jei mokėtojas juos patyrė veikdamas nesažiningai arba tyčia ar dėl didelio neatsargumo neįvykdo vienos ar kelių pareigų, nustatytų 69 straipsnyje;
- 76 straipsnio (Gavėjo ar per jį inicijuotų mokėjimo operacijų sumų grąžinimas) 1 dalis: Valstybės narės užtikrina, kad mokėtojui būtų suteikta teisė atgauti gavėjo ar per jį inicijuotos autorizuotos ir jau įvykdytos mokėjimo operacijos sumą, kurią mokėjimo paslaugų teikėjas grąžina, jeigu tenkinamos šios abi sąlygos: a) autorizuojant nebuvo nurodyta tiksli mokėjimo

⁴ Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 2015 m. lapkričio 25 d. dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB: <https://eur-lex.europa.eu/eli/dir/2015/2366/oj>

operacijos suma; b) mokėjimo operacijos suma buvo didesnė už sumą, kurios pagrįstai galėjo tikėtis mokėtojas atsižvelgdamas į ankstesnių išlaidų struktūrą, bendrosios sutarties sąlygas ir atitinkamas to atvejo aplinkybes. Mokėjimo paslaugų teikėjo prašymu mokėtojas turi įrodyti, kad tokios sąlygos tenkinamos;

- 77 straipsnio (Prašymai dėl gavėjo ar per jį inicijuotų mokėjimo operacijų sumų grąžinimo) 1 dalis: Valstybės narės užtikrina, kad mokėtojas galėtų prašyti grąžinti gavėjo ar per jį inicijuotos autorizuotos mokėjimo operacijos sumą, kaip nurodyta 76 straipsnyje, per 8 savaites nuo dienos, kai lėšos buvo nurašytos iš sąskaitos;
- 80 straipsnio (Mokėjimo nurodymo neatšaukiamumas) 1–3 dalys: 1. Valstybės narės užtikrina, kad mokėjimo paslaugų vartotojas negalėtų atšaukti mokėjimo nurodymo po to, kai jį gauna mokėtojo mokėjimo paslaugų teikėjas, išskyrus atvejus, kai šiame straipsnyje nurodyta kitaip. 2. Kai mokėjimo operacija inicijuojama mokėjimo inicijavimo paslaugų teikėjo arba gavėjo ar per jį, mokėtojas negali atšaukti mokėjimo nurodymo po to, kai mokėjimo inicijavimo paslaugų teikėjui duoda sutikimą inicijuoti mokėjimo operaciją arba gavėjui duoda sutikimą įvykdyti mokėjimo operaciją. 3. Tačiau tiesioginio debeto atveju ir nedarant poveikio teisei į grąžinimą mokėtojas gali atšaukti mokėjimo nurodymą vėliausiai iki darbo dienos, einančios prieš dieną, kurią susitarta nurašyti lėšas iš sąskaitos, pabaigos.

2025 m. spalio pabaigoje Lietuvos banko valdybos pirmininko pavaduotoja Vaida Markevičienė teigė, kad netrukus bankams gali tekti dažniau padengti žmonėms sukčių išviliotus pinigus. Kol kas tokį grąžinimą daugeliu atveju riboja teisės aktai, tačiau tai gali keistis – Lietuvos iniciatyva šiuo metu keičiama ES Mokėjimo paslaugų direktyva, leisianti su sukčiais susijusį reguliavimą suvienodinti visoje Bendrijoje. Pasak jos, europinis teisėkūros procesas įsiklausė į tai, ką kelia Lietuvos atstovai, kad finansinis sukčiavimas turi atsirasti europiniuose teisės aktuose. Naujas reguliavimas turėtų būti vienodas visos ES mastu, nes pinigai gali keliauti per įvairias valstybes – tik tuomet sistema veiktų efektyviai.

V. Markevičienės teigimu, mokėjimo paslaugų tiekėjai, bankai ar kitos įstaigos kai kuriais atvejais ir dabar turi padengti sukčių išviliotus pinigų sumas. „Jeigu žmonės parodo, kad jie neinicijavo to mokėjimo ir kažkas panaudojo jų tapatybę ir duomenis, pavyzdžiui, į savo įrenginį atsisiuntė programėlę ir be jų žinios padarė mokėjimus, jau ir dabar bankai yra įpareigoti grąžinti pinigus. Tačiau manome, kad ta pareiga turėtų išsiplėsti“.

Be to, pasak V. Markevičienės, šiuo metu kuriama platforma, kurioje bankai ir kitos mokėjimo įstaigos galėtų keistis informacija apie atpažintus sukčiavimo atvejus. „Rinkos dalyviai kartu su Pinigų plovimo prevencijos centru (...) kuria platformą, kurioje būtų galima keistis duomenimis, jeigu rinkos dalyvis įtartų sukčiavimą. Ta platforma leistų realiu laiku reaguoti ir automatiškai atlikti tam tikrus veiksmus“. Toks duomenų keitimasis vyksta ir dabar, tačiau tai užtrunka kelias valandas ir dažniausiai būna pavėluota, nes Lietuvoje yra labai dažni momentiniai mokėjimai, todėl laikas per trumpas, kad būtų spėta sureaguoti⁵.

Šiuo metu Europos Parlamente yra svarstomi siūlymai, kad bankams tektų tam tikra atsakomybė ir jie esant tam tikroms aplinkybėms turėtų kompensuoti nukentėjusiems klientams. Iš svarstomų siūlymų, be kita ko, yra šie: taip galėtų būti, jei bankai nepakankamai rūpinosi klientų apsaugos priemonėmis; jei klientai tapo bankų apsimetėlių finansinio sukčiavimo aukomis; jei mokėjimai sukčiams buvo atlikti be klientų sutikimo. Taip pat tam tikra atsakomybė tektų ir socialinei žiniasklaidai, kuri turėtų kompensuoti bankams už paskelbtą finansinių sukčių turinį, nors apie tai ji buvo įspėta⁶.

⁵ LB valdybos narė: bankams gali tekti dažniau atlyginti sukčių iš sąskaitų išviliotus lėšas:

https://www.lrt.lt/naujienos/verslas/4/2730032/lb-valdybos-nare-bankams-gali-tekti-dazniau-atlyginti-sukciu-is-saskaitu-isviliotas-lesas?srsId=AfmBOorLBJCe9D4qMEqtV6XuJpewcHRB7BJ8l-WRvHMk-yPimW4hK7_V

⁶ Social media giants liable for financial scams under new EU law: <https://www.politico.eu/article/social-media-giants-meta-tiktok-labile-for-financial-scams-under-new-eu-law/>

Australija

Bausmės finansiniams sukčiams gal būti laisvės atėmimas iki 10 metų, didelės baudos, turto įšaldymas, kelionių draudimas. Bausmės gali būti skirtos tiek fiziniams asmenims ir įmonėms Australijoje, tiek užsienyje. Australijos policija kovoja su tamsiojo interneto svetainėmis, kurios prisideda prie kibernetinių nusikaltimų. Australijos konkurencijos ir vartotojų komisija (ACCC) gali skirti iki 50 mln. Australijos dolerių dydžio baudas verslams, kurie nevykdo savo kovos su sukčiavimu prevencijos įsipareigojimų. Galimas kompensacijų išmokėjimas nusikaltimų aukoms taip pat skatina sektorius daugiau investuoti į finansinio sukčiavimo aptikimą ir prevenciją.

Kovojant su finansiniu sukčiavimu, Australijos bankai, be kita ko, nuo 2025 m. liepos mėn. taiko gavėjo patvirtinimo technologiją, panašią į dabar taikomą ES, ypač atliekant pirmą mokėjimą tam tikram gavėjui. Taip pat kai kurie bankai taiko biometriją (veido atpažinimą) naujiems klientams, atidarantiems sąskaitas, taip siekiant išvengti sukčiavimo su tapatybe. Bankai realiu laiku keičiasi duomenimis, susijusiais su įtariamais finansiniais sukčiais. Taip pat veikia kliento kontroliuojama saugumo sistema (angl. *SafeBlock*), leidžianti klientui iš karto blokuoti skaitmeninį mokėjimą, pinigų pervedimą ar išėmimą iš bankomato, jei įtariama sukčių veikla. Kai kurie bankai pereina nuo SMS komunikacijos prie saugių programėlių.

Pagal 2025 m. vasario mėn. priimtą Australijos Finansinio sukčiavimo prevencijos gairių įstatymą, jei reguliuojamas subjektas neįvykdė savo įsipareigojimų pagal minėtą įstatymą ir dėl to klientas patyrė finansinių nuostolių, klientas iš reguliuojamo subjekto gali atgauti pinigus. Kol kas įstatymas taikomas trimis sektoriams (bankams, telekomunikacijų paslaugoms ir skaitmeninėms platformoms), tačiau ilgainiui jo aprėptis gali išsiplėsti. Įstatyme nustatyta aiški tvarka, kaip pranešti apie finansinio sukčiavimo atvejį arba reguliuojamam subjektui pateikti skundą. Pirmiausia reikia kreiptis į atitinkamą verslo įmonę, kurioje turės veikti skaidri vidaus ginčų sprendimo procedūra. Jei su finansiniu sukčiavimu susiję keletas verslo įmonių, klientas gali kreiptis į bet kurią iš jų, o tada su tuo susijusios įmonės turės bendradarbiauti tarpusavyje sprendžiant ginčą. Jei verslo įmonė ar įmonės nustato, kad neįvykdė savo įsipareigojimų ir dėl to klientas patyrė nuostolių, iš jų bus tikimasi kompensacijos klientui dar pagal vidaus ginčų sprendimo procedūrą. Jei ginčas patenkinamai neišsprendžiamas, klientas galės kreiptis į išorės ginčų sprendimo instituciją. Australijos finansinių skundų valdyba (AFCA) išorės ginčų sprendimo instituciją kol kas yra numaciusi trimis minėtiems sektoriams. AFCA nustatys kiekvienos verslo įmonės veiksmus ir skirs kompensaciją, atsižvelgdama proporcingai į kiekvienos įmonės atsakomybę. Klientai taip pat galės kreiptis į teismus, jei verslo įmonės neįvykdys savo įsipareigojimų. Į teismą galės kreiptis ir reguliuotojas klientų vardu ir jiems sutikus. Priešingai nei JK modelyje, klientams teks atsakomybė už patirtus neatgaunamus nuostolius, nebent prie to kažkaip bus prisidėjęs reguliuojamas subjektas. Taigi klientai bus skatinami būti budrūs ir saugotis sukčių⁷.

Austrija

Austrija taiko įvairias teises ir prevencines priemones, siekiant kovoti su finansiniu sukčiavimu, nukreiptu prieš gyventojus. Austrijos Baudžiamasis kodeksas (BK)⁸ apibrėžia sukčiavimo ir sunkaus sukčiavimo nusikaltimą. BK 146 str. nustato, jog tas, kuris apgaulės būdu suklaidindamas kitą asmenį dėl esminių faktų, paskatina jį atlikti, toleruoti ar neatlikti veiksmo, dėl kurio kyla finansinė ar kita materialinė žala jam ar trečiajam asmeniui, ir kuris siekia neteisėtos naudos sau ar trečiajam asmeniui, baudžiamas laisvės atėmimu iki 6 mėn. arba pinigine bauda.

⁷ *Combatting Scams in Australia and the United Kingdom*: <https://www.klgates.com/Combatting-Scams-in-Australia-and-the-United-Kingdom-2-19-2025>; *Scams Prevention Framework Bill 2025*: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7275

⁸ *Strafgesetzbuch – StGB*:

<https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296>

Sunkaus sukčiavimo atveju, kai žala viršija 300 tūkst. eurų, baudžiama laisvės atėmimu nuo 1 iki 10 metų. Įstatymai specialiai numato sunkesnę atsakomybę už sukčiavimą, naudojant netikrus ar suklastotus teisinius dokumentus, netikras, suklastotas ar neteisėtai pritaikytas negrynųjų pinigų mokėjimo priemones, sužinotus negrynųjų pinigų mokėjimo priemonės duomenis ar kitas suklastotas priemones.

Austrijos finansų rinkos priežiūros tarnyba⁹ aktyviai skelbia išpėjimus apie abejotinus (nelicencijuotus) finansinių paslaugų teikėjus, ypač tuos, kurie veikia iš užsienio ir kuriems ji negali taikyti administracinių priemonių. Be to, Federalinė finansų ministerija turi specialias tarnybas, skirtas kovai su sukčiavimu, kurių užduotis – ginti Austrijos ir ES finansinius interesus, vartotojų apsaugą ir sąžiningos ekonomikos palaikymą.

Kalbant apie bankų klientų apsaugą, pažymėtina, jog už komercinių bankų veiklos priežiūrą yra atsakingas Austrijos nacionalinis bankas¹⁰ kaip centrinis šalies (euro sistemos) bankas. Vis dėlto konkrečias priemones dėl bankų klientų apsaugos nuo sukčių įgyvendina atskiri komerciniai bankai. Šios priemonės gali šiek tiek skirtis, priklausomai nuo konkretaus banko, tačiau galioja kelios taisyklės, kurios taikomos (gali būti taikomos) visuotinai, pavyzdžiui:

- daugiapakopis autentifikavimas, kuris naudojamas prisijungimui mokėjimų patvirtinimui (pavyzdžiui, mobiliojoje programėlėje, SMS kodu ar biometriniais duomenimis);
- mokėjimų stebėjimas. Bankai naudoja sudėtingas sistemas, kurios stebi įtartinus sandorius (pavyzdžiui, neįprastai dideles sumas, mokėjimus į didelės rizikos šalis ar sąskaitas ar neįprastas kliento operacijas). Kilus įtarimui, bankas gali laikinai sustabdyti operaciją ir susisiekti su klientu patvirtinimui;
- klientų informavimas. Bankai nuolat siunčia perspėjimus apie naujas sukčiavimo schemas (*phishingą*, investicines apgavystes, socialinę inžineriją) ir primena apie saugumo taisykles (pavyzdžiui, kad bankas niekada neprašo atskleisti PIN kodų ar prisijungimo duomenų per SMS ar el. pašta);
- sąskaitos savininko vardo (pavadinimo) ir sąskaitos numerio sutapties tikrinimas.

Jei asmuo tapo sukčių auka, jis turi nedelsiant kreiptis į banką. Jei mokėjimas dar neįvykdytas (pavyzdžiui, laukia patvirtinimo), bankas gali jį sustabdyti. Tačiau jei lėšos jau pervestos, jų susigrąžinimas priklauso nuo situacijos – kartais įmanoma inicijuoti lėšų grąžinimo procedūrą (angl. *chargeback*), ypač jei tai buvo kreditinės kortelės operacija.

Žemiau pateikiamos kelios konkrečių bankų taikomos priemonės didžiausiuose šalyje veikiančiuose bankuose *UniCredit Bank Austria*¹¹, *Erste Bank Austria*¹², *Raiffeisen Bank Austria*¹³:

Bankas gali sustabdyti įtartiną mokėjimą, jei jis dar neįvykdytas. Pavyzdžiui, buvo sustabdytas 4500 eurų mokėjimas į Turkiją, kai klientė buvo įtikinta pervesti pinigus tariamam gydytojui.

Bankas susisieks telefonu ir raštu, prašydamas paaiškinti mokėjimo aplinkybes. Jei klientas nesupranta, kad tapo sukčių auka, bankas gali įtraukti teisėsaugą, padedant klientui suvokti situaciją ir inicijuoti lėšų grąžinimą.

Bankas informuoja apie romantinį, investicinį, telefoninį ir *phishingo* tipo sukčiavimą.

Danija

Danija taiko gana stiprų teisinių ir prevencinių priemonių derinį kovojant su finansiniu sukčiavimu, ypač nukreiptu prieš gyventojus. Danijos Baudžiamasis kodeksas¹⁴ numato atsakomybę

⁹ Financial Market Authority Austria: <https://www.fma.gv.at/en/>

¹⁰ Oesterreichische Nationalbank: <https://www.oenb.at/finanzmarkt/bankenaufsicht/organisation-bankenaufsicht-oesterreich.html>

¹¹ UniCredit Bank Austria: <https://www.bankaustria.at/en/index.jsp>

¹² Erste Bank Austria: <https://www.sparkasse.at/erstebank-en/about-us>

¹³ Raiffeisen Bank Austria: <https://www.raiffeisen.at/de/privatkunden.html>

¹⁴ Straffeloven: <https://www.retsinformation.dk/eli/ta/2021/1851>

už sukčiavimą, kuris bendrąja prasme apibrėžiamas kaip apgaulės būdu įgyto turto pasisavinimas ar neteisėtos naudos gavimas. Bausmės už sukčiavimą priklauso nuo žalos dydžio ir nusikaltimo sudėtingumo (nuo piniginių baudų iki laisvės atėmimo). Už sunkius ir organizuotus sukčiavimo atvejus, susijusius su didelėmis sumomis ar viešaisiais finansais, skiriamos griežtos bausmės.

Danijos Finansų priežiūros institucija (dan. *Finanstilsynet*)¹⁵ nuolat prižiūri finansų sektorių, užtikrindama, kad įstaigos, dirbančios Danijos rinkoje, laikytųsi taisyklių, įskaitant pinigų plovimo prevenciją ir vartotojų apsaugos reikalavimus. *Finanstilsynet* yra įgaliota skirti dideles baudas finansų įstaigoms, kurios nesugeba užtikrinti pakankamos kovos su pinigų plovimu kontrolės, kas netiesiogiai apsunkina sukčiams galimybes pasinaudoti sistema.

Kalbant apie bankų klientų apsaugą nuo sukčiavimo, pažymėtina, jog Danijos bankai nepriklauso euro sistemai, tačiau šalyje įgyvendinamos visos efektyviausios klientų apsaugos priemonės, kaip ir euro zonos bankuose. Remiantis Danijos nacionalinio banko¹⁶ duomenimis, skaitmeniniai mokėjimo sprendimai sudaro daugiau nei 92 proc. visų Danijos piliečių mokėjimų vertės. Tai daugiausia lemia skaitmeninių mokėjimo sprendimų teikiamas patogumas ir nuolatinė Danijos visuomenės skaitmenizacija. Skaitmeninių mokėjimų infrastruktūra daugeliu atvejų yra saugi ir efektyvi.

Vis dėlto sukčiavimo modelių tendencijos rodo, kad nusikaltėliai nuolat prisitaiko prie naujų technologijų ir griežtėjančios teisinės aplinkos. Todėl svarbu, kad skaitmeninėje erdvėje visuomenė ir įmonės žinotų, jog joms vis labiau gresia pavojus būti apgautoms autorizuojant mokėjimus.

Kalbant konkrečiau, pažymėtina, jog Danijos bankai taiko griežtas saugumo ir prevencijos priemones, kad apsaugotų klientus nuo finansinio sukčiavimo. Pagrindinės taikomos priemonės:

- daugiafaktorinis autentifikavimas. Prisijungiant prie banko ar atliekant mokėjimus klientai privalo patvirtinti tapatybę naudodami *NemID* arba *MitID* – tai nacionalinės skaitmeninės tapatybės sistemos, kurios užtikrina aukštą saugumo lygį;
- automatinis sukčiavimo aptikimas. Bankai naudoja dirbtinį intelektą (DI) ir elgsenos analizę, kad aptiktų neįprastus mokėjimus ar prisijungimą;
- SMS ir el. pašto įspėjimai. Klientai informuojami apie įtartinas operacijas, kad galėtų greitai reaguoti;
- saugumo kampanijos. Danijos bankų asociacija (*Finans Danmark*)¹⁷ vykdo informacines kampanijas apie investicinius, romantinius ir techninio palaikymo sukčiavimo tipus.

Įvykus sukčiavimo atvejui, Danijos bankai rekomenduoja kuo greičiau pranešti apie įtartiną veiklą, kadangi kai kuriais atvejais mokėjimas dar gali būti sustabdytas.

Svarbu pažymėti, jog galioja tam tikros taisyklės ir apribojimai dėl lėšų susigrąžinimo. Jei sukčiavimas įvyko dėl techninių banko saugumo spragų, klientui gali būti kompensuojama visa suma. Tačiau jei klientas pats patvirtino mokėjimą, kompensacija gali būti ribota.

Bankų veiklą ir saugumo standartus prižiūri Finansų priežiūros tarnyba¹⁸. Taip pat yra nacionalinės kibernetinio saugumo institucijos, tokios kaip CERT-DK¹⁹, padedančios bankams reaguoti į kibernetines grėsmes.

Pavyzdžiui, *Danske Bank* savo oficialioje informacijoje skelbia, jog klientų apsaugos srityje visada teikia pirmenybę etikai, o ne pelnui bei konstruktyviai bendradarbiauja su visomis suinteresuotomis šalimis, įskaitant valdžios institucijas. Bankas įgyvendina vadinamąjį trijų gynybos linijų modelį, kuris padeda užtikrinti aiškiai apibrėžtų vaidmenų ir atsakomybės nustatymą²⁰.

¹⁵ *Finanstilsynet*: <https://www.finanstilsynet.dk/>

¹⁶ *Danmarks Nationalbank. Digital payment fraud in Denmark*: <https://www.nationalbanken.dk/en/news-and-knowledge/publications-and-speeches/analysis/2024/digital-payment-fraud-in-denmark>

¹⁷ *Finans Danmark*: <https://finansdanmark.dk/>

¹⁸ *Finanstilsynet*: <https://www.dfsa.dk/>

¹⁹ *CERT-DK*: <https://www.cert.dk/>

²⁰ *Danske Bank. Fighting Financial Crime*: <https://danskebank.com/about-us/corporate-governance/compliance/fighting-financial-crime>

Ispanija

Finansinis sukčiavimas, ypač naudojant technologijas, laikomas sukčiavimu sunkinančiomis aplinkybėmis. Už sukčiavimą gresia laisvės atėmimo bausmės nuo 6 mėn. iki 3 metų, tačiau jei sukčiavimo mastai ypač dideli arba tai susiję su daugeliu nukentėjusiųjų, už tai gali būti baudžiama laisvės atėmimu iki 8 metų. Kartu su laisvės atėmimu skiriamos piniginės baudos, kurių dydis proporcingas iš sukčiavimo gautai naudai. Taip pat taikoma civilinė atsakomybė už padarytą žalą. Gali būti taikomas ir draudimas užsiimti tam tikra veikla.

Keletas Ispanijos bankų ėmėsi bendros iniciatyvos, pavadintos *FraudDefense*. Projektas leidžia lengviau dalytis informacija apie finansinio sukčiavimo būdus ir taikomomis kovos su sukčiavimu priemonėmis. Daugelis bankų analizuoja klientų elgesio modelius, pavyzdžiui, naršymą, kad nustatytų ir užkirstų kelią finansiniams nusikaltimams. Tai gana veiksmingos priemonės nuo sąskaitų perėmimo. *Iberpay*, teikiantis mokėjimų infrastruktūros paslaugas, įdiegė DI ir mašininį mokymąsi į *Payguard* paslaugą. Ši technologija analizuoja pervedimų modelius ir leidžia pastebėti neįprastus veiksmus.

2018 m. lapkričio 23 d. karališkojo įstatymo-dekreto dėl mokėjimo paslaugų ir kitų skubių priemonių finansų klausimais²¹ 43–46 straipsniuose nustatyta, kad klientui gali tekti atsakomybė, sudaranti daugiausia iki 50 eurų, už nuostolius, atsiradusius dėl neautorizuoto pinigų pervedimo, susijusius su pamesta, pavogta arba trečiosios šalies kitaip pasisavinta mokėjimo priemone. Klientui tenka visa atsakomybė už patirtus nuostolius, susijusius su neautorizuotu mokėjimu, jei klientas sukčiavo arba pažeidė – tyčia arba dėl didelio neatsargumo – savo įsipareigojimus.

Šalyje iš esmės laikomasi nuostatos, kad bankai turėtų kompensuoti klientams, tapusiems finansinio sukčiavimo aukomis, jei taip neatsitiko dėl kliento „didelio neatsargumo“ ir apie tai buvo nedelsiant pranešta. Tam, kad pinigų pervedimas būtų pripažintas neautorizuotu, klientas dėl jo neturi būti davęs aiškaus savo sutikimo. Norėdamas išvengti kompensacijos mokėjimo, pats bankas turi įrodyti, kad klientas sukčiavo arba buvo neatsargus²².

Pagal 2025 m. balandžio 9 d. Aukščiausiojo Teismo priimtą nutartį atsiranda precedentas, kad bankai privalo prisiimti atsakomybę už klientų neautorizuotus mokėjimus, atsiradusius dėl kliento tapatybės vagystės, net jei buvo pasinaudota kliento asmens duomenimis (slaptažodžiais), pavyzdžiui, tais atvejais, kai mokėjimai yra daugkartiniai, atliekami neįprastu laiku ir jų sumos didelės. Kartu ši nutartis reiškia, kad bankai turi stiprinti savo apsaugos sistemas, ypač kovojant su rafinuotu skaitmeniniu sukčiavimu²³.

Jungtinė Karalystė

Remiantis rinkos dalyvių pranešimais, 2024 m. finansiniai sukčiai iš šalies gyventojų išviliojo apie 1,2 mlrd. svarų sterlingų. Kaip teigiama, patirta emocinė žala ir tyrimų išlaidos šią sumą dvigubina²⁴.

Finansiniams sukčiams gali būti taikomos bausmės iki 10 metų laisvės atėmimo (lengvesniais atvejais – iki 12 mėn.), taip pat didelės piniginės baudos, kompensacijos nusikaltimų aukoms ir tyrimo išlaidų atlyginimas bei turto įšaldymas. Taip pat nukenčia nuteistų sukčių reputacija, kas gali neleisti ateityje jiems užimti tam tikrų pareigų, ypač finansų sektoriuje. Nusikaltimų aukos taip pat gali pateikti civilinius ieškinius žalai atlyginti.

²¹ *Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera:* <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16036>

²² *Jurisprudencia del Phishing Bancario: el Tribunal Supremo se pronuncia a favor del estafado:* <https://asobanabogados.com/blog/jurisprudencia-del-phishing-bancario/>

²³ *Banks' liability for digital fraud: new ruling by the Tribunal Supremo:* <https://www.abogacia.es/en/publicaciones/blogs/blog-de-derecho-de-los-los-consumidores/responsabilidad-de-los-bancos-ante-fraudes-digitales-nueva-sentencia-del-tribunal-supremo/>

²⁴ *Banking fraud:* <https://researchbriefings.files.parliament.uk/documents/CBP-8545/CBP-8545.pdf>

Šiuo metu bankai gali užlaikyti įtartinus mokėjimus iki 72 val. Per tą laiką bankas nusprendžia, ar mokėjimas teisėtas ir ar jį įvykdyti, ar atmesti. Anksčiau šis terminas buvo iki kitos darbo dienos pabaigos. Bankai taip pat gali tirti neįprastą elgesį atliekant mokėjimus ir susisiekti su klientais dėl neįprastų pervedimų patvirtinimo. Bankai taip pat naudoja duomenų kodavimą, automatinį atsijungimą dėl prieigos nenaudojimo, deaktivuoja interneto prieigas, jei kelis kartus surenkamas neteisingas slaptažodis. Finansinio elgesio valdyba (angl. *Financial Conduct Authority*) aptinka sukčių svetaines ir informuoja vartotojus. Bankai susisiečia su klientais automatinėmis sistemomis, telefonu, tekstiniais pranešimais arba programėlėmis, jei nori patvirtinti kliento tapatybę. Kai kurie bankai reikalauja, kad klientas patikrintų mokėjimo rekvizitus, įskaitant banko pranešimų perskaitymą. Kai kurie bankai leidžia klientams išdėlioti mokėjimus laike, nustatant vėlesnę datą, taip leidžiant klientui apsigalvoti²⁵.

Nuo 2024 m. spalio 7 d. JK galioja Kompensacijos schema, kuri taikoma mokėjimo paslaugų teikėjams. Schema parengė Mokėjimų sistemų reguliuotojas (*Payment Systems Regulator*). Schema taikoma autorizuotiems mokėjimams, atliktiems nuo minėtos datos. Pagal Kompensacijos schema, mokėjimo paslaugų teikėjai privalo kompensuoti klientams, kurie tapo autorizotų mokėjimų finansiniams sukčiams aukomis (*Authorised Push Payment Fraud Reimbursement Scheme*). Kompensacijos schema iš esmės taikoma nuo finansinių sukčių nukentėjusiems fiziniams asmenims, labdaros organizacijoms ir smulkiesiems verslams. Kompensacijos išlaidas po lygiai (50/50) dalijasi kliento mokėjimo paslaugų teikėjas ir tas paslaugų teikėjas, kuriuo pasinaudojo sukčius. Tačiau mokėjimo paslaugų teikėjas neprivalo kompensuoti klientui, jei tai atsitiko dėl jo didelio neatsargumo, nesilaikyta vadinamojo kliento atsargumo standarto (*Consumer Standard of Caution*), arba jei klientas pats buvo susijęs su finansiniu sukčiavimu.

Kliento atsargumo standartas, be kita, ko reiškia, kad klientas turi reaguoti į mokėjimo paslaugų teikėjo arba policijos įspėjimus, laiku pranešti apie įvykį (vėliausiai per 13 mėn., kaip ES), teikti informaciją mokėjimo paslaugų teikėjui ir pranešti policijai (tai gali padaryti arba jis pats, arba mokėjimo paslaugų teikėjas).

Jei klientas yra „pažeidžiamas“, jam netaikomas kliento atsargumo standartas. Pažeidžiamas klientas yra tas, kuris dėl tam tikrų asmeninių aplinkybių yra ypač pažeidžiamas. Tai gali būti: sveikatos būklė ar ligos, traumuojantys gyvenimo įvykiai, gebėjimas pakelti finansinį ar emocinį šoką, žinių kliūtys (pavyzdžiui, nepakankamas kalbos mokėjimas arba menkas skaitmeninis ar finansinis raštingumas).

Didžiausia mokėjimo paslaugų teikėjo išmokamos kompensacijos suma nustatyta 85 tūkst. svarų. Minimali kompensacijos riba nenustatyta. Mokėjimų paslaugų reguliuotojas iš pradžių siūlė, kad didžiausio dydžio kompensacijos suma siektų 415 tūkst. svarų, tačiau buvo atsižvelgta į rinkos dalyvių pageidavimus. Į tokio dydžio (85 tūkst. svarų) kompensacijos sumos ribą patenka daugiau nei 99 proc. visų sukčiavimo atvejų, o kompensuojama apie 90 proc. pretenzijų. Taip pat numatyta, kad mokėjimo paslaugų teikėjai nukentėjusiam klientui, išskyrus pažeidžiamus klientus, gali taikyti iki 100 svarų papildomą atskaitymą, tačiau ne visi paslaugų teikėjai taip daro. Manoma, kad šis papildomas atskaitymas, be kita ko, turėtų skatinti kliento atsargumą. Jei siūloma kompensacijos suma nukentėjusio kliento netenkina arba jo patirta žala yra didesnė, jis gali kreiptis į Finansų kontrolieriaus tarnybą, kuri gali nuspręsti, kad kompensacija galėtų siekti iki 430 tūkst. svarų.

JK Kompensacijos schema taikoma mokėjimo paslaugų teikėjams pagal vadinamąją Greitesnių mokėjimų schema (*Faster Payments Scheme*, FPS) arba pagal automatizuotą mokėjimų sistemą (*Clearing House Automated Payment System*, CHAPS) ir susijusi su vadinamosiomis atitinkančiomis sąskaitomis (*Relevant Accounts*). Tai netaikoma tarptautiniams mokėjimams, mokėjimams neteisėtiems tikslams, taip pat ginčytiniams mokėjimams, kai, pavyzdžiui, klientas nepatenkintas užsakytų prekių kokybe.

Greitesnių mokėjimų schema yra viena iš aštuonių JK Iždo pripažintų mokėjimų sistemų. Beveik visi mokėjimai internetu ir telefonu vyksta naudojantis Greitesnių mokėjimų schema.

²⁵ *Understanding the New UK Banking Regulations on Fraud – Are you and the banks prepared for October 7?*: <https://www.comsuregroup.com/news/understanding-the-new-uk-banking-regulations-on-fraud-are-you-and-the-banks-prepared-for-october-7/>

Atitinkama sąskaita yra tokia, kuri suteikiama paslaugos naudotojui, ji turi būti JK ir joje galima atlikti ir gauti mokėjimus naudojantis Greitesnių mokėjimų schema. Prie atitinkamų sąskaitų nepriskiriamos kredito unijų, savivaldybių bankų ir nacionalinių taupomųjų bankų sąskaitos.

Nukentėjęs klientas pretenziją privalo pareikšti ne vėliau nei per 13 mėn. nuo įvykio. Pretenzija turi būti patenkinta per 5–35 darbo dienas. 35 darbo dienų terminas taikomas, jei mokėjimo paslaugų teikėjui reikia atlikti išsamų įvykio aplinkybių tyrimą.

Nors buvo baiminamasi nukentėjusiųjų antplūdžio ir kompensacijų mastų, per 2024 m. paskutinį ketvirtį, kai galioja Kompensacijos schema, buvo patenkinta apie 86 proc. nukentėjusių klientų pretenzijų, finansine išraiška tai sudarė apie 27 mln. svarų, o 84 proc. pretenzijų išspręsta per 5 darbo dienas. Tik 2 proc. pretenzijų buvo atmestos dėl nesilaikyto kliento atsargumo standarto. Finansinio sukčiavimo mastas Anglijoje ir Velse toks, kad tai sudaro daugiau nei 40 proc. visų registruotų nusikaltimų, tačiau tam tirti skiriama tik 1 proc. policijos išteklių²⁶.

Remiantis tikslesniais Mokėjimų sistemų reguliuotojo duomenimis, per 2024 m. IV ketv. patenkinta 87 proc. pretenzijų (27,6 mln. svarų), 2025 I ketv. – 88 proc. (38,4 mln. svarų), 2025 m. II ketv. – 88 proc. (45,7 mln. svarų). Nuo 82 iki 88 proc. kompensacijų išmokėtos per 5 darbo dienas. Atmesta nuo 2 iki 4 proc. pretenzijų (atitinkamai pagal metų ketvirčius – 1,1 tūkst., 1,7 tūkst., 2,7 tūkst.). Bendras pretenzijų skaičius: 2024 m. IV ketv. – 46 tūkst., 2025 I ketv. – 62,6 tūkst., 2025 m. II ketv. – 72 tūkst.²⁷.

Nyderlandai

Bausmės už finansinį sukčiavimą gali būti laisvės atėmimas iki 4 metų arba piniginė bauda iki 90 tūkst. eurų, arba pritaikytos abi šios bausmės. Bausmės priklauso nuo sukčiavimo pobūdžio ir masto. Nusikalstama veika sunkinančiomis aplinkybėmis (pavyzdžiui, nusikalstamo susivienijimo) gali būti baudžiama įkalinimu iki 6 metų. Taip pat gali būti taikoma civilinė atsakomybė.

Nyderlanduose bankai naudoja DI ir pažangias sukčiavimo aptikimo sistemas, kad proaktyviai reaguotų į galimo finansinio sukčiavimo atvejus. Klientai raginami naudoti saugias patvirtinimo programas ir nustatyti išlaidų limitus. Bankai bendradarbiauja su policija, prokuratūra ir telekomunikacijų paslaugų teikėjais, ypač dėl internetinio sukčiavimo atvejų. Bendradarbiaujant su telekomunikacijų įmonėmis, geriau užtikrinama vadinamojo bankų apsimetėlių sukčiavimo (angl. *bank helpdesk scams*) prevencija. Taip pat daug dėmesio skiriama visuomenės informavimui.

2020 m. pabaigoje keturi didžiausi šalies bankai nusprendė dėl savanoriškos kompensacijos schemos asmenims, nukentėjusiems nuo bankų apsimetėlių sukčiavimo. Bankai šį reiškinį gali šiek tiek kontroliuoti, pavyzdžiui, aiškindami klientams, kaip jie kontaktuoja ir komunikuoja su klientais.

Kompensacija nėra automatiška ir bankai atsižvelgia į konkrečius faktus bei aplinkybes. Per maždaug metus, iki 2021 m. pabaigos, nuostoliai dėl bankų apsimetėlių sukčiavimo išaugo nuo 26,2 mln. iki 47,6 mln. eurų, ir toks sukčiavimas išaugo nuo 53 proc. iki 75 proc. visų finansinio sukčiavimo atvejų. Dar įdomiau tai, kad sukčiavimo problema, atrodo, susijusi su kompensacijos suma. 2021 m., didžiausio sukčių aktyvumo metais, 92 proc. bankų apsimetėlių sukčiavimo atvejų baigėsi kompensacijų išmokėjimu. 2023 m., kai bankų apsimetėlių sukčiavimas gerokai sumažėjo, bankai kompensavo 69 proc. patirtų nuostolių. 2024 m. kompensuota maždaug pusė visų bankų apsimetėlių sukčiavimo nuostolių. Vis dėlto yra ir tam tikra pačių klientų atsakomybė – 50 eurų

²⁶ APP fraud reimbursement protections: <https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/>; Authorised Push Payment Fraud Reimbursement: <https://www.ukfinance.org.uk/authorised-push-payment-fraud-reimbursement/>; The U.K.'s Authorised Push Payment (APP) Fraud Reimbursement Scheme: <https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/the-uks-authorised-push-payment-app-fraud-reimbursement-scheme>; Six Months of the UK's APP Scam Reimbursement: Lessons for Banks: <https://www.threatmark.com/six-months-of-psr-scam-reimbursement/>

²⁷ APP scams reimbursement dashboard for Q2 2025: <https://www.psr.org.uk/information-for-consumers/app-scams-reimbursement-dashboard/>

padengia klientas, jei tai nesusiję su jo „dideliu neatsargumu“. Klientų autorizuotų mokėjimų, atitekusių finansiniams sukčiams, bankai neprivalo kompensuoti²⁸.

Prancūzija

Už finansinį sukčiavimą baudžiama laisvės atėmimo bausmėmis ir piniginėmis baudomis. Už bandymą sukčiauti taip pat baudžiama, ypač organizuoto susivienijimo atveju. Bausmės už finansinį sukčiavimą: iki 5 metų įkalinimo ir 375 tūkst. eurų bauda. Sunkinančiomis aplinkybėmis (pavyzdžiui, kai auka yra pažeidžiamas asmuo (dėl amžiaus ar sveikatos), kai apsimetama valstybės pareigūnu ar tarnautoju, arba kai nukenčia viešoji institucija): iki 7 metų įkalinimo ir 750 tūkst. eurų bauda. Organizuotas susivienijimas: iki 10 metų įkalinimo ir 1 mln. eurų bauda. Gali būti skiriamos papildomos bausmės: draudimas užsiimti tam tikra veikla; sukčiavimo būdu įgytų lėšų arba panaudotų priemonių konfiskavimas; nuosprendžio pavišinimas; pašalinimas iš tam tikrų rinkų. Juridiniams asmenimis gali būti skiriamos iki 5 kartų didesnės piniginės baudos ir jie gali būti uždaryti (išformuoti)²⁹.

Bankai daug investuoja į kibernetinį saugumą ir vykdo įvairias iniciatyvas klientų budrumui skatinti. Atlikti pokyčiai visose programėlėse visoje mokėjimo procedūroje. Programėlėse matoma, be kita ko, pervedimo suma, gavėjas, pranešimas, kad tai yra mokėjimas, taip pat yra galimybė patvirtinti arba atšaukti mokėjimą. 2025 m. lapkričio mėn. priimtas teisės aktas dėl finansinio sukčiavimo, susijusio su elektroniniais mokėjimų būdais, pavyzdžiui, tiesioginiu debetu. Pagal šį įstatymą, sukuriama nacionalinis registras įtartinų sąskaitų, kurios pažymėtos kaip keliančios sukčiavimo riziką. Į registrą pateks sąskaitos, kurias nustatė bankų vidaus kontrolės sistemos. Registrą tvarkys Prancūzijos bankas, o jį išlaikys mokėjimų paslaugų rinkos dalyviai.

Bankai ragina telekomunikacijų operatorius vykdyti reguliavimo įsipareigojimus. Kai kurie skambučiai operatorių nuožiūra gali būti blokuojami. Sukčiavimo prevencijoje taip pat turėtų dalyvauti socialinė žiniasklaida ir el. pašto paslaugų teikėjai, ypač investavimo sukčiavimo prevencijoje. Būtent per socialinę žiniasklaidą reklamuojamos apgaulingos investicijos ir nukreipiami į sukčių svetaines. Klientams taip pat rekomenduojama bent kartą per savaitę prisijungti prie savo sąskaitos ir patikrinti, ar joje nėra nieko neįprasto.

Už neautorizuotą mokėjimą, jei bankas nereikalavo sustiprinto kliento patvirtinimo, klientui turi būti kompensuojama. Jei buvo įdiegtas sustiprintas kliento patvirtinimas (pavyzdžiui, biometrija), nukentėjusysis vis tiek gali kreiptis į banką dėl kompensacijos, o kliento pretenzija išnagrinėjama per laikotarpį iki 30 dienų³⁰.

Iš esmės bankai privalo kompensuoti klientams už neautorizuotus pinigų pervedimus, jei klientas apie tai praneša ne vėliau kaip per 13 mėn. ir jei tai nebuvo susiję su kliento „dideliu neatsargumu“. Šios nuostatos į Prancūzijos teisę perkeltos iš ES Pirmosios mokėjimo paslaugų

²⁸ *Is the EU taking the right approach to APP (authorized push payment) fraud?:*

[https://www.cer.eu/sites/default/files/Is the EU taking the right approach to A.pdf](https://www.cer.eu/sites/default/files/Is%20the%20EU%20taking%20the%20right%20approach%20to%20A.pdf); *Criteria for awarding compensation for loss arising from bank help desk scams:* <https://www.nvb.nl/media/5661/criteria-for-awarding-compensation-for-loss-arising-from-bank-help-desk-scams-spoofing-june-2nd-2021.pdf>; *Bank helpdesk fraud drops 30% in Netherlands; losses fall to €23 million:* <https://nltimes.nl/2025/04/19/bank-helpdesk-fraud-drops-30-netherlands-losses-fall-eu23-million>

²⁹ *La définition de l'escroquerie en droit pénal expliquée simplement:* <https://goldwin-avocats.com/fr/definition-escroquerie-en-droit-penal/>

³⁰ *Que font les banques françaises pour lutter contre la fraude aux moyens de paiement?:*

<https://www.fbf.fr/fr/que-font-les-banques-francaises-pour-lutter-contre-la-fraude-aux-moyens-de-paiement%E2%80%AF/>; *Opérations bancaires à distance: comment vous protéger des fraudes?:* <https://www.economie.gouv.fr/particuliers/mes-droits-conso/eviter-les-arnaques/operations-bancaires-distance-comment-vous-protger-des-fraudes>; *Loi du 6 novembre 2025 visant à renforcer la lutte contre la fraude bancaire:* <https://www.vie-publique.fr/loi/300664-loi-du-6-novembre-2025-renforcer-la-lutte-contre-la-fraude-bancaire>; *Vers une uniformisation des pratiques et un renforcement de la sécurité et de la lutte contre la fraude bancaire:* <https://www.economie.gouv.fr/daj/vers-une-uniformisation-des-pratiques-et-un-renforcement-de-la-securite-et-de-la-lutte-contre-la-fraude-bancaire>

direktyvos 2007/64/EB. Pagal Prancūzijos Monetarinio ir finansų kodekso nuostatas, reikalaujama, kad kompensacija klientui būtų išmokama nedelsiant. Už delsimą taikomos nuobaudos, t. y. palūkanos, pavyzdžiui, 15 punktų už 30 pradelstų dienų³¹.

Suomija

Suomija turi tvirtą sistemą, skirtą kovai su finansiniu sukčiavimu. Šis atsakas apima griežtą baudžiamąją teisę ir aktyvų finansų priežiūros institucijos darbą.

Suomijos Baudžiamasis kodeksas³² numato baudžiamąją atsakomybę už sukčiavimą. Iš esmės sukčiavimas apibrėžiamas kaip veiksmas, kai asmuo, apgaule suklaidindamas kitą asmenį, paskatina jį atlikti veiksmą, dėl kurio patiriama finansinė žala. Numatytos griežtesnės bausmės už sukčiavimo formas sunkinančiomis aplinkybėmis, atsižvelgiant į sukčiavimo būdą, žalos mastą ar nusikaltimo organizuotumą. Už sunkius finansinius nusikaltimus gali būti skiriamos gana griežtos laisvės atėmimo bausmės. Jei sukčiavimo veiksmai atliekami įmonės naudai arba dėl nepakankamos priežiūros (pavyzdžiui, neįdiegus tinkamų sukčiavimo prevencijos priemonių), pačiai įmonei gali būti skiriamos didelės baudos.

Nacionalinis tyrimų biuras (suom. *Keskusrikospoliisi*, KRP)³³ specializuojasi tiriant sunkius finansinius ir ekonominius nusikaltimus, įskaitant didelio masto sukčiavimo schemas. KRP aktyviai bendradarbiauja su bankais ir tarptautinėmis teisėsaugos institucijomis, siekiant sustabdyti tarptautinio sukčiavimo srautus.

Kalbant apie bankų klientų apsaugą nuo sukčiavimo, pažymėtina, jog Suomijos bankai taiko griežtas saugumo ir prevencijos priemones, kad apsaugotų klientus nuo finansinio sukčiavimo. Paminėtini šie pagrindiniai aspektai:

- skaitmeninis tapatybės patvirtinimas – prisijungimui prie bankų naudojamos saugios autentifikavimo sistemos, kurios reikalauja kelių patvirtinimo žingsnių;
- automatinis sukčiavimo aptikimas – bankai naudoja elgsenos analizę ir DI, kad aptiktų neįprastus mokėjimus ar prisijungimą;
- įspėjimai klientams – klientai informuojami apie įtartinas operacijas SMS žinutėmis ar el. paštu;
- informavimo kampanijos – bankai ir Suomijos finansų sektoriaus asociacija (*Finance Finland*, FFI)³⁴ vykdo informacines kampanijas apie investicinius, romantinius ir techninio palaikymo sukčiavimo tipus.

Minėta asociacija yra išplėtojusi didelio masto informacinę kampaniją, kurios metu kuo labiau prieinamu ir suprantamu įvairioms visuomenės grupėms būdu stengiasi pateikti informaciją apie egzistuojančius sukčiavimo būdus, kaip juos atpažinti bei užkirsti jiems kelią. Visa informacija apie kampaniją pateikiama internetinėje svetainėje *Huijaamaton.fi*³⁵.

Pagrindinė valstybinė institucija, koordinuojanti bankų klientų apsaugos priemones ir glaudžiai bendradarbiaujanti su šalyje veikiančiais komerciniais bankais šiuo klausimu yra Suomijos finansų priežiūros tarnyba (FIN-FSA)³⁶.

Įvykus sukčiavimo incidentui, kai kurias atvejais mokėjimai gali būti sustabdyti, tačiau tai priklauso nuo mokėjimo būdo (pavyzdžiui, mokėjimas kredito kortele ir pan.) bei nuo kitų aplinkybių. Be to, jei asmuo nukentėjo dėl techninių spragų banko saugumo sistemoje, jis gali reikalauti kompensacijos.

³¹ *Navigating legal challenges in French civil fraud cases*: <https://perspectives.bclplaw.com/confronting-corruption/navigating-legal-challenges-in-french-civil-fraud-cases-in-depth-analysis/>

³² *Rikoslaki*: <https://www.finlex.fi/fi/lainsaadanto/1889/39-001>

³³ *Keskusrikospoliisi, KRP*: <https://poliisi.fi/en/national-bureau-of-investigation>

³⁴ *Finance Finland – FFI*: <https://www.finanssiala.fi/en/>

³⁵ *Huijaamaton.fi*: <https://www.huijaamaton.fi/en/>

³⁶ *FIN-FSA. Financial Supervisory Authority. Scams*: <https://www.finanssivalvonta.fi/en/consumers/scams/>

Atskiras ir išsamias informacines kampanijas taip pat yra išplėtoję ir Suomijoje veikiantys komerciniai bankai. Pavyzdžiui *Nordea.fi*³⁷ tinklapyje pateikiamos ne tik išsamios instrukcijos, kaip elgtis nukentėjus nuo sukčių, bet ir raginimai padėti savo artimiesiems, kurie gali būti labiau pažeidžiami skaitmeninėje erdvėje.

Bankas nurodo, jog susidūrus su sukčiavimo atveju asmuo nedelsiant turi užblokuoti savo internetinės bankininkystės kodus ir kortelę. Taip pat asmuo gali pateikti skundą dėl kortelės operacijos (kortelės operacijos ginčijimas), kuris turės būti išnagrinėtas. Atskirais atvejais operacija gali būti sustabdyta.

Norint pateikti ginčą, asmuo turi palaukti, kol operacija bus rodoma kaip debetas kortelės operacijose. Kitaip tariant, negalima ginčyti laukiančios (angl. *pending*) operacijos. Operaciją asmuo turi užginčyti ne vėliau kaip per 2 mėn. nuo debeto datos.

Operaciją galima ginčyti, jei:

- sąskaitos išrašė ar kredito kortelės sąskaitoje faktūroje pastebėta pirkimų kortele, pervedimų iš savo kredito sąskaitos ar grynųjų pinigų išėmimo, kurių asmuo neatpažįsta;
- iš kortelės buvo du kartus nuskaičiuota už tą pačią operaciją ir pardavėjas negrąžino dvigubo nuskaitymo iš asmens kortelės;
- asmuo negavo užsakytų prekių ar paslaugų;
- asmuo gavo nekokybiškas prekes;
- kortelės operacija susijusi su susitarimu, kuris nėra privalomas vartotojams pagal vartotojų apsaugos įstatymus³⁸.

Be kita ko, pateikiama informacija, jog nukentėjęs asmuo gali kreiptis į Suomijos paramos nukentėjusiesiems organizaciją (RIKU)³⁹.

Pažymėtina, jog šalyje didelis dėmesys teikiamas būtent sukčiavimo prevencijai ir visuomenės plataus masto informavimui. Tam daug resursų skiria tiek atsakingos valstybės institucijos, tiek ir šalyje veikiantys komerciniai bankai.

Švedija

Švedija yra viena iš valstybių, kurioje finansinis sukčiavimas, ypač skaitmeninėmis priemonėmis, yra didelė problema. Reaguodama į tai, šalis taiko griežtą teisinę bazę ir pažangias prevencijos priemones.

Baudžiamajame kodekse⁴⁰ numatyta atsakomybė už sukčiavimą, kuris apibrėžiamas kaip asmens neteisėtos turtinės naudos siekis sau ar kitiems asmenims, pasitelkiant apgaulę. Numatytos žymiai griežtesnės bausmės už sukčiavimą sunkinančiomis aplinkybėmis – dėl padarytos didelės žalos, apgaulės sudėtingumo ar organizuoto nusikalstamo pobūdžio. Bausmės už sunkius finansinius nusikaltimus gali siekti 6 metus laisvės atėmimo.

Pažymėtina, jog teisės aktai baudžia ir už melagingos arba klaidingos informacijos pateikimą, kuris gali turėti įtakos finansiniam vertinimui, kaip tai matyti iš rezonansinių bankų bylų.

Švedijos finansų priežiūros tarnyba (šved. *Finansinspektionen*)⁴¹ yra atsakinga už finansų rinkos stabilumą ir vartotojų apsaugą. Ji nuolat stebi įmones, kad būtų užtikrintas jų atitikimas pinigų plovimo prevencijos priemonėms ir vartotojų teisių apsaugos reikalavimams. Be kita ko, tarnyba aktyviai skelbia oficialius įspėjimus apie įtartinus ir nelicencijuotus finansų paslaugų teikėjus, kurie veikia Švedijos rinkoje, siekdama apsaugoti investuotojus ir gyventojus.

³⁷ *Nordea.fi*. What to do if you think you have been scammed: <https://www.nordea.fi/en/personal/your-life/security/have-you-been-scammed.html>

³⁸ *Nordea.fi*. How to dispute a transaction: <https://www.nordea.fi/en/personal/our-services/credit-payment-cards/use-cards-safely/card-complaint.html>

³⁹ RIKU: <https://www.riku.fi/en/>

⁴⁰ *Brottsbalken*: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700/

⁴¹ *Finansinspektionen*: <https://www.fi.se/>

Kalbant apie bankų klientų apsaugą nuo sukčiavimo, pažymėtina, jog Švedijos, kaip ir Danijos, bankai nepriklauso euro sistemai, todėl šioje šalyje registruotos asmenų bankų sąskaitos negali būti patikrinamos naująja euro zonos sąskaitos savininko identifikavimo priemone, kurią pradėjo taikyti euro zonos bankai ES. Kita vertus, atsakingos šalies institucijos, glaudžiai bendradarbiaudamos su šalyje veikiančiais komerciniais bankais, taiko virtualią apsaugos ir prevencijos priemonių, siekiant sumažinti bankinio sukčiavimo atvejų pabeigti didinti bankų klientų apsaugą.

Švedijos bankai naudoja daugiasluoksnią apsaugą nuo sukčiavimo, įskaitant privalomą saugią *BankID* sistemą, skirtą apsisaugoti nuo sukčiavimo, sukčiavimo aptikimą realiuoju laiku naudojant DI ir elgsenos biometriją, taip pat kliento nustatytus operacijų limitus ir pavėlintus mokėjimus. Be kita ko, daug dėmesio skiriama darbuotojų mokymui ankstyvo pažeidimų aptikimo srityje bei kibernetiniam saugumui. Bankai taip pat prisiima didesnę savo pačių atsakomybę už neteisėtas operacijas ir įgyvendina griežtesnę operacijų stebėseną, laikydamiesi griežtėjančio ES reglamentavimo (tokio kaip Mokėjimo paslaugų direktyva 2015/2366).

Konkrečios bankų Švedijoje taikomos priemonės:

- *BankID* saugi prisijungimo sistema;
- DI ir elgsenos biometriniai duomenys – bankai naudoja mašininį mokymąsi ir DI įrankius, kad realiuoju laiku analizuotų vartotojų elgesį, aptiktų sukčiavimą signalizuojančius nukrypimus ir prisitaikytų prie naujų sukčiavimo modelių;
- operacijų stebėjimas – bankai naudoja pažangias sistemas, kad stebėtų operacijas, ar nėra įtartinos veiklos, ir įgyvendina griežtesnės operacijų stebėsenos reikalavimus, kad būtų galima aptikti ir užkirsti kelią sukčiavimui.

Su klientais susiję įrankiai ir funkcijos:

- pritaikomi limitai ir pavėlinti mokėjimai – klientai gali nustatyti savo mokėjimų limitus ir prašyti tam tikrų operacijų atidėjimo, taip kompromituodami sukčių darbo schemas;
- antrinis autorizavimas – kai kuriems sandoriams galima nustatyti antro autorizavimo reikalavimą iš patikimo asmens, taip užtikrinant papildomą saugumo lygį ir kt.

Finansinspektionen siekia užtikrinti finansinį stabilumą ir veiksmingą vartotojų apsaugą, prisidėdama prie šių apsaugos priemonių.

Kaip savo oficialioje informacijoje pažymi Švedijos centrinis bankas, bankams tenka didelė atsakomybė už savo klientų saugumą. Pavyzdžiui, bankas gali būti įpareigotas atkurti sąskaitos lėšas, jei vartotojas buvo apgautas. Tai priklauso nuo to, kaip vartotojas elgėsi. Pagal 2022 m. Aukščiausiojo Teismo sprendimą, kuris buvo pirmasis tokio pobūdžio byloje, bankas privalėjo atkurti vartotojo sąskaitos lėšas po to, kai jis sukčiui pateikė savo *BankID* kodus. Aukščiausiasis Teismas nurodė, kad vartotojo elgesys neužtraukė jam atsakomybės už visus nuostolius, atsiradusius dėl sukčiavimo, o dalį atsakomybės turi prisiimti ir pats bankas.

Nuo 2023 m. sausio mėn. įsigaliojo naujos taisyklės, reikalaujančios griežto klientų autentifikavimo apmokant sąskaitas internetu, pavyzdžiui, už paslaugas „pirk dabar, mokėk vėliau“, siekiant užkirsti kelią sukčiavimui. Šis reikalavimas jau buvo taikomas mokėjimams, naudojant, pavyzdžiui, debeto ar kredito korteles, *Swish* paslaugą ir banko pavedimus⁴².

Vokietija

Vokietija finansinio sukčiavimo, nukreipto prieš gyventojus, prevencijai ir baudžiamajam persekiojimui naudoja griežtas teises priemones ir aktyvią priežiūrą. Vokietijos Baudžiamajame kodekse⁴³ (263 str.) sukčiavimas yra apibrėžtas kaip veiksmas, kai asmuo, apgaule suklaidindamas

⁴² *Sveriges Riksbank. Banks have a major responsibility for consumer protection:* <https://www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-report--2024/safety-efficiency-and-accessibility/are-payments-in-sweden-safe/banks-have-a-major-responsibility-for-consumer-protection/>

⁴³ *Strafgesetzbuch – StGB:* <https://www.gesetze-im-internet.de/stgb/>

kitą asmenį, paskatina jį atlikti veiksmą, dėl kurio patiriama turtinė žala. Už šią veiką baudžiama laisvės atėmimu iki 5 metų arba pinigine bauda.

Ypač sunkiais atvejais baudžiama laisvės atėmimu nuo 6 mėn. iki 10 metų. Paprastai laikoma, kad yra ypač sunkus nusikaltimas, jei:

- veikiama komerciniais tikslais arba nusikalstamoje grupuotėje;
- veikiama pakartotinai;
- padaroma didelė finansinė žala arba veikiama siekiant sukelti pavojų daugelio žmonių turtui;
- veikiama piktnaudžiaujant savo kaip pareigūno įgaliojimais ar pareigomis ir kt.

Pažymėtina, jog BK atskirai apibrėžia kompiuterinio sukčiavimo atvejus (263a str.). Šis specialus straipsnis yra itin svarbus kovojant su šiuolaikiniu finansiniu sukčiavimu, pavyzdžiui, suklasztojant duomenis ar naudojant neteisėtas prieigos priemones pinigams iš banko sąskaitų pervesti. Aptariamasis straipsnis apibrėžia, jog tas, kuris, siekdamas gauti neteisėtos turtinės naudos sau ar trečiajam asmeniui, sugadina kito asmens turtą, darydamas įtaką duomenų tvarkymo operacijos rezultatui netinkamai suprojektuojamas programą, naudodamas neteisėtus ar nepilnus duomenis, neteisėtai naudodamas duomenis arba kitaip neteisėtai įsikišdamas į procesą, baudžiamas laisvės atėmimu iki 5 metų arba bauda.

Vokietijos federalinės kriminalinės policijos biuras⁴⁴ aktyviai bendradarbiauja su tarptautinėmis institucijomis (pavyzdžiui, *Europolu*) ir kitų šalių teisėsaugos institucijomis, kadangi dauguma didelio masto finansinio sukčiavimo schemų yra tarptautinės.

Kalbant apie bankų klientų apsaugą nuo sukčiavimo, pažymėtina, jog Vokietijos bankai naudoja įvairias atitikties priemones, pavyzdžiui, IBAN ir asmens pavardės (pavadinimo) patikrinimus gavėjo tapatybei nustatyti, siekdami užkirsti kelią sukčiavimui. Taip pat yra naudojami elgesio pagrįsti saugumo sprendimai, padedantys aptikti naudotojų anomalijas, analizuoti įrenginių duomenis, kad būtų galima nustatyti sukčiavimo įrenginius.

Bankai taip pat diegia naujus būdus, skirtus informuoti klientus apie socialinės inžinerijos taktiką ir bendradarbiauja su reguliavimo institucijomis dėl atsakomybės perkėlimo už sukčiavimo atvejus, kai manipuluojama klientais, kad jie leistų atlikti sukčiavimo operacijas.

Kai kurios bankų taikomos konkrečios priemonės:

- gavėjo tapatybės patikrinimas (IBAN vardo patikrinimas);
- klientų tapatybės ir tikrųjų sąskaitų savininkų patikrinimas, kad būtų užkirstas kelias pinigų plovimui ir teroristų finansavimui;
- skaidrumo registras. Vokietija tvarko skaidrumo registrą, skirtą kovai su pinigų plovimu ir mokesčių slėpimu, teikdama informaciją apie tikruosius įmonių savininkus;
- Federalinės finansų priežiūros institucijos (vok. *BaFin*)⁴⁵ priežiūra. *BaFin* stebi bankų komercinę praktiką ir atitiktį reglamentams.

Techninės sukčiavimo prevencijos priemonės:

- elgesio analizė. Bankai naudoja sistemas, kurios analizuoja naudotojų sąveiką, pavyzdžiui, pelės judesius ir spausdinimo modelius, kad nustatytų anomalijas, kurios gali rodyti sukčiavimą, prieš patvirtinant operaciją;
- įrenginių pirštų atspaudų nustatymas. Technologija naudojama sukčiavimo įrenginiams atpažinti analizuojant jų paliktus skaitmeninius pėdsakus internete (skaitmeninis pirštų atspaudas), siekiant užkirsti kelią sukčiavimui;
- mašininio mokymosi algoritmai. Šiuolaikiniai mašininio mokymosi algoritmai naudojami sudėtingiems operacijų duomenų modeliams ir ryšiams nustatyti, padedant aptikti įtartina veiklą.

Didelis dėmesys yra skiriamas klientų švietimui ir informuotumui. Ypač aktyviai įgyvendinama kova su socialinės inžinerijos priemonėmis. Bankai perkelia savo dėmesį nuo įprastinių – ir dažnai jau pasenusių – saugumo patarimų prie klientų švietimo, kaip atpažinti psichologinės manipuliacijos taktiką, naudojamą sukčiavimo atvejais.

⁴⁴ Bundeskriminalamt: https://www.bka.de/DE/Home/home_node.html

⁴⁵ BaFin: https://www.bafin.de/EN/Homepage/homepage_node.html

Kartu pažymėtina, jog palaipsniui yra didinama ir pačių bankų atsakomybė. Tai reiškia, jog tam tikrais atvejais gali būti perkelta sukčiavimo aukos atsakomybė bankui už tam tikras sukčiavimo schemas, kai klientais manipuluojama, kad jie patvirtintų operacijas. Žinoma, labai svarbi išlieka ir kliento atsakomybė – bankai pabrėžia klientų budrumo ir dalyvavimo kovoje su sukčiavimu poreikį, nes nusikaltėliai nuolat kuria naujas taktikas socialiniuose tinkluose ir skaitmeninėse platformose⁴⁶.

Parengė

Informacijos ir komunikacijos departamento

Tyrimų skyriaus

Patarėjas Sigitas Daukša

Tel. (0 5) 209 6172, el. p. sigitas.dauksa@lrs.lt

Patarėjas dr. Tomas Lavišius

Tel. (0 5) 209 6181, el. p. tomas.lavisius@lrs.lt

Seimo kanceliarijos Informacijos ir komunikacijos departamento Tyrimų skyriaus parengti analitiniai ir informaciniai darbai skirti Seimo narių parlamentinei ir Seimo kanceliarijos veiklai. Šiuose darbuose pateikta informacija nėra oficiali Lietuvos Respublikos Seimo pozicija. Šį darbą atgaminti, išleisti, platinti, versti, perdirbti, viešai skelbti, išskyrus įstatymų nustatytas išimtis, galima tik gavus Seimo kanceliarijos leidimą.

Visais atvejais naudojant šį darbą privaloma nurodyti šaltinį.

© Lietuvos Respublikos Seimo kanceliarija, 2025

⁴⁶ Banken Verband. Payments market: we must work together to combat fraud: <https://bankenverband.de/en/die-deutsche-kreditwirtschaft/payments-market-we-must-work-together-combat-fraud>