Verkkomaksamisen turvallisuuden seuranta-arvio

24.10.2025

Sisällys

1 Seuranta-arvion tausta

Finanssivalvonta selvitti loka-marraskuussa 2023 tekemällään kyselyllä Suomessa toimivien luottolaitosten verkko- ja mobiilipankkien sekä verkkomaksamisen turvallisuuteen liittyviä kontrolleja ja prosesseja, joilla pyritään varmistamaan asiakkaiden vahva tunnistautuminen sekä maksamisen turvallisuus maksuvälineiden väärinkäytöksiä ja muita huijauksia vastaan. Teema-arvion perusteella Finanssivalvonta suositti luottolaitoksia kehittämään verkkopankki- ja mobiilimaksamisen kontrolleja niin, että käyttäjällä olisi mahdollisuus asettaa nykyistä monipuolisemmin turvarajoituksia tekemiinsä tilisiirtopohjaisiin maksuihin. Lisäksi Finanssivalvonta suositti luottolaitoksia kehittämään maksujen monitorointia siten, että ne voisivat entistä tarkemmin pysäyttää maksut, jotka poikkeavat merkittävästi asiakkaan aikaisemmasta maksuhistoriasta, esimerkiksi maksun suuruuden tai sen tahon mukaan, jolle asiakas on aikaisemmin lähettänyt maksuja.

Tämän seuranta-arvion tavoitteena oli selvittää ovatko luottolaitokset noudattaneet Finanssivalvonnan antamia suosituksia tilisiirtopohjaisten maksujen osalta, millä muilla toimenpiteillä verkkomaksamisen petosten torjuntaa on toteutettu, ja tullaan jatkossa toteuttamaan, sekä miten sääntely luottolaitosten näkemyksen mukaan vaikuttaa petosten torjumiseen.

Seuranta-arvion kysely lähetettiin kymmenelle luottolaitokselle ja vastaukset käytiin läpi myös kahdenvälisissä tapaamisissa. Kysely koostui neljästä kysymyksestä, joita täydennettiin kasvokkain pidetyissä tapaamisissa. Kyselyn vastausaika oli 28.3. - 30.4.2025 ja tapaamiset järjestettiin touko-kesäkuussa 2025.

2 Luottolaitoksien kirjallisten ja tapaamissa saatujen vastausten läpikäynti

2.1 Verkko- ja mobiilimaksamisen kontrollit

Suurin osa luottolaitoksista kertoi kehittävänsä joko parhaillaan tai myöhemmin vuoden 2025 aikana toiminnallisuutta, missä henkilöasiakas voi itse asettaa maksu- ja/tai päiväkohtaiset euromääräiset rajat tilisiirtopohjaisille maksuille, tai että tällaisten rajojen asettamismahdollisuudet ovat jo olemassa. Kaikki luottolaitokset eivät kuitenkaan vahvistaneet, että vastaavanlainen toiminnallisuus tulisi henkilöasiakkaiden saataville vuoden 2025 aikana, sillä toimenpiteet olivat vielä kehitteillä tai arvioitavana sekä aikataulu muutoksille oli auki.

Muutama luottolaitos kertoi harkitsevansa tai oli jo aikeissa asettaa luottolaitoksen toimesta oletusarvoiset tilisiirtopohjaiset turvarajat kaikille niille henkilöasiakkaille, jotka eivät olleet ottaneet turvarajoja käyttöön. Yksittäiset luottolaitokset kertoivat myös mahdollisuudesta asettaa rajoituksia säästötileille riskiperusteisesti. Luottolaitosten kommenteista kävi ilmi, että niiden asiakkaiden kohdalla, joilla on jo tällä hetkellä mahdollisuus asettaa maksu- ja päiväkohtainen euromääräinen raja tilisiirtopohjaisille maksuille, vain harva asiakas oli tehnyt niin. Tämän lisäksi muutama luottolaitos kertoi asettavansa uusille asiakkaille tilimaksamisen turvarajat oletuksena silloin, kun verkkopankkisopimusta tehdään.

Useat luottolaitokset vastasivat, että niillä on käytössä maakohtaisia rajoitteita tilisiirtopohjaisille maksuille. Usea luottolaitos kertoi myös, että asiakkailla on tällä hetkellä mahdollisuus rajoittaa verkko- ja mobiilipankissa tehtäviä tilisiirtoja valittuihin maihin ja turvallisuussyistä osa luottolaitoksista on asettanut oletusarvoiseksi rajaukseksi lähtökohtaisesti pelkän Suomen. Myös ulkomaanmaksujen lähetykset verkko- ja mobiilipankeissa on estetty kokonaan joissakin luottolaitoksissa. Luottolaitosten vastauksissa kuitenkin todettiin, että maakohtaisten rajoitteiden hyöty voi olla vähäinen petostentorjunnassa, sillä nämä rajoitteet voidaan helposti kiertää esimerkiksi muulitilejä hyödyntämällä.

2.2 Petollisten/oikeudettomien maksutapahtumien monitorointi

Puolet arvioon osallistuneista luottolaitoksista kertoi käyttävänsä asiakkaiden käyttäytymiseen perustuvia sääntöjä petosmonitoroinnissa. Monitoroinnissa voidaan esimerkiksi seurata henkilön aiempaa maksuhistoriaa, maksun suuruutta, tapahtuma-aikaa, maksukanavaa ja maksun vastaanottajaa. Jos maksutapahtuma poikkeaa asiakkaan aiemmasta käyttäytymisestä, se merkitään korkean riskin tapahtumaksi ja asetetaan manuaaliseen lisäselvitystilaan tutkittavaksi luottolaitoksen petosasiantuntijalle.

Useat luottolaitokset kertoivat hyödyntävänsä myös asiakkaiden kirjautumiskäyttäytymistä petosten tunnistamisessa, erityisesti teknisiä tunnisteita tai poikkeavaa

käyttäytymistä. Maantieteellistä sijaintia ei kuitenkaan yleisesti käytetä suoraan tunnistuskriteerinä. Kirjautumiset, laiterekisteröinnit, epäjohdonmukaisuudet laitteiden käytössä sekä maksutapahtumissa ovat osa petosmonitorointia useissa luottolaitoksissa. Lisäksi palvelukanavien käyttöä seurataan osana petosten torjuntaa joissakin luottolaitoksissa.

Osassa luottolaitoksia petosten tunnistamisessa hyödynnetään myös asiakkaiden demografisia tietoja kuten ikää, jos data osoittaa selkeän yhteyden tietyn huijaustavan ja ikäryhmän välillä. Tällöin kontrollit voivat kohdistua tarkemmin riskialttiisiin ryhmiin. Esimerkiksi uudet IP-osoitteet ja tuntemattomat laitteet nostavat riskipisteitä ja voivat laukaista tarkempaa valvontaa. Toisaalta osa luottolaitoksista ei käytä henkilökohtaisia ominaisuuksia, kuten ikää, suoraan riskipisteytyksessä, vaan keskittyy teknisiin tunnisteisiin ja käyttäytymiseen.

Luottolaitosten käytännöt asiakkaiden itsepalvelukanavien sessioiden seuraamisessa vaihtelevat. Yksittäiset luottolaitokset kertoivat seuraavansa kirjautumisen jälkeen asiakkaan toimien ketjuuntumista kuten poikkeavia tilisiirtoja ja lähes samanaikaisia luottohakemuksia. Tällainen seuranta voi johtaa riskialttiiden maksujen keskeyttämiseen. Vaikka kyseiset tapahtumat eivät ole yleisimpiä petostapauksia, ne voivat silti nostaa riskitasoa. Yksittäiset luottolaitokset kertoivat kehittävänsä parhaillaan järjestelmiä, jotka mahdollistavat sessioiden tarkemman seurannan, esimerkiksi kirjautumisen ajankohdan tai maantieteellisen sijainnin perusteella. Toiset luottolaitokset kommentoivat, ettei sessioseuranta ole käytössä, mutta tunnistusvälineiden käyttöönoton ajankohtaa ja ensimmäisiä transaktioita seurataan osana monitorointia. Käytännöt ovat siis kehittymässä, mutta eivät vielä ole yhdenmukaisia toimialalla.

Monitorointitoimien lisäksi osa luottolaitoksista kertoi pyytävänsä tilisiirtopohjaisiin maksuihin lisävahvistuksen silloin, kun maksutapahtuman petosriski on arvioitu monitoroinnissa tavanomaista korkeammaksi. Näiden lisäksi esimerkiksi verkkopankkitunnusten tai muiden varmennussovellusten automaattinen sulkeminen monitoroinnissa havaitun petosepäilyn vuoksi on jo käytössä osalla luottolaitoksista. Tämän lisäksi tekoälyä hyödynnetään maksujen monitoroinnissa osassa luottolaitoksia.

Seuranta-arviossa muutamat luottolaitokset mainitsivat monitoroinnin haasteeksi myös sen, että monitorointisääntöjen pitää pystyä vastaamaan petostentorjunnan tarpeisiin niin, ettei kaikki maksuliikenne pysähdy petosmonitoroinnin takia.

2.3 Muut menettelyt petosten estämiseen

2.3.1 Tiedotus, koulutus ja resurssien lisääminen

Asiakkaiden ja yhteiskunnan yleinen tietoisuus petosriskeistä on vahvistunut jatkuvan koulutuksen ja kampanjoinnin myötä. Kaikki luottolaitokset kertoivatkin tehostaneensa koulutusta sekä henkilöstölleen että asiakkailleen, jotta erilaiset

petosrikollisuuden muodot tunnettaisiin mahdollisimman laajasti ja ajantasaisesti. Seuranta-arvion perusteella luottolaitokset ovat myös kehittäneet petostentorjuntaa vahvistamalla osaamista ja prosesseja organisaatioidensa sisällä sekä lisäämällä henkilöstöresursseja petosten torjuntaan. Tämän lisäksi luottolaitokset ovat panostaneet monitorointitiimien vahvistamiseen ja parantaneet sisäistä tiedonjakoa petostentorjunnan osalta.

2.3.2 Teknologiset ratkaisut

Useat luottolaitokset kertoivat asettaneensa viiveitä ja uusia kontrollimekanismeja uusien laitteiden asennusten yhteyteen. Uuden laitteen tai sovelluksen käyttöönotto käynnistää useita turvatoimia. Muutama luottolaitos kertoi edellyttävänsä vahvaa tunnistautumista QR-koodin avulla. Lisäksi useat luottolaitokset viivästyttävät uuden laitteen käyttöönoton yhteydessä tunnuslukusovelluksen aktivointia. Maksut uuden laitteen kautta ovat myös erityisen seurannan kohteena, ja osa luottolaitoksista ilmoitti seuraavansa maksuja uuden laiterekisteröinnin jälkeen tehostetusti. Tämän lisäksi jotkin luottolaitoksista vastasivat lähettävänsä tilinhaltijalle tekstiviestillä tiedon turvarajojen muutoksesta.

Luottolaitokset ovat myös tarkentaneet lähetettävien varoitustekstiviestien sisältöä ja lisänneensä yhteistyöstä teleoperaattorien kanssa huijausviestien torjumiseksi. Useat luottolaitokset kertoivat rekisteröineensä SMS Sender ID:n Traficomille. Tämä tarkoittaa, että uhkatoimijat eivät pysty lähettämään tekstiviestejä luottolaitoksen nimissä. Vastaavanlaisia toimia on tehty sähköpostiturvallisuuteen ja niiden ansiosta rikolliset eivät voi enää helposti lähettää luottolaitoksen nimissä väärennettyjä sähköposteja.

Usealla luottolaitoksella on myös suunnitteilla asiakkaan tunnistamiskontrolli, jossa käytettäisiin passin tunnistamistietoja tai NFC-sirua uuden laitteen rekisteröinnin yhteydessä. Yksittäiset luottolaitokset kertoivat vahvistaneensa luottopäätösjärjestelmien kontrolliympäristöjä siten, että niiden avulla pystyttäisiin tunnistamaan mahdollisia huijausten kautta haettuja uusia luottoja tai olemassa olevien luottojen korotuksia entistä tehokkaammin. Yksittäiset luottolaitokset kertoivat myös teknologisista ratkaisuista kuten TOR-verkon käytön estämisestä. Lisäksi jotkin luottolaitoksista kertoivat tunnistaneensa mahdollisia kryptovaluuttoihin liittyviä petoksia ja pyrkinyt aktiivisesti estämään niitä.

Seuranta-arvion perusteella teleoperaattoreiden eSIM-palveluihin liittyvät riskit tunnistautumisprosesseissa eivät ole vielä merkittävästi konkretisoituneet luottolaitosten arjessa. Joitain yksittäisiä tapauksia on havaittu, mutta ei laajamittaisesti tai kampanjaluontoisesti. Sellaiset luottolaitokset, jotka eivät käytä tekstiviestivahvistuksia laajasti maksujen lisävarmentamisessa, eivät näe eSIM:iä tällä hetkellä suurena riskinä. Muutama luottolaitos sen sijaan tunnisti, että eSIM voi muodostaa riskin erityisesti silloin, kun tekstiviestivahvistuksia hyödynnetään uusien laitteiden aktivoinnissa. Tämän vuoksi olisi tärkeää, että teleoperaattoreilla olisi yhdenmukaiset ja turvallisuutta varmistavat vahvistusmekanismit eSIM:n käyttöönotossa.

Virtuaaliset IBAN-tilinumerot nähdään luottolaitosten keskuudessa petosriskiä lisäävänä tekijänä. Niiden avulla maksunsaajan tili voi vaikuttaa turvallisemmalta kuin se todellisuudessa on, mikä voi johtaa asiakkaita harhaan ja vaikeuttaa huijausten tunnistamista. Virtuaali-IBANit voivat myös aiheuttaa haasteita maksunsaajan tietojen tarkistuksessa erityisesti pikamaksamisen yhteydessä, jossa nopeus korostuu ja läpinäkyvyys vastaanottajasta voi olla heikko. Yksittäiset luottolaitokset kommentoivat, että virtuaali-IBANeja tarjoavat palveluntarjoajat näkyvät selvästi petostapauksissa ja erityisesti silloin, kun varoja siirretään pois Suomesta. Vastausten mukaan virtuaali-IBAN-palveluihin voidaan avata tilejä helpommin kuin perinteisiin luottolaitoksiin. Kokonaisuudessaan virtuaali-IBANit tuovat mukanaan uusia haasteita, jotka edellyttävät tarkempaa seurantaa.

2.4 Lainsäädännön vaikutukset

2.4.1 Pikamaksamisasetus

Pikamaksaminen tuo mukanaan sekä turvallisuutta parantavia uudistuksia että merkittäviä riskejä petosten torjunnan kannalta. Nopeus on sekä etu että haaste, ja toimialan on kehitettävä valvontaa ja automaatiota, jotta turvallisuus säilyy myös uudessa maksamisen ympäristössä.

Luottolaitokset pitävät lähtökohtaisesti maksun saajan tilinumeron ja nimen täsmäytystä hyvänä asiana. Tietojen tarkistuksella pyritään estämään maksujen päätyminen väärille tileille sekä ehkäisemään vilpillisiä tilisiirtoja.

Luottolaitokset kuitenkin nostivat esiin useita petosten torjuntaan liittyviä riskejä. Maksujen nopea välittäminen vaikeuttaa petosten tunnistamista ja estämistä, sillä kontrollien integrointi näin lyhyeen aikarajaan on teknisesti haastavaa. Nopeus voi hyödyttää rikollisia, koska varat siirtyvät nopeasti ulkomaille tai muulitileille. Lisäksi luottolaitokset korostivat tarvetta selkeille sääntelypuitteille, jotka mahdollistavat maksujen pidättämisen petosepäilyissä. Kolmannessa maksupalveludirektiivissä (PSD3) sekä uudessa maksupalveluasetuksessa (PSR) on näillä näkymin tulossa tarkempia lisäsääntelypuitteita. Kontrollien ulottaminen pikamaksujen monitorointiin vaatii luottolaitosten mukaan seurantaa ja aikaa.

2.4.2 Kolmas maksupalveludirektiivi (PSD3) ja uusi maksupalveluasetus (PSR)

Luottolaitosten mukaan tulevat sääntelymuutokset, kuten kolmas maksupalveludirektiivi (PSD3) ja uusi maksupalveluasetus (PSR) tuovat uusia velvoitteita, mutta myös mahdollisuuksia petosten torjuntaan.

Luottolaitokset kertoivat teema-arviossa PSD3/PSR-sääntelyn tuovan mukanaan merkittäviä velvoitteita, kuten henkilöstön koulutusta, asiakkaiden varoittamista, petostietojen jakamista sekä vahvan tunnistautumisen laajentamista. Maksupalveluasetuksen luonnoksen pohjalta useat luottolaitokset olivat sitä mieltä, että siinä on paljon

hyviä puolia, kuten esimerkiksi kattava lista petosten monitorointiin liittyvää säädäntöä. Toiset luottolaitokset taas pitävät lainsäädäntöön suoraan kirjattavia petosmonitorointisääntöjä vanhentuneita jo sääntelyn astuessa voimaan.

Useimmat luottolaitokset ilmaisivat huolensa PSD3/PSR-asetuksen korvausvastuusta. Muun muassa kuluttajansuojaa vahvistetaan antamalla kuluttajille laajemmat oikeudet vaatia varojen palautusta petostilanteissa, erityisesti silloin kun huijaus tapahtuu esiintymällä palveluntarjoajan edustajana. Vastausten perusteella yksittäiset luottolaitokset kokivat, että korvausvastuukynnyksen alentaminen voi lisätä riskiä uusista rikollisuuden muodoista, kuten valeuhriutumisesta.

Luottolaitokset myös esittävät huolen, että vastuu petoksien estämisestä jää lähtökohtaisesti luottolaitosten vastuulle eikä muiden toimijoiden kuten teleoperaattoreiden, sosiaalisen median ja verkkosivustojen omistajien vastuuta petosten torjunnan osalta ole sääntelyssä huomioitu. Rikolliset hyödyntävät monikanavaisuutta ja rajapintojen hajanaisuutta, mikä vaikeuttaa petosten tunnistamista. Esimerkiksi huijaukset, joissa asiakas ohjataan väärennettyjen sivujen kautta (esim. Kela tai Omavero), ovat yleisiä ja vaikeasti torjuttavia.

2.4.3 Tietojenvaihdon ongelmat

Luottolaitosten kanssa käydyissä keskusteluissa koroistui, kuinka tärkeää on varmistaa, ettei tehokkaalle ja perustellulle petostietojen vaihdolle muodostu tarpeettomia esteitä. Tehokas yhteistyö ja tiedonvaihto muun muassa petostrendien ja toimintatapojen jakamisessa mahdollistavat petosten ja niiden yrittämisen oikea-aikaisen havaitsemisen ja pysäyttämisen sekä muiden tarvittavien toimenpiteiden käynnistämisen.

Useat luottolaitokset korostivat, että tämänhetkiseen petostietojenvaihtoon liittyy haasteita. Luottolaitokset muun muassa indikoivat, että luottolaitoslain pankkisalaisuussääntelyä tulisi tarkistaa niin, että se sallisi tietojen jakamisen pankkien ja muiden maksuliikenteeseen osallistuvien palveluntarjoajien välillä talousrikollisuuden torjumiseksi. Seuranta-arviossa luottolaitokset muun muassa kertoivat, että luottolaitokset saavat jakaa tietoja vain asiakashäiriörekisterin kautta ja sinne saa tallentaa tietoja vain tapauksista, joissa rikos kohdistuu luottolaitokseen. Luottolaitokset eivät voi kirjata rekisteriin asiakkaisiin kohdistuneita rikoksia, esimerkiksi rikoksissa käytettyjä välitilejä.

Luottolaitosten mukaan tietosuojalainsäädäntöön tarvittaisiin lisää selkeyttä ja joustavuutta, erityisesti rikostietojen käsittelyn osalta. Luottolaitokset mainitsivat myös, että uusi rahanpesuasetus, joka astuu voimaan vuonna 2027, mahdollistaa joiltakin osin tiedon jakamisen. Luottolaitokset kuitenkin korostivat, että kansallista tulkintaa ja valmistelua tulisi edistää asetuksen rinnalla.

Teknisistä ja rakenteellisista ratkaisuista vastauksissa todettiin, että tarvitaan strukturoituja tiedonvaihtomalleja, jotka mahdollistavat nopean reagoinnin. Petostiedon jakaminen reaaliaikaisesti eri luottolaitosten ja toimijoiden välillä olisi keskeistä huijaustrendien torjunnassa. Euroopassa ja pohjoismaissa on esimerkkejä hyvin toimivasta tiedonvaihtofoorumeista ja luottolaitosten mukaan esimerkiksi Finanssi-ISAC-mallin laajentaminen petosten torjuntaan voisi parantaa koordinaatiota ja tehokkuutta. Kansainvälisistä esimerkeistä mainittiin Tanska, jossa viranomaisten ja luottolaitosten yhteinen työryhmä kehittää alustaa petostentorjuntatiedon jakamiseksi. Tämän lisäksi keskusteluissa mainittiin Baltian maat, missä luottolaitokset voivat jakaa asiakaskohtaista petostietoa keskenään.

3 Yhteenveto ja analyysi

Luottolaitokset ovat kehittäneet tilipohjaisen maksamisen turvallisuutta Finanssivalvonnan suosituksia huomioiden. Useimmat luottolaitokset kertoivat ottavansa vuoden 2025 loppuun mennessä käyttöön maksu- ja/tai päiväkohtaiset turvarajat tilisiirtopohjaisille maksuille. Useat luottolaitokset myös tarjoavat asiakkailleen mahdollisuuden asettaa maa- tai aluekohtaisia rajoituksia tilisiirtopohjaisille maksuille.

Finanssivalvonnan suosituksen mukaisesti luottolaitokset ovat parantaneet myös muita kontrollimekanismeja turvatakseen tilipohjaisia maksuja. Teknologian osalta luottolaitokset ovat kehittäneet luottopäätösjärjestelmiensä kontrolliympäristöjä, lisänneet viiveitä tai muita kontrolleja uusien laitteiden käyttöönoton yhteyteen sekä tiivistäneet yhteistyötä teleoperaattoreiden kanssa huijausviestien torjumiseksi. Luottolaitokset ovat myös tarkentaneet lähetettävien varmennusviestien sisältöä ja muun muassa lisänneet varoituksia mahdollisista petosyrityksistä. Suunnitteilla on myös asiakkaan tunnistamiskontrolli, jossa hyödynnetään passin NFC-sirua tai muuta passissa olevaa tunnistamistietoa.

Finanssivalvonnan suosituksien mukaisesti luottolaitokset monitoroivat tilisiirtopohjaisia maksuja osana petostentorjuntatyötä. Tilisiirtomonitorointia pitää kuitenkin kehittää edelleen niin, että asiakkaiden käyttäytymiseen perustuvia tekijöitä lisätään monitorointiin nykyistä monipuolisemmin. Luottolaitokset hyödyntävät petosmonitoroinnissa muun muassa asiakkaiden kirjautumis- ja maksukäyttäytymisen teknisiä tunnisteita ja poikkeavaa toimintaa. Maantieteellistä sijaintia ei yleensä käytetä suoraan tunnistuskriteerinä. Joissain pankeissa hyödynnetään myös demografisia tietoja, kuten ikää, jos se liittyy tiettyihin huijaustyyppeihin. Kirjautumiset, laiterekisteröinnit, epäjohdonmukaisuudet laitteiden käytössä sekä maksutapahtumissa ovat osa petosmonitorointia useimmissa luottolaitoksissa ja tällaista toimintaa täytyy edelleen vahvistaa kaikissa luottolaitoksessa. Yleisellä tasolla kaikki luottolaitokset kertoivat lisänneensä resursseja petostentorjuntatiimeihin.

eSIM-palveluihin liittyvät riskit eivät ole toistaiseksi merkittävästi konkretisoituneet luottolaitosten arjessa, mutta yksittäisiä tapauksia on havaittu. Virtuaaliset IBAN-tilinumerot voivat lisätä petosriskiä, koska ne voivat johtaa asiakkaita harhaan ja vaikeuttaa huijausten tunnistamista erityisesti pikamaksuissa. Virtuaali-IBANien avaaminen on helpompaa kuin perinteisen tilin avaaminen luottolaitoksessa ja siksi petosriskit ovat virtuaali-IBANien kohdalla koholla.

Erilaiset tunnusten kalastelut näyttävät olevan pysyvä ja lisääntyvä ilmiö. Useat luottolaitokset kertoivat lisänneensä erilaisia turvatoimenpiteitä, ja näiden toimenpiteiden myötä toteutuneiden petollisten maksutapahtumien lukumäärä on merkittävästi pienentynyt. Samalla luottolaitokset kuitenkin korostavat, että jatkuvasti muuttuva toimintaympäristö edellyttää jatkuvaa seurantaa ja turvakontrollien kehittämistä. Useimmat luottolaitokset korostivat myös, että petostentorjunta on yhtiössä tällä hetkellä yksi tärkeimmistä prioriteeteista. Luottolaitokset muun muassa kouluttavat

säännöllisesti sekä henkilöstöään että asiakkaitaan ja käytännön toimenpiteisiin kuuluu osaamisen, prosessien ja henkilöstömäärän vahvistaminen.

Pikamaksaminen tuo maksamiseen nopeutta ja turvallisuutta, mutta samalla se kasvattaa petosriskejä. Luottolaitokset pitävät maksun saajan tietojen täsmäytystä tärkeänä turvakeinona, mutta nopea maksujen välitys vaikeuttaa petosten estämistä. Useiden luottolaitosten mielestä PSD3/PSR-sääntely tuo uusia ja tarpeellisia petosten-torjuntaan liittyviä velvoitteita, mutta myös keskittyy paljon korvausvastuuseen.

Kaikki luottolaitokset pitivät ensiarvoisen tärkeänä, että lainsäädäntöä voitaisiin muuttaa niin, että tiedonjako olisi nykyistä helpompaa eri toimijoiden kesken. Tämän lisäksi luottolaitosten vastauksissa korostui kaikkien osapuolien vastuu petostentorjunnassa – myös verkkopalveluiden ja somealustojen sekä operaattoreiden vastuuta petosten torjunnassa tulisi luottolaitosten mielestä vahvistaa.

4 Seuranta-arvion pohjalta tehtävät jatkotoimet ja suositukset

4.1 Finanssivalvonnan suositukset

4.1.1 Tilisiirtomaksujen turvarajat

9.10.2025 voimaantulevan pikamaksamisasetuksen mukaisesti luottolaitosten on tarjottava palvelu, jossa asiakas voi itse asettaa maksu- tai päiväkohtaisen euromääräisen rajan pikamaksuille.

Finanssivalvonta suosittaa, että luottolaitokset tarjoaisivat turvarajat sekä maksu- että päiväkohtaisesti tilipohjaisille maksuille myös normaaleissa tilisiirroissa.

Tämän lisäksi Finanssivalvonta suosittaa, että luottolaitos asettaisi henkilöasiakkaiden tilisiirtopohjaisille maksuille oletusarvona maksu- ja päiväkohtaisen euromääräisen rajan, mikäli henkilöasiakas ei ole itse asettanut rajaa. Luottolaitokset voivat itse määrittää euromääräiset rajat henkilöasiakkailleen riskiperusteisesti.

Finanssivalvonta katsoo, että turvarajan muuttaminen edellyttää vahvan tunnistamisen toteuttamista maksupalvelulain 85 c §:n 1 momentin 3 kohdan mukaisesti.

4.1.2 Muut maksamisen kontrollit

Finanssivalvonta suosittaa, että luottolaitokset parantavat myös muita maksamisen turvallisuuteen liittyviä kontrolleja, kuten esimerkiksi:

- viiveiden asettaminen tai muu vastaava turvallisuuskontrolli uuden tunnistussovelluksen asentamisen yhteydessä.
- lisävahvistuksen pyytäminen maksuissa, joissa pankin monitorointi epäilee petollista maksua.

4.1.3 Petosmonitoroinnin kehittäminen

Finanssivalvonta suosittaa, että luottolaitokset kehittävät reaaliaikaista petosmonitorointia niin, että monitoroinnissa käytettäisiin asiakkaan käyttäytymiseen perustuvia tekijöitä kuten esimerkiksi aikaisempaa maksuhistoriaa, maksun suuruuta, tapahtuma-aikaa, maksukanavaa, maksun vastaanottajaa tai maksajan poikkeavaa sijaintipaikkaa.

4.2 Viranomaiskeskustelujen käynnistys lainsäädäntömuutoksien kartoittamiseksi

Keskusteluissa luottolaitosten kanssa tuli ilmi petostietojenvaihtoon liittyviä haasteita. Finanssivalvonta on tunnistanut vastausten ja keskusteluiden perusteella lainsäädännöllisiä haasteita, jotka saattavat rajoittaa petosten torjunnan kannalta tärkeää tiedonvaihtoa eri toimijoiden välillä. Finanssivalvonta selvittää eri viranomaisten kanssa, miten tietojen jakamisen esteet tulisi poistaa.

4.3 Sosiaalisen median ja verkkosivustojen vastuuttaminen

Luottolaitokset ilmaisivat kyselyssä huolensa sosiaalisen median ja verkkosivustojen kautta leviäviin petoksiin. Niiden mukaan sosiaalisen median ja verkkosivustojen omistajat mahdollistavat huijauksia mm. sallimalla väärennettyjä mainoksia tai kalastelusivustoja ja EU:n ulkopuoliset toimijat, kuten hakukoneet ja sosiaalisen median alustat, vaikeuttavat valvontaa ja vastuuttamista. Finanssivalvonta on tietoinen näistä haasteista ja saattaa teema-arvion tulokset tältä osin myös Euroopan komission tietoisuuteen.