Ginčai dėl finansinių paslaugų. 2023 m. II ketvirtis

366 kreipimaisi

199 prašymai nagrinėti ginčus

107 paklausimai

181 išnagrinėtas ginčas

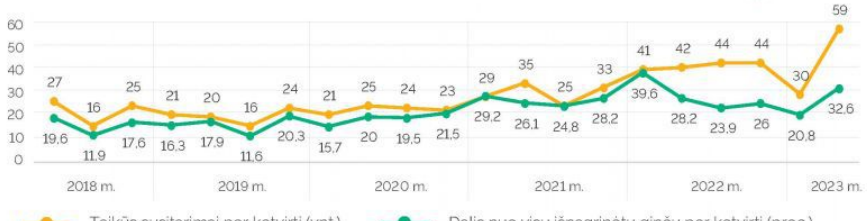
67 priimti sprendimai dėl ginčo esmės

59 pasiekti taikūs susitarimai (sprendimų dėl ginčų esmės šiais atvejais priimti nereikėjo)

Čia galite susipažinti su mūsų sprendimais dėl ginčo esmės

Išnagrinėti ginčai pagal finansų rinkos dalyvio tipą

Taikūs susitarimai (tendencijos)



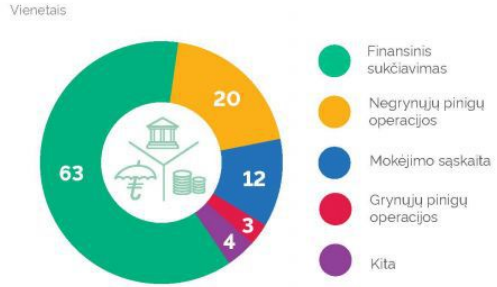
Rekordinis taikių susitarimų skaičius

Antrąjį ketvirtį pasiektas rekordinis taikių susitarimų rodiklis, kompromisu arba patenkintais vartotojų reikalavimais baigėsi trečdalis (33 %) visų išnagrinėtų ginčų – net 59 (iki šiol per vieną metų ketvirtį buvo pasiekta daugiausia 44 taikūs susitarimai).

Prevencija

Įvyko 3 prevenciniai susitikimai su dviem didžiosiomis draudimo bendrovėmis ir vienu banku, jų metu aptartos pagrindinės kylančių nesutarimų priežastys ir kiti efektyviai ginčų prevencijai aktualūs klausimai.

Ginčų dėl mokėjimo paslaugų pasiskirstymas pagal nesutarimų objektą



Būkite budrūs ir saugokitės sukčių įtakos

Lietuvos bankas apžvelgiamu laikotarpiu išnagrinėjo net 63 ginčus tarp mokėjimo paslaugas teikiančių bendrovių (bankų, elektroninių pinigų įstaigų ir mokėjimo paslaugų įstaigų) ir jų klientų, patekusių į sukčių pinkles. Pastarąjį rodiklį pradėta atidžiai sekti nuo šių metų; pirmąjį ketvirtį tokių atvejų buvo 48. Pastaruoju metu vartotojai lėšas dažniausiai praranda patekę į investicinio sukčiavimo ir duomenų viliojimo (angl. *phishing*) spąstus.

Pirmuoju atveju sukčiai (neretai rusakalbiai asmenys), apsimesdami brokeriais ir siūlydami greitą bei garantuotą uždarbį, įtikina pervesti pinigines lėšas įvairiems fiziniams asmenims ar pasipildyti savo virtualiųjų valiutų piniginę investavimo platformose ir sudaro įspūdį, kad šios lėšos bus investuojamos į virtualiąsias valiutas. Pasitaiko atvejų, kai vartotojai perveda sukčiams ne tik pinigines lėšas, bet ir virtualiąsias valiutas, prieš tai įgytas taip pat sukčių nurodytose virtualiųjų valiutų keityklose (pvz., *Binance*, *Coinbase* ar kt.). Visų Lietuvos banko išnagrinėtų ginčų baigtis buvo vienoda – paaiškėja, kad lėšos ar virtualiosios valiutos niekur nebuvo investuotos, sukčių rekomenduotose platformose reali investavimo veikla nėra vykdoma, o siųstos ataskaitos apie investicijų būklę tėra sukčių sukurtos klastotės. Turto atgauti nebepavyksta, o trečiųjų asmenų sąskaitos bankuose būna ištuštintos.

Antruoju atveju sukčiai dažniausiai apsimeta kokios nors paslaugos teikėjais, susidomėjusiais pirkėjais, bankais ar valstybinėmis institucijomis ir apgaulės būdu išgauna vartotojų duomenis, kuriuos panaudoja vartotojų lėšoms bankų sąskaitose pasisavinti. Pavyzdžiui, apsimetus siuntų tarnyba (pvz., DPD, *Omniva* ar kt.) ir pateikus suklastoto interneto puslapio nuorodą prašoma atlikti mokėjimą už vartotojui skirtos menamos siuntos pristatymą, apsimetus valstybine institucija (pvz., VMI ar Policija) reikalaujama sumokėti baudą, suvedant mokėjimo kortelės duomenis. Apsimesdami internetu parduodamo daikto potencialiais pirkėjais (pvz., radę skelbimą *Vinted* platformoje) sukčiai prašo pardavėjų prisijungti prie interneto banko paskyrų tam, kad jie galėtų atlikti mokėjimus už prekes, o apsimetę banko darbuotojais prašo pateikti mokėjimo kortelių duomenis, prisijungti prie banko paskyros pagal pateiktas nuorodas ar suvesti SMART ID slaptažodžius dėl neva esančio poreikio atnaujinti kokius nors asmens duomenis. Pasitelkę apgaulę sukčiai vartotojų vardu sukuria naujas ir tik jiems prieinamas SMART ID paskyras, pasisavina pateiktus mokėjimo kortelių ar banko sąsakaitų duomenis ir panaudoja juos mokėjimams iš duomenis atskleidusių vartotojų sąskaitų atlikti.

Pastaruoju metu padažnėjo kreipimųsi dėl galimo sukčiavimo, susijusio su *booking.com* viešbučių užsakymo internetu platforma, atvejų. Panašu, kad sukčiai šiuo atveju taip pat pasitelkia duomenų viliojimo metodus, pavyzdžiui, atsiunčia pranešimą, informuojantį, kad neva kažkas negerai su mokėjimams atlikti naudojama mokėjimo kortele ir prašoma pakartotinai pateikti jos duomenis, nurodant, kad kitaip viešbučio rezervacija bus atšaukta. Pateikus kortelės duomenis, jie perimami ir panaudojami mokėjimams atlikti, taip pasisavinant mokėjimo kortelės naudotojo lėšas.

Visus vartotojus skatiname būti ypač atsargiais ir atsakingai naudotis turimomis mokėjimo priemonėmis, saugoti tik jums žinomus mokėjimo kortelių duomenis, SMART ID slaptažodžius ir kitą informaciją, kurią sužinoję sukčiai apgaulės būdu gali išvilioti jūsų turimas lėšas. Niekada šios informacijos neteikite telefonu, neveskite į neaiškius tinklalapius, nespauskite nuorodų, kritiškai įvertinkite prašomus atlikti veiksmus. Primenane, kad komerciniai bankai telefonu neprašo nurodyti jūsų turimos individualios informacijos (slaptažodžių ir kt.), išskyrus atvejus, kai patys kreipiatės oficialiais banko kontaktais ir tam tikri pavieniai duomenys reikalingi jums identifikuoti ar pan. Jeigu kyla abejonių dėl turimų mokėjimo priemonių ir su jų naudojimu susijusių duomenų saugumo, nedelsdami kreipkitės į savo mokėjimo paslaugų teikėjus ir teisėsaugos institucijas. Išsamią informaciją apie vyraujančias sukčiavimo schemas, sukčių atpažinimą bei veiksmus patekus į jų pinkles rasite Lietuvos banko interneto svetainėje.