**SMJERNICE ZA UPRAVLJANJE RIZIKOM OD PRANJA NOVCA I FINANSIRANJA TERORIZMA U SISTEMU INSTANT PLAĆANJA (TIPS CLONE)**

## GLOSARIJ

- **Operativna konvergencija:** Integrisani pristup i saradnja između bankarskih sektora za IT/Anti-Fraud (prevencija prevara) i sektora za SPN/FT, u cilju izbjegavanja postojanja operativnih silosa.
- **TIPS Clone:** Sistem za instant plaćanja u Crnoj Gori koji omogućava izvršenje transakcija u realnom vremenu (unutar 10 sekundi), 24/7/365, uz neopozivost i konačnost poravnanja.
- **Real-time Screening (Skrining u realnom vremenu):** Automatizovana provjera transakcija prema listama sankcija i internim indikatorima sumnje u trenutku iniciranja naloga.
- **TFS Screening (Targeted Financial Sanctions):** Provjera učesnika u transakciji prema listama ciljanih finansijskih sankcija (UN, EU i nacionalne liste).
- **Inter-batch Screening:** Provjera onih klijenata koji su unijeti ili ažurirani u bazu podataka u periodu između dva redovna ciklusa grupnog (dnevnog) skrininga klijentske baze.
- **Fail-Closed princip:** Tehnički protokol po kojem se transakcija automatski odbija (reject) ako sistem za kontrolu (AF/SPN/FT) usljed tehničkih problema ne može izvršiti procjenu rizika u propisanom roku.
- **Kill-switch (Protokol za hitnu obustavu kanala):** Mehanizam za trenutno suspendovanje svih instant kanala ili specifičnih grupa klijenta u situacijama ekstremnog bezbjednosnog rizika.
- **Digitalni otisak (Device ID / Fingerprinting):** Skup tehničkih podataka koji jedinstveno identifikuju uređaj (telefon, tablet, PC) sa kojeg je inicirana transakcija.
- **IP adresa (Internet Protocol):** Numerička oznaka uređaja u mreži koja se koristi za geolokaciju nalogodavca i prepoznavanje sumnjivih promjena lokacije.
- **VPN (Virtual Private Network):** Servis za prikrivanje stvarne lokacije korisnika; njegova upotreba u instant plaćanjima često se tretira kao indikator povišenog rizika.
- **Impossible Travel (Geografska neusklađenost):** Detekcija dvije ili više transakcija sa istog naloga na fizički udaljenim lokacijama u vremenskom intervalu u kojem je fizički nemoguće preći tu razdaljinu.
- **Remote Access softver:** Alati (poput AnyDesk ili TeamViewer) koji omogućavaju udaljeni pristup uređaju; detekcija njihovog rada tokom sesije plaćanja ukazuje na rizik od prevare.
- **Mule Account (Račun "mula"):** Račun koji se koristi kao tranzitna tačka za prenos protivpravno stečenog novca. U instant sistemu ga karakteriše brzi priliv i još brži odliv sredstava.
- **Fan-in (Agregacija):** Primanje velikog broja malih uplate od različitih lica u kratkom roku na jedan račun (često povezano sa finansiranjem terorizma ili investicionim prevarama).
- **Fan-out (Disperzija):** Jedan veliki priliv koji se odmah dijeli na seriju brzih instant odliva ka većem broju nepovezanih fizičkih lica (faza raslojavanja novca).
- **Smurfing (Usitnjavanje):** Iniciranje serije transakcija u iznosima neposredno ispod zakonskih ili internih pragova za izvještavanje i dubinsku provjeru.
- **Pass-through (Brzi protok):** Dinamika prometa gdje novac ostaje na računu ekstremno kratko (npr. manje od 5 minuta) prije nego što se podigne u gotovini ili proslijedi dalje.
- **Dormant Account (Neaktivni račun):** Račun bez prometa koji se iznenada aktivira za visokofrekventne instant transakcije, što je čest indikator kompromitacije naloga.
- **Hold / Suspenzija:** Privremeno zadržavanje sumnjivog naloga prije slanja u kliring, radi dodatne provjere ili po nalogu Finansijsko-obavještajne jedinice.

- **Recall (Opoziv):** Međubankarski zahtjev za povraćaj sredstava iniciran nakon što je transakcija već realizovana, zasnovan na naknadno utvrđenoj sumnji na kriminalnu aktivnost.
- **Ex-post analiza:** Retrospektivna provjera već izvršenih transakcija radi uočavanja obrazaca koji se nisu mogli detektovati u intervalu od 10 sekundi (npr. strukturna agregacija tokom 24 sata).

## 1. UVOD I PREDMET SMJERNICA

1.1 Svrha ovih smjernica (u daljem tekstu: Smjernice) je uspostavljanje jasnog i koherentnog okvira koji će omogućiti obveznicima (u daljem tekstu: Kreditne institucije) identifikaciju, procjenu i efikasno ublažavanje specifičnih rizika od pranja novca i finansiranja terorizma. Iako se primarno zakonska obaveza odnosi na sprječavanje pranja novca i finansiranja terorizma (u daljem tekstu: SPN/FT), ove smjernice prepoznaju i rizike od prevarnih aktivnosti (fraud) kao predikatnih krivičnih djela čiji se imovinski efekti – protivpravnog sticanja imovine, nastoje integrisati u legalne tokove kroz sisteme instant plaćanja u kreditnim institucijama. Shodno tome, mehanizmi za detekciju prevara tretiraju se kao neodvojiv segment sistema za SPN/FT, jer neadekvatna zaštita od prevarnih akivnosti direktno generiše rizik od pranja novca i finansiranja terorizma, dobijenog kriminalnim aktivnostima.

1.2 Smjernice su donesene u skladu sa Zakonom o sprječavanju pranja novca i finansiranja terorizma [("Sl. list CG", br. 110/2023, 065/24 i 024/25), u daljem tekstu: Zakon] i oslanjaju se na opšte Smjernice za analizu rizika i uspostavljanje sistema upravljanja rizikom od PN/FT Centralne banke Crne Gore (u daljem tekstu:Opšte smjernice). Ove smjernice služe kao okvir za implementaciju međunarodno prihvaćenih standarda koje obveznici treba da inkorporiraju u svoje sisteme upravljanja rizicima od pranja novca i finansiranja terorizma, u cilju očuvanja integriteta finansijskog sistema Crne Gore.

1.3 Karakteristike sistema instant plaćanja (TIPS Clone) karakteriše izvršenje transakcija u realnom vremenu (unutar 10 sekundi), 24/7/365 dostupnost i njihova neopozivost. Opisani zahtjevi u pogledu brzine i kontinuitet poslovanja čine tradicionalne mehanizme kontrole, monitoringa klijenata i transakcija koji se zasnivaju na prethodnoj (ex-ante) analizi, koje se smatraju neadekvatnim za blagovremeno sprječavanje nezakonitih aktivnosti. Stoga, smjernice nalažu kreditnim institucijama prilagođavanje internih akata i mjera poznavanja i praćenja klijenta specifičnostima realizacije instant transakcija, prelazeći sa modela tradicionalne kontrole na proaktivni model holističkog praćenja poslovnog odnosa i transakcija klijenata u realnom vremenu (tzv. relationship monitoring).

1.4 Cilj smjernica je da:

- Osiguraju usklađenost sa zahtjevima Evropske unije i preporukama FATF-a, promovišući najbolje prakse u detekciji i sprječavanju zloupotrebe finansijskog sistema;
- Unaprijede efikasnost automatizovanih sistema za provjeru u realnom vremenu (tzv. real-time screening) u odnosu na liste ciljanih finansijskih sankcija (tzv.TFS screening);
- Podstaknu razvoj naprednih IT sistema koji su sposobni da kroz definisane pragove i limite (tzv. thresholds) prepoznaju sumnjive obrasce ponašanja, uključujući identifikaciju računa "mula" (tzv. mule accounts) u trenutku iniciranja transakcije;

- Osnaže saradnju ovlašćenih lica u kreditnim institucijama i njihovu sposobnost da upravljaju sklonostima ka riziku (tzv. risk appetite) kreditne institucije u digitalnom okruženju.

1.5 Ove smjernice predstavljaju dinamički dokument koji podliježe redovnom ažuriranju i usklađivanju sa novim trendovima prevara, tipologijama pranja novca i finansiranja terorizma, kao i sa očekivanim narednim fazama razvoja Tips clone platnog sistema u cilju uspostavljanja prekograničnih transakcija sa državama Zapadnog Balkana (WB6). Obveznici su dužni da obezbijede ekvivalentan nivo sigurnosti i integriteta finansijskog sistema Crne Gore, tretirajući ove smjernice kao minimalni standard u izgradnji otpornosti na rizike PN/FT u instant okruženju.

## 2. PROCJENA RIZIČNOSTI USLUGA I KANALA DOSTAVE

Shodno članu 12 Zakona, obveznik je dužan da vrši procjenu rizika za nove proizvode, usluge ili distributivne kanale (u koje se ubraja i sistem instant plaćanja) i da na osnovu te procjene ažurira svoju analizu rizika. Analiza rizika mora biti sačinjena u pisanoj i elektronskoj formi, srazmjerna prirodi i obimu poslovanja obveznika, te redovno ažurirana.

2.1. Inherentni rizici instant plaćanja kao distributivnog kanala

U skladu sa zakonskom definicijom distributivnog kanala (čl. 6, stav 1, t. 42 Zakona), TIPS Clone sistem uvodi specifične ranjivosti koje kreditna institucija mora identifikovati u svojoj analizi rizika:

- Realizacija transakcije u roku od 10 sekundi drastično skraćuje vrijeme za detekciju sumnjivih obrazaca, što ovaj kanal čini privlačnim za brzo raslojavanje (tzv.layering) sredstava;
- Neopozivost i konačnost poravnanja podrazumijevaju da je jednom inicirano plaćanje neopozivo, što zahtijeva da se automatizovani mehanizmi kontrole aktiviraju i završe prije same finalizacije transakcije;
- Dostupnost 24/7/365, odnosno kontinuirano funkcionisanje instant platnog sistema zahtijeva od kreditnih institucija da obezbijede adekvatno upravljanje rizicima i van redovnog radnog vremena, sprječavajući zloupotrebe u periodima smanjenog ljudskog nadzora.

2.2. Tehnološki rizici i digitalna lokacija – Analiza adekvatnosti sistema za sprječavanje prevara

U skladu sa obavezom identifikacije rizika novog distributivnog kanala, analiza rizika kreditne institucije mora obuhvatiti ocjenu uspostavljenih sistema za sprječavanje prevara (Anti-fraud - AF sistemi). Zaključci proizašli iz ove analize direktno opredjeljuju nivo inherentnog i preostalog rizika od PN/FT, s obzirom na to da AF rješenja predstavljaju primarnu preventivnu barijeru za nastanak predikatnih krivičnih djela.

2.3 Analiza rizika obveznika u ovom segmentu mora utvrditi postojanje i efikasnost sljedećih AF kontrola:

- Identifikacija i validacija digitalnog otiska - uspostavljeni sistemi trebaju imati sposobnost prikupljanja i analize metapodataka u realnom vremenu (npr. IP adresa, Device ID,

precizna geolokacija). Ukoliko se analizom utvrdi odsustvo ovih mehanizama, zaključak mora ukazati na postojanje neadekvatno uspostavljenog sistema za prevenciju prevarnih aktivnosti, što nivo rizika od PN/FT distributivnog kanala automatski pozicionira u kategoriju "Visok".

- Detekcija tehnoloških anomalija i prikrivanja identiteta, što znači da AF sistemi trebaju kroz pristup procjene rizika biti adekvatno kalibrisani za prepoznavanje:
    - Upotrebe anonimizatora - korišćenje VPN servisa ili anonimnih proksija s ciljem prikrivanja stvarne lokacije korisnika;
    - Kompromitacije integriteta sesije - detekcija softvera za daljinsko upravljanje (npr. AnyDesk, TeamViewer) koji ukazuju na visok rizik od neovlašćenog raspolaganja sredstvima klijenta kreditne institucije.
- Operativna konvergencija i protokoli izvještavanja - analiza rizika mora definisati jasnu vezu između operativnih incidenata i PN/FT rizika. U skladu sa članom 56 b Zakona o platnom prometu, kreditna institucija je dužna da uspostavi okvir sa odgovarajućim mjerama ublažavanja i kontrolnim mehanizmima za upravljanje operativnim i bezbjednosnim rizicima, u vezi sa platnim uslugama koje pruža. Takođe, svaki značajan operativni ili bezbjednosni incident koji obveznik prijavljuje Centralnoj banci, mora istovremeno inicirati i aktivaciju SPN/FT protokola. Ovaj zaključak se temelji na činjenici da prevara na instant kanalu predstavlja početnu tačku za proces pranja novca, te da blagovremena interna razmjena podataka omogućava hitnu identifikaciju i blokadu računa "mula" (mule accounts).

2.4 Uticaj analize na utvrđivanje nivoa rizika izloženosti od PN/FT:

- Pozitivan nalaz bi podrazumijevao postojanje uspostavljenih i integrisanih AF alata, i isto omogućava zaključak o nižoj stopi ranjivosti od PN/FT. Takav nalaz daje osnov obvezniku da u okviru svog pristupa zasnovanog na procjeni rizika definiše liberalnije kumulativne pragove i veću dostupnost usluge.
- Negativan nalaz bi podrazumijevao da je analizom rizika utvrđen nedostatak potrebnih tehničkih AF kontrola, što kreditnu instituciju obavezuje na uvođenje umanjenih internih limita i pojačanog dodatnog nadzora nad svim transakcijama unutar kanala za instant plaćanja, s obzirom na to da se takav sistem smatra neotpornim na zloupotrebe u svrhe PN/FT.

2.5. Rizici prekogranične interoperabilnosti

U okviru procesa procjene rizika, obveznici moraju analizirati implikacije proširenja dostupnosti instant plaćanja na prekogranični nivo. Analiza mora obuhvatiti geografski rizik povezan sa jurisdikcijama sa kojima se ostvaruje platni promet, oslanjajući se na smjernice iz Nacionalne procjene rizika (NPR) i uvažavajući specifičnu dinamiku i brzinu izvršenja transfera u međunarodnom kontekstu.

2.6. Upravljanje rizicima u ranoj fazi eksploatacije kanala

Uvođenje instant plaćanja zahtijeva od kreditnih institucija uspostavljanje adekvatnih kontrola od prvog dana funkcionisanja servisa. Tokom početnog perioda eksploatacije distributivnog kanala (do 6 mjeseci), institucije su dužne sprovoditi intenzivnu kalibraciju sistema za automatizovani nadzor transakcija. Tokom ovog procesa, obveznik ne smije umanjiti efikasnost kontrolnih mjera, već kroz analizu podataka iz realnog vremena osigurati da sistem upravljanja rizicima adekvatno odgovara na specifičnu dinamiku instant transfera.

2.7 U okviru ove faze, analiza rizika obveznika može predvidjeti:

- Korišćenje inicijalnih mjeseci za "mašinsko učenje" i prilagođavanje scenarija nadzora specifičnostima domaćeg tržišta, čime se smanjuje broj lažno pozitivnih rezultata (false positives) i omogućava preciznije profilisanje klijenata;
- Postepeno skaliranje pragova i limita (tzv. thresholds) - dodatna mjera opreza kod novog distributivnog kanala, kreditne institucije mogu definisati privremene, niže interne limite (npr. do 1.000 EUR po transakciji) za određene kategorije klijenata. Ovo omogućava obvezniku da testira otpornost svojih AF i PN/FT sistema prije prelaska na maksimalne sistemske iznose (maksimalni propisani iznosi od 3,000 EUR po transakciji);
- Kreditne institucije koje su dio međunarodnih grupa i koje primjenjuju već dokazane grupne standarde za instant monitoring, mogu ovaj period skratiti ili prilagoditi, uz obavezu da u svojoj unutrašnjoj analizi dokumentuju razloge za takvu odluku i dokaze o efikasnosti preuzetih kontrola;
- Kreditne institucije koje primjenjuju već testirane standarde unutar svojih bankarskih grupa mogu, na osnovu sopstvene dokumentovane procjene, skratiti ili prilagoditi ovu fazu, pod uslovom da osiguraju ekvivalentan nivo sigurnosti.

2.8. Obaveza procjene rizika prije uvođenja distributivnog kanala

Shodno članu 16 Zakona, obveznik je dužan da procijeni rizik od PN/FT u odnosu na novi proizvod, uslugu ili distributivni kanal, kao i u odnosu na korišćenje savremenih tehnologija koje omogućavaju anonimnost ili brzinu, prije njihovog uvođenja. Na osnovu te procjene, obveznik je dužan da preduzme dodatne mjere radi ublažavanja i upravljanja identifikovanim rizicima.

2.9 U skladu sa navedenim, obveznici su dužni da:

- Izvrše formalnu reviziju analize rizika prije aktivacije TIPS Clone sistema – kreditna institucija mora dokumentovati procjenu uticaja ovog kanala na ukupni profil rizika od PN/FT kreditne institucije;

- Ukoliko se analizom utvrdi da savremena tehnologija instant plaćanja povećava izloženost riziku od PN/FT, kreditna institucija je dužna da uvede strože mjere (npr. napredne AF sisteme ili prilagođavanje uspostavljenih automatizovanih alata za SPN/FT ) prije nego što klijenti dobiju pristup usluzi;

- Svaka naknadna promjena u tehnologiji ili načinu pružanja instant usluge (npr. uvođenje biometrije ili proširenje plaćanja sa drugim državama) zahtijeva ponovnu primjenu člana 16 i ažuriranje pratećih mjera ublažavanja rizika;

2.10 Uslovljavanje maksimalnih limita i princip Fail-Closed

Prije produkcijskog puštanja usluge u TIPS Clone sistemu, kreditna institucija je dužna da sprovede i dokumentuje stres-test integracije AF i SPN/FT sistema. Na osnovu rezultata, kreditna institucija primjenjuje sljedeći okvir:

- **Nivo 1** (Puna operativna spremnost): Ukoliko institucija dokaže da su AF sistemi (biometrija, geolokacija, device ID) integrisani sa SPN/FT monitoringom, da se TFS skrining baze vrši dnevno i da obrada traje kraće od vremena potrebnog za procesiranje instant naloga (<10s), preporučuje se postavljanje maksimalnog sistemskog limita do 3.000 EUR po transakciji;
- **Nivo 2** (Uslovna spremnost / pojačan rizik): Ukoliko institucija ne posjeduje sisteme za analizu ponašanja klijenta u realnom vremenu (nedostatak metapodataka) ili se TFS provjere vrše periodično (ne na dnevnom nivou), smatra se da distributivni kanal nosi visok preostali rizik. U tom slučaju, institucija je obavezna da primijeni mjeru ublažavanja rizika kroz ograničavanje maksimalnog iznosa instant transakcije (npr. do 500 EUR ili 1.000 EUR), dok se ne uspostave adekvatne tehnološke kontrole;
- **Princip "Fail-Closed":** U slučaju tehničkog prekida u radu AF/SPN/FT modula ili nemogućnosti sistema da obradi i procijeni rizik transakcije unutar propisanog vremena za izvršenje instant plaćanja, kreditna institucija mora primijeniti "Fail-Closed" pristup, odnosno transakcija mora biti automatski odbijena (reject), uz obavještenje klijentu o tehničkoj nemogućnosti realizacije.

## 3. MJERE POZNAVANJA I PRAĆENJA KLIJENTA U INSTANT OKRUŽENJU (KYC / CDD)

Članom 16, 17 i 18 Zakona, kreditna institucija je dužna da sprovede mjere poznavanja i praćenja klijenta, koje uključuju identifikaciju, verifikaciju i prikupljanje podataka o prirodi poslovnog odnosa, kao i praćenje transakcija klijenta tokom čitavog trajanja poslovnog odnosa.

### 3.1. Specifičnosti poznavanja i praćenja klijenta u instant okruženju

S obzirom na digitalnu prirodu kanala za instant plaćanje, kreditna institucija mora osigurati da su podaci o klijentu ažurni i verifikovani na način koji omogućava nesmetano funkcionisanje sistema za provjeru u realnom vremenu (real-time screening) kao i da osigura da su sve faze identifikacije i verifikacije završene prije iniciranja naloga, što podrzumijeva i da:

- Kreditna institucija osigura da su identifikacioni podaci (ime, adresa, JMBG/PIB) u bazi podataka klijenata ažurirani i precizni, jer bilo kakva nepodudaranja tokom obrade instant transakcije dovodi do neopravdanog odbijanja naloga ili propusta u detekciji sumnjivog klijenta ili transakcije;

- Ukoliko se za iniciranje plaćanja koriste proksi podaci (npr. broj telefona povezan sa IBAN računom klijenta), obveznik mora osigurati da je veza između tog podaka i identiteta klijenta prethodno potvrđena kroz sigurne metode autentifikacije.

### 3.2 Praćenje specifičnih obrazaca ponašanja klijenta u instant okruženju

Kreditna institucija je dužna da:

- Svako značajno odstupanje od parametara kao što su uobičajeno vrijeme iniciranja transakcije, geografska lokacija (geolocation) i Device ID (digitalni otisak uređaja), tretira kao indikator povećanog rizika;
- Utvrdi biometriju, odnosno digitalno ponašanja klijenta - primjena tehnologija koje analiziraju način interakcije korisnika sa aplikacijom, kako bi se u fazi iniciranja naloga prepoznali obrasci koji ukazuju na to da nalogom ne upravlja klijent (npr. botovi ili udaljeni pristup putem softvera kao što su AnyDesk ili TeamViewer);
- Utvrdi transakcije ka nepoznatom primaocu – instant nalozi visokih iznosa ka licima sa kojima klijent ranije nije imao promet zahtijevaju dodatnu validaciju putem AF/SPNFT algoritama (tzv. first-time payee).
- Identifikuje prilive na račune klijenata koji su duži period bili neaktivni, a koji se odmah nakon priliva disperzuju putem više instant naloga ka trećim licima (tzv. mule account indikatori).
- Tehnološka diskrepanca i sumnja (član 18, tačka 4) - u slučaju da anti-fraud (AF) alati detektuju sumnju na neovlašćeni pristup računu klijenta (VPN, Remote Access ili nepoznat uređaj), kreditna institucija momentalno pokreće postupak produbljene provjere identiteta klijenta.

### 3.3. Provjera klijentskog portfolija kreditne institucije prema listama sankcija (TFS screening)

Primjena ciljanih finansijskih sankcija (Targeted Financial Sanctions – TFS) u okviru TIPS Clone sistema predstavlja jedan od najzahtjevnijih aspekata usklađenosti kreditne institucije. Iako priroda instant plaćanja nalaže izvršenje unutar vremenskog okvira od 10 sekundi, ova brzina ne oslobađa kreditnu instituciju obaveze da spriječi izvršenje transakcije u kojoj učestvuju lica sa lista sankcija.

U skladu sa međunarodnim standardima (EU direktiva: Instant Payments Regulation - IPR), fokus se pomjera sa provjere pojedinačnih transakcija u realnom vremenu na visokofrekventni skrining baze klijenata.

- Kreditne institucije su dužne da vrše ažuriranje i provjeru cjelokupne baze svojih klijenata u odnosu na liste sankcija (UN, EU, nacionalne liste) najmanje jednom dnevno. Ovaj pristup osigurava da su svi podaci o klijentima validirani prije same inicijacije instant naloga.
- Provjera klijenata u periodu između dva grupna skrininga (Inter-batch Screening) - obaveza dnevnog grupnog skrininga ne isključuje obavezu provjere klijenta u trenutku uspostavljanja poslovnog odnosa (on-boarding screening). Za sve klijente koji su otvorili račun ili su ažurirani u bazi nakon sprovedenog prethodnog grupnog skrininga klijentske baze, kreditna institucija je dužna da obezbijedi neposrednu provjeru prema listama sankcija prije aktivacije usluge instant plaćanja. Time se osigurava da je svaki učesnik u TIPS Clone sistemu validiran u odnosu na najnovije dostupne liste sankcija, čime se

minimizuje rizik od izvršenja transakcije prije narednog redovnog ciklusa grupne obrade klijentske baze.

- S obzirom na kontinuiranu dostupnost TIPS Clone sistema (24/7/365), kreditne institucije su dužne da uspostave tehničke mehanizme za automatizovano preuzimanje i implementaciju izmjena lista sankcija (UN, EU, nacionalne liste) bez odlaganja, čime se eliminiše vremenski jaz između objave nove liste i njene primjene u kontrolnim sistemima. U slučaju da nadležne međunarodne organizacije objave ažurirane liste van redovnog radnog vremena ili između dva grupna ciklusa skrininga klijentske baze, obveznik je dužan da kroz automatizovanu provjeru identifikuje i momentalno suspenduje sve odlazne transakcije i digitalne kanale klijenta koji se podudara sa novim unosom na relevantnoj sankcionoj listi.
- Restriktivne mjere primjenjuju se bez odlaganja, najkasnije u roku od 24 časa od momenta usvajanja rezolucija UN, odnosno danom donošenja odluka, bez odlaganja, o uvođenju restriktivnih mjera na osnovu akata EU ili drugih međunarodnih institucija, odnosno danom donošenja odluka, bez odlaganja, o utvrđivanju nacionalnih restriktivnih mjera. Svako izvršenje instant transakcije nakon objave izmjena na listama sankcija, a usljed kašnjenja u ažuriranju internih sistema, smatra se propustom u upravljanju operativnim i PN/FT rizikom.

### 3.4. Osiguranje integriteta podataka i primjena "travel rule" standarda (član 35 Zakona)

U cilju obezbjeđivanja pune transparentnosti finansijskih tokova u okviru TIPS Clone sistema, kreditne institucije su dužne da osiguraju da svaka platna poruka sadrži potpun i tačan set informacija o platiocu i primaocu, čime se sprječava anonimnost transakcija.

- Obavezni set podataka koji nalog instant plaćanja mora sadržati

    1. Ime i prezime / naziv platioca i primaoca;
    2. Broj računa (IBAN) platioca i primaoca, odnosno jedinstvenu oznaku transakcije ako se instant plaćanje vrši bez otvaranja platnog računa;
    3. Adresu platioca ili, kao alternativu, njegov JMBG / PIB ili datum i mjesto rođenja;

- Banka primaoca u instant sistemu ima samo par sekundi da odluči da li će prihvatiti ili odbiti nalog. Banka primaoca instant plaćanja je dužna da uspostavi efikasne procedure za detekciju naloga kojima nedostaju obavezni podaci o nalogodavcu. Takve transakcije moraju biti automatski suspendovane ili odbijene (Reject).

### 3.5. Monitoring tačnosti podataka u stvarnom vremenu i obaveza odbijanja instant naloga (član 37 Zakona)

U skladu sa članom 37 stav 1 Zakona, kreditna institucija primaoca je dužna da uspostavi efikasne procedure za otkrivanje nedostatka podataka u realnom vremenu.

Shodno članu 37 Zakona, kreditna institucija primaoca plaćanja ima ulogu kontrolnog organa integriteta i tačnosti dolaznih instant poruka. S obzirom na brzinu izvršenja TIPS transakcija, obveznici su dužni da kroz svoje interne akte preciziraju sljedeće operativne standarde:

- Sistemska detekcija i monitoring (Stav 1): Iako Zakon ostavlja mogućnost izbora između ex-post praćenja i praćenja u stvarnom vremenu, priroda instant plaćanja (izvršenje unutar 10 sekundi) nalaže isključivo model praćenja u stvarnom vremenu. Interni akti moraju predvidjeti automatizovane kontrole koje u trenutku prijema poruke provjeravaju postojanje podataka iz člana 35 Zakona;
- Mjere kod nedostatka podataka (Stav 2): U slučaju da poruka ne sadrži tačne i potpune podatke, banka primaoca, u skladu sa sopstvenom procjenom rizika, sprovodi jednu od sljedećih radnji: a) **odbijanje prenosa** (Reject) -automatizovano odbijanje naloga kao najsigurnija mjera očuvanja integriteta, b) **obustava do prijema podataka** - zadržavanje sredstava (izuzetno, ako sistem to dozvoljava bez kršenja pravila platnog sistema) dok se od banke pošiljaoca ne dobiju informacije, c) **izvršenje uz naknadno potraživanje** – koje dozvoljeno samo za niskorizične transakcije, uz obavezu naknadnog kompletiranja dokumentacije;
- Postupanje prema neusklađenim institucijama (Stav 3, 4 i 5): Kreditna institucija je dužna da prati učestalost propusta drugih pružalaca platnih usluga. Ukoliko se identifikuje kreditna institucija koja kontinuirano šalje nepotpune podatke, banka je obavezna da: a) uputi zvanično upozorenje i odredi rok za usklađivanje, b) u slučaju nepostupanja, odbije buduće prenose ili prekine poslovnu saradnju, c) o svim preduzetim mjerama i identitetu neusklađenog pružaoca usluga obavijesti Centralnu banku Crne Gore;
- SPN/FT analiza i izvještavanje (Stav 6 i 7) - nedostatak podataka se ne smije tretirati isključivo kao tehnička greška. Banka primaoca je dužna da utvrdi da li nepotpun nalog ukazuje na sumnju u PN/FT.

## 4. KONTINUIRANO PRAĆENJE POSLOVNOG ODNOSA I KONTROLA TRANSAKCIJA (član 49 Zakona)

Shodno članu 49 Zakona, obveznik je dužan da sprovodi stalno praćenje poslovnog odnosa i kontrolu transakcija radi usklađenosti sa profilom rizika klijenta.

### 4.1. Dinamički profil klijenta i uobičajeni obim realizovanih transakcija u realnom vremenu

Shodno članu 49 stav 1 tačka 3 Zakona, obveznik je dužan da prati usaglašenost poslovanja sa klijentovim uobičajenim obimom poslovanja. U TIPS Clone sistemu, ovo podrazumijeva:

- Profilisanje frekvencije (tzv.velocity profiling) - umjesto mjesečnog obima, sistem mora definisati "uobičajeno" kroz broj instant transakcija u satu ili danu. Svako naglo odstupanje (npr. klijent koji šalje jedan nalog mjesečno, naglo realizuje deset naloga u 30 minuta) mora inicirati automatski alarm ili privremenu suspenziju kanala;
- Vremenski otisak (tzv.temporal analysis) kao ključni parametar za identifikaciju anomalija u ponašanju klijenata - kontrola transakcija mora uzeti u obzir vrijeme iniciranja. Transakcije inicirane u terminima koji značajno odstupaju od uspostavljenog profila klijenta klasifikuju se kao visokorizične sa aspekta AF i SPN/FT rizika, prvenstveno zbog sumnje na kompromitaciju naloga ili korišćenje računa u svrhe "novčanih mula". Kao indikativni scenariji visokog rizika izdvajaju se:

-Aktivacija neaktivnih računa (tzv. dormant accounts) - situacije u kojima klijent sa dugom istorijom pasivnog korišćenja računa (npr. samo plaćanje režija) iznenada aktivira nalog u neuobičajeno vrijeme (npr. 02:00h) i inicira seriju instant transfera ka subjektima bez prethodne poslovne istorije;

-Odstupanje od poslovnog ciklusa pravnih lica - identifikacija transakcionih aktivnosti subjekata van njihovog deklarisanog ili uobičajenog radnog vremena (npr. transferi velikih iznosa tokom vikenda ili u kasnim noćnim satima kod pravnih lica čiji je profil vezan isključivo za radne dane i standardno radno vrijeme);

-Tranzitni profil (tzv.money mule) kod niskoplatežnih kategorija - detekcija priliva na računima studenata, nezaposlenih lica ili penzionera tokom neradnih dana ili u ranim jutarnjim časovima, nakon čega slijedi neposredna disperzija sredstava (dalji transferi ili podizanje gotovine na ATM-u) u intervalu od nekoliko minuta;

-Geografsko-temporalna neusklađenost (tzv.impossible travel) - detekcija transakcija koje se realizuju u nerealno kratkom vremenskom razmaku na fizički udaljenim lokacijama (npr. plaćanje računa putem mobilne aplikacije iz Crne Gore, a neposredno zatim podizanje gotovine na ATM terminalu u drugoj vremenskoj zoni ili udaljenoj državi).

### 4.2. Tipologije i specifičnosti kontrole transakcija u realnom vremenu (SPN/AF)

U skladu sa članom 49 stav 1 tačka 2, sprovođenje kontrola se prilagođava identifikovanom riziku, uz poseban fokus na mehanizme detekcije „mula" računa koji predstavljaju kritičnu tačku presjeka između prevare i pranja novca, sistem za monitoring treba integrisano alarmirati sljedeće tipologije u realnom vremenu:

- Monitoring brzog protoka sredstava (tzv. pass-through monitoring) - sistem je dizajniran da u realnom vremenu identifikuje situacije u kojima se instant priliv sredstava (npr. iznosi neposredno ispod praga maksimalno dozvoljenog limita po nalogu, poput 2.900 EUR) u kratkom vremenskom intervalu (npr. unutar istog sata) disperzuje kroz više manjih instant odliva ka različitim primaocima. Ovakva dinamika prometa predstavlja primarni indikator za tzv. „mule accounts" (račune mule) koji se koriste kao tranzitne tačke za prikrivanje traga novca. Detekcija ovakvog obrasca ponašanja automatski aktivira mehanizam za momentalno ažuriranje stepena rizika klijenta na „Visok", uz obaveznu restrikciju daljih transakcija do okončanja procesa pojačane provjere (EDD);
- Agregacija sredstava (tzv. "fan-in" / mule aggregation) - identifikacija računa klijenta koji u kratkom vremenskom intervalu (unutar 24 do 48 sati) prima veći broj instant uplata od lica bez prethodne istorije transakcija. Poseban fokus je na prilivima u iznosima neposredno ispod pragova za dubinsku provjeru (smurfing). Ovakav obrazac je primarni indikator investicionih prevara, piramidalnih šema ili funkcije „komandnog računa mula" (tzv. master mule account) u koji se konsoliduju sredstva stečena kriminalnim aktivnostima;
- Disperzija sredstava (tzv. "fan-Out" / layering) - detekcija priliva visoke vrijednosti (često proisteklih iz kompromitacije poslovne e pošte – tzv. (Business Email Compromise-BEC) prevare ili krađe identiteta) koji se odmah po dospijeću disperzuju kroz seriju brzih instant naloga ka većem broju nepovezanih fizičkih lica. Ovakva strategija služi za otežavanje praćenja toka novca u fazi raslojavanja (layering) imovine;
- Sindrom nultog salda (tzv. "useless balance") - indikator u kojem račun klijenta sistematski ne zadržava likvidna sredstva na kraju izvještajnog perioda. Sredstva koja pristignu putem instant kanala se u cjelosti, u roku kraćem od 15 minuta, podižu u gotovini na ATM

uređajima ili prosljeđuju dalje, ostavljajući stanje na računu blizu nule. Ovo ukazuje na isključivo tranzitnu ulogu računa bez stvarne ekonomske svrhe.

### 4.3. Ažuriranje stepena rizika (Član 49 stav 1 tačka 5)

Sistem za automatizovani nadzor mora osigurati neposrednu korelaciju između detektovanih anomalija u instant kanalu i ukupnog profila rizičnosti klijenta. Proces se definiše kroz sljedeće parametre:

- Automatizovana inicijacija revizije - svaki identifikovani alarm visoke kritičnosti (bilo da je SPN/FT ili AF prirode) generisan kroz instant platne kanale, mora automatski inicirati proces vanredne revizije stepena rizika klijenta u bazi podataka obveznika;
- Eskalacija na kategoriju "Visok rizik" - u slučajevima kada sumnjiva instant aktivnost (poput tzv.pass-through prometa ili tzv. impossible travel anomalije) rezultira reklasifikacijom klijenta u kategoriju višeg rizika, obveznik je dužan da, bez odlaganja primijeni mjere pojačanog praćenja iz člana 52 Zakona.
- Integralni pristup poslovnom odnosu – produbljene mjere praćenja ne smiju biti ograničene isključivo na digitalne kanale ili instant transakcije, već se moraju primijeniti na cjelokupan poslovni odnos klijenta. To podrazumijeva pojačani nadzor nad svim transakcijama klijenta, provjeru porijekla imovine i pojačano praćenje svih budućih transakcija putem bilo kojeg distributivnog kanala (npr. šalter, e-banking, ATM).

## 5. PRODUBLJENE MJERE POZNAVANJA I PRAĆENJA KLIJENTA U INSTANT OKRUŽENJU

### 5.1. Specifičnosti kod politički eksponiranih lica (Član 52 i 56 Zakona)

U cilju dosljedne primjene zakonske obaveze utvrđivanja porijekla imovine i sprovođenja produbljenih mjera poznavanja i praćenja transakcija politički eksponiranih lica, obveznik je dužan da u okviru sistema za kontrolu instant plaćanja implementira sljedeće standarde:

- Definisanje očekivanog profila transakcione aktivnosti - kako bi se osigurala efikasnost izvršenja bez ugrožavanja kontrolnih mehanizama, obveznik za svako politički eksponirano lice utvrđuje profil i obim uobičajenih transakcija na osnovu prethodno dokumentovanog i utvrđenog porijekla imovine (shodno članu 56 stav 1 tačka 1). Svaki instant nalog koji radikalno odstupa od uobičajenog intenziteta i obima transakcija, posebno u pogledu neuobičajeno visokog iznosa ka primaocu bez prethodne transakcione istorije, podliježe automatskom zadržavanju realizacije transakcije radi obavezne manuelne verifikacije;
- Detekcija značajnog usitnjavanja transakcija - s obzirom na brzinu instant kanala, sistem mora primjenjivati specifične scenarije koji prate kumulativne iznose u realnom vremenu. Poseban fokus je na detekciji serije instant transakcija srednjih iznosa koje se iniciraju u kratkom vremenskom razmaku ka različitim fizičkim licima (npr. plaćanja navodnih "usluga" ili "konsultacija"). Ovakav obrazac ponašanja, ukoliko nije u skladu sa prijavljenim prihodima i prirodom posla politički eksponiranog lica, sistem mora prepoznati kao pokušaj prikrivenog transfera sredstava (tzv. fragmented laundering) i blokirati do pojašnjenja svrhe transakcija.

### 5.2. Postupanje kod složenih i neuobičajenih transakcija (Član 58 Zakona)

U okviru instant platnog sistema, identifikacija neuobičajenih i složenih transakcija vrši se u realnom vremenu primjenom naprednih algoritama koji porede trenutnu aktivnost sa istorijskim profilom klijenta. Obveznik je dužan da obezbijedi sljedeće kontrolne mehanizme:

- Obaveza definisanja internih pragova za kumulativnu aktivnost - obveznik je dužan da internim aktima precizno definiše kvantitativne i kvalitativne pragove za detekciju neuobičajenog intenziteta transakcija. Sistem mora biti kalibrisan da identifikuje visokofrekventna sukcesivna plaćanja, prateći agregaciju iznosa na dnevnom, nedjeljnom i mjesečnom nivou. Neuobičajenim se smatra svako odstupanje koje podrazumijeva naglu akumulaciju vrijednosti kroz realizaciju više instant naloga, čak i kada su pojedinačni nalozi unutar dozvoljenog limita, ukoliko takva dinamika nije u skladu sa najavljenim ili istorijskim prometom po računu.
- Režim monitoringa tokom vikenda i van radnog vremena - obveznik je dužan da specifikuje pragove materijalnosti za transakcije koje se realizuju u periodima smanjenog operativnog nadzora (vikendi, državni praznici i radni dani van standardnog radnog vremena). Svaka aktivnost velikog obima u ovim terminima, koja značajno odstupaju od prethodnih transakcionih navika klijenta, mora biti tretirana kao neuobičajena. Internim procedurama se moraju odrediti tačni iznosi i frekvencija koji se smatraju anomalijom u ovim specifičnim vremenskim okvirima, uz obaveznu primjenu automatskih preventivnih restrikcija;
- Sistemska evidencija i dokumentovanje neuobičajenih i složenih transakcija (član 58 Zakona) - za svaku identifikovanu neuobičajenu ili složenu instant transakciju, obveznik je dužan da formira i čuva evidenciju u formi elektronskog izvještaja. Ovaj izvještaj treba biti strukturiran na način da se tehnički i operativni podaci (sistemski generisani) automatski arhiviraju (podaci o digitalnom otisku uređaja, IP adresi inicijatora, geografskoj lokaciji, odstupanju od uobičajenog vremena i intenziteta, opis algoritamske anomalije koja je aktivirala alarm).
- Analiza i zaključak Ovlašćenog lica za SPN/FT - Ovlašćeno lice za SPNFT dužno je da u izvještaju navede obrazložen zaključak zasnovan na sprovedenoj analizi. Zaključak mora jasno definisati razloge zbog kojih transakcija nije eskalirala ka Finansijsko-obavještajnoj jedinici, usljed dokazane ekonomske opravdanosti i otklonjene sumnje, ili razloge zbog kojih je ista kvalifikovana kao sumnjiva i proslјeđena kao sumnjiva transakcija. Evidencija mora biti dostupna nadležnom organu u cilju dokazivanja kvaliteta procesa analize neuobičajenih transakcija.

### 5.3. Produbljene mjere poznavanja i praćenja klijenata povezanih sa visokorizičnim trećim državama (Član 59 Zakona)

Iako je sistem instant plaćanja primarno ograničen na domaći platni promet, obveznik je dužan da identifikuje i minimizira rizike koji se odnose na klijente čije je porijeklo, sjedište ili poslovanje povezano sa visokorizičnim trećim državama. Navedene kontrole imaju za cilj ublažavanje rizika da nerezidentna lica pod pojačanim nadzorom koriste brzinu i efikasnost domaćeg instant kanala za operativne faze pranja novca ili finansiranje terorizma unutar Crne Gore čime bi se prikrilo stvarno porijeklo i krajnja destinacija sredstava, te se u skladu sa tim preporučuju sljedeći standardi:

- Obveznik je dužan da primjenjuje produbljene mjere praćenja kontrole realizacije svih instant transakcija unutar Crne Gore ukoliko je nalogodavac, primalac ili stvarni vlasnik klijenta povezan sa visokorizičnom trećom državom;
- Obveznik je dužan da za ovu kategoriju klijenata, obezbijedi da sistem za monitoring transakcija mora generisati alarme na iznosima koji su značajno niži od standardnih parametara. Cilj je preventivno djelovanje protiv metoda raslojavanja sredstava koja su prethodno transferisana u domaći finansijski sistem iz visokorizičnih jurisdikcija;
- Uspostavi sistemske restrikcije, shodno članu 59 stav 2, obveznik je dužan da predvidi mogućnost automatskog ograničavanja broja i ukupnog dnevnog/nedjeljnog volumena instant transakcija za klijente povezane sa visokorizičnim trećim državama. Ovim se visokorizični klijenti usmjeravaju na standardne platne kanale koji omogućavaju detaljnu provjeru prateće dokumentacije u realnom vremenu;
- Za klijente povezane sa visokorizičnim trećim državama, obveznik je dužan da sprovodi češću analizu svih izvršenih instant naloga (tzv. post-transaction review). Umjesto standardnih periodičnih kontrola, ovaj režim omogućava blagovremeno uočavanje atipičnih obrazaca koji mogu ukazivati na finansiranje terorizma ili šeme pranja novca.

### 5.4. Integracija produbljenih mjera u IT arhitekturu sistema za prepoznavanje i prevenciju prevarnih aktivnosti i sistema za sprječavanje pranja novca i finansiranja terorizma

Obveznici su dužni da implementiraju produbljene mjere na način koji obezbjeđuje maksimalnu prohodnost instant transakcija, uz očuvanje integriteta sistema kontrole istih. Kako bi se izbjeglo neopravdano odbijanje transakcija i generisanje prekomjernog broja lažnih alarma, primjenjuju se sljedeći mehanizmi:

- Hibridni model monitoringa (tzv. post-execution enhanced monitoring) - u situacijama kada produbljena provjera osnova ili porijekla sredstava (shodno Članu 58 stav 1 tačka 3) zahtijeva analizu koja prevazilazi tehnički okvir od 10 sekundi, a transakcija ne aktivira kritične stop-indikatore (kao što su indikatori neuobičajenih, složenih ili sumnjivih transakcija, pozitivno poklapanje klijenta sa sankcionim listama ili indikatori prevarnih šablona), obveznik primjenjuje hibridni pristup. Transakcija se realizuje uz istovremeno generisanje naloga za prioritetni ex-post nadzor. Obveznik je dužan da ovu analizu finalizuje u najkraćem mogućem roku, a najkasnije do kraja istog radnog dana, čime se postiže balans između zakonske usklađenosti i brzine sistema.
- U cilju smanjenja broja neopravdanih zastoja, IT sistemi moraju biti kalibrisani tako da razlikuju niskorizična plaćanja (npr. plaćanja provjerenim pravnim licima, komunalne usluge, interni transferi) od visokorizičnih indikatora koji su prethodno navedeni. Sistem mora omogućiti dinamičko prilagođavanje parametara kako bi se fokus kontrole usmjerio isključivo na anomalije, čime se osigurava neometan protok legitimnog platnog prometa.
- Ukoliko obveznik, usljed nemogućnosti prikupljanja neophodnih podataka (npr. klijent ne odgovara na zahtjev za ažuriranje podataka ili dokazivanje porijekla imovine), ne može sprovesti mjere poznavanja i praćenja klijenta, dužan je da primijeni odredbe člana 19 stav 4 Zakona. Umjesto potpunog raskida poslovnog odnosa, obveznik može primijeniti ciljanu deaktivaciju isključivo instant kanala. Ova mjera se koristi kao privremeni zaštitni mehanizam dok se produbljene mjere u potpunosti ne sprovedu, čime se klijent usmjerava na kanale koji dozvoljavaju manuelnu provjeru dokumentacije.

## 6. ZADRŽAVANJE SUMNJIVE TRANSAKCIJE I IZVJEŠTAVANJE U REALNOM VREMENU

### 6.1 Izvještavanje o sumnjivim klijentima i transakcijama u instant okruženju (član 66 Zakona)

Član 66 stav 6 Zakona propisuje striktnu obavezu obveznika da zadrži od izvršenja svaku transakciju za koju postoje osnovi sumnje na pranje novca ili finansiranje terorizma. U instant okruženju, ovaj pravni standard se implementira kroz sljedeće operativne mehanizme:

- Automatski „hold" status - ukoliko sistem detektuje podudaranje sa listom indikatora sumnjivih klijenata i transakcija instant nalog se momentalno suspenduje prije slanja u kliring;
- Obavještavanje o sumnjivom klijentu i transakciji (član 66 stav 7) - podaci o zadržanoj sumnjivoj transakciji moraju biti dostavljeni finansijsko-obavještajnoj jedinici prije njene realizacije. S obzirom na to da operativni prozor instant sistema od 10 sekundi ne ostavlja prostor za manuelno odlučivanje, zadržana transakcija mora automatski dobiti status suspendovane transakcije. Ukoliko pravila platne šeme ne dozvoljavaju produženi status čekanja, transakcija se odbija ka nalogodavcu, dok sredstva na računu ostaju pod nadzorom banke do prijema instrukcija od finansijsko-obavještajne jedinice u skladu sa članom 93 Zakona;
- Obrazloženje nemogućnosti zadržavanja (član 66 stav 8) - u izuzetnim situacijama, ukoliko zbog prirode instant transakcije ili drugih opravdanih razloga obveznik ne uspije da zadrži realizaciju sumnjive transakcije, dužan je da najkasnije sljedećeg radnog dana od dana realizacije transakcije dostavi finansijsko-obavještajnoj jedinici detaljno obrazloženje o razlozima nepostupanja u skladu sa članom 66 stav 6, uz prateće dokaze o sprovedenim mjerama iz člana 117 Zakona.

### 6.2 Naknadno (ex-post) izvještavanje i retrospektivna analiza transakcija u instant okruženju

U specifičnim okolnostima instant platnog prometa, gdje se transakcije izvršavaju u realnom vremenu i neopozivo, obveznik može identifikovati sumnjive obrasce (poput naknadno utvrđene strukturalne agregacije ili primjene novih indikatora na istorijske podatke) tek nakon što su sredstva napustila sistem banke. U tom slučaju, obveznik postupa shodno članu 66 stav 8 Zakona:

- Obaveza hitnog naknadnog izvještavanja - od trenutka kada se kroz naknadnu analizu (ex-post) utvrde osnovi sumnje u vezi klijenta ili realizovane transakcije, obveznik je dužan da bez odlaganja, a najkasnije u roku od 24 sata od realizacije transakcije, dostavi finansijsko-obavještajnoj jedinici naknadni izvještaj o sumnjivoj transakciji. Ovaj izvještaj mora sadržati detaljno obrazloženje razloga zbog kojih transakcija nije mogla biti zadržana u trenutku iniciranja;
- U izvještaju o sumnjivom klijentu i transakciji se obavezno naznačava da su sredstva realizovana putem instant platnog kanala. Obveznik dostavlja i sve raspoložive digitalne metapodatke (IP adrese, digitalni otisak uređaja, precizno vrijeme realizacije, podatke o primaocu isl.), kako bi se omogućilo hitno međuinstitucionalno praćenje traga novčanih sredstava i eventualna blokada sredstava u banci primaoca.

- Sprovođenje retrospektivne analize - identifikacija sumnje na već izvršenim instant nalozima obavezuje ovlašćeno lice da sprovede reviziju cjelokupne transakcione istorije klijenta u određenom periodu (retrospektivna analiza). Cilj je utvrđivanje šireg obrasca sumnjivog ponašanja koji bi mogao zahtijevati dopunu inicijalnog izvještaja o sumnjivoj transakciji i sumnjivom klijentu;
- Primjena restriktivnih mjera na klijenta - odmah po identifikaciji sumnje, a nezavisno od toga što su novčana sredstva kroz instatnt nalog već realizovana, obveznik je dužan da automatski suspenduje pristup kanalu instant plaćanja za tog klijenta. Ova mjera ostaje na snazi do okončanja interne istrage ovlašćenog lica za SPN/FT banke ili prijema obavezujućih instrukcija od strane finansijsko-obavještajne jedinice, čime se spriječava dalji odliv kapitala kroz brze kanale banke.

### 6.3 Režim monitoringa i restrikcija instant naloga van radnog vremena, vikendom i državnim praznicima

U cilju minimiziranja rizika koji su vezani za period smanjenog operativnog nadzora, obveznik je dužan da uspostavi specifičan režim automatizovanog monitoringa koji se aktivira van standardnog radnog vremena, tokom vikenda i državnih praznika. Ovaj sistem funkcioniše na bazi unaprijed definisanih pragova materijalnosti i indikatora sumnjivih klijenata i transakcija:

- Definicija pragova materijalnosti i neuobičajenih aktivnosti – internim procedurama obveznik određuje tačne iznose i frekvenciju transakcija koji se smatraju anomalijom u ovim specifičnim vremenskim okvirima. Svaka aktivnost velikog obima ili učestalosti koja značajno odstupa od prethodnih transakcionih navika klijenta, a realizuje se u terminima odsustva manuelnog nadzora, mora biti tretirana kao neuobičajena i potencijalno sumnjiva;
- Obavezna primjena automatskih preventivnih restrikcija – ukoliko sistem detektuje transakciju koja se podudara sa unaprijed predviđenim indikatorima sumnje ili prelazi definisane pragove materijalnosti van radnog vremena, obveznik je dužan da primijeni mjeru automatskog zaustavljanja realizacije instant transakcije. Ovako zadržana transakcija momentalno dobija status suspendovane i ne može biti izvršena putem automatizovanih kanala plaćanja;
- Manualna autorizacija i procesuiranje – svaka transakcija zaustavljena primjenom automatskih restrikcija van radnog vremena ostaje u statusu suspenzije do prvog narednog radnog dana. Deblokada ili konačno odbijanje ovakve transakcije isključivo je uslovljeno ručnim ovlašćenjem (odobrenjem) ovlašćenog lica za SPN/FT ili njegovog zamjenika, nakon sprovedene analize razloga zaustavljanja i provjere usklađenosti sa odredbama člana 66 Zakona;
- Snižavanje pragova osjetljivosti **-** preporučuje se da banke u svojim internim aktima definišu niže kumulativne limite za instant plaćanja tokom noćnih sati i vikenda, kako bi se smanjila potencijalna šteta u slučaju masovnih prevarnih aktivnosti ili pranja novca.

### 6.4 Definisanje sopstvene liste indikatora za prepoznavanje sumnjivih klijenata i transakcija u instant okruženju (Član 83 Zakona)

Shodno zakonskoj obavezi, obveznik je dužan da izradi sopstvenu listu indikatora za prepoznavanje sumnjivih klijenata i transakcija, specifično prilagođenu instant platnim kanalima. Ovi indikatori moraju biti integrisani u sistem za nadzor i obuhvatiti najmanje sljedeće oblasti:

- Strukturne anomalije priliva i odliva (fan-in / one-out) - obrazac koji prati akumulaciju sredstava od više nepovezanih lica ka jednom računu, nakon čega slijedi hitna disperzija ili podizanje gotovine.
- Brzi odliv sredstava (rapid outflow) - indikator koji prepoznaje situacije u kojima se sredstva zadržavaju na računu u ekstremno kratkom intervalu (npr. manje od 5 minuta) prije daljeg transferisanja;
- Reaktivacija pasivnih računa (dormant account activation) - iznenadno korišćenje instant kanala na računima koji su duži period bili neaktivni ili su imali minimalan promet.
- Geografsko-vremenska odstupanja (impossible travel / geo-fencing) - logička neusklađenost mjesta i vremena iniciranja naloga, kao i pristup aplikaciji sa IP adresa iz visokorizičnih jurisdikcija;
- Učestala sukcesivna plaćanja (velocity / smurfing) - serija naloga neposredno ispod pragova izvještavanja, inicirana u kratkim razmacima u cilju izbjegavanja detekcije;
- Biometrijska odstupanja uređaja digitalni otisak uređaja (device fingerprinting) - iniciranje transakcija sa novih, neprovjerenih uređaja ili putem neadekvatnih virtuelizovanih okruženja( emulatora), što ukazuje na automatizovane napade ili neovlašćeno preuzimanje korisničkog naloga klijenta (account takeover).

### 6.5. Preporuke za uspostavljanje mehanizma opoziva sumnjivih transakcija (recall)

S obzirom na neopozivost instant naloga u okviru standardne platne šeme, obveznik bi trebalo da teži uspostavljanju tehničkih i operativnih rješenja koja omogućavaju korektivno djelovanje u situacijama kada se sumnja na PN/FT identifikuje neposredno nakon realizacije transakcije. U tom smislu, preporučuje se implementacija sljedećih mehanizama:

- Tehnička mogućnost opoziva (SPN/FT/AF recall) - obveznik bi trebalo da osigura tehničke preduslove za slanje hitnih međubankarskih poruka ili sigurnih komunikacionih kanala sa zahtjevom za blokadu ili povraćaj novčanih sredstava. Takav zahtjev bi se inicirao u slučajevima kada ex-post analiza ili prijava prevare ukažu na visok rizik, sa ciljem da se banka primaoca upozori na sumnjivu prirodu priliva prije nego što sredstva budu dalje disperzovana;
- Paralelno izvještavanje i koordinacija - u trenutku iniciranja zahtjeva za opoziv ka drugoj banci, obveznik bi trebalo da uputi Izvještaj o sumnjivoj transakciji finansijsko-obavještajnoj jedinici. U samoj prijavi sumnje obavezno se navodi detaljna informacija o pokrenutom recall protokolu, čime se omogućava hitna međuinstitucionalna koordinacija i daje pravni osnov finansijsko-obavještajnoj jedinici da hitno interveniše prema banci primaoca radi privremenog zaustavljanja daljeg odliva sredstava;
- Preporučuje se definisanje protokola po kojem bi banka, u svojstvu pošiljaoca, u najkraćem roku kontaktirala dežurne službe banke primaoca. Cilj je da se, na bazi uzajamne obaveze sprječavanja kriminalnih aktivnosti, omogući privremeno zadržavanje sredstava na računu primaoca do dobijanja zvanične naredbe finansijsko-obavještajne jedinice shodno članu 93 Zakona.

## 7. SPECIFIČNOSTI SPRJEČAVANJA FINANSIRANJA TERORIZMA U INSTANT PLATNOM SISTEMU

### 7.1. Monitoring mikro-obrazaca i detekcija prikupljanja sredstava (fan-in pattern)

Iako su instant nalozi ograničeni na nacionalni platni promet Crne Gore, njihova brzina i dostupnost (24/7) predstavljaju potencijalni rizik za fazu prikupljanja sredstava namijenjenih finansiranju terorizma. Obveznik je dužan da implementira specifične scenarije monitoringa fokusirane na:

- Agregacija malih iznosa – automatski sistem mora prepoznati i automatski označiti račune koji primaju mnoštvo mikro-uplata (npr. od 5 EUR do 50 EUR) od strane velikog broja različitih fizičkih lica u kratkom vremenskom intervalu. Fokus je na identifikaciji primaoca koji služi kao čvorište (hub) za akumulaciju legalno stečenih sredstava koja, u zbiru, formiraju značajan kapital za dalje sumnjivo usmjeravanje.
- Zloupotreba neprofitnog sektora i udruženja (NPO indikatori) - poseban nadzor postavlja se na račune neprofitnih organizacija i udruženja koja koriste instant kanale za hitno prikupljanje donacija. Kritični indikatori uključuju atipičnu frekvenciju priliva (iznenadni talas mikro-uplata vikendom ili tokom globalnih kriza) i povezane nalogodavce (identifikacija grupa koje sinhronizovano vrše uplate, često sa istih IP adresa ili uređaja);
- Obveznik je dužan da definiše sopstvene liste indikatora za prepoznavanje sumnjivih klijenata i transakcija u instant okruženju u vezi sa sprečavanjem finansiranja terorizma u skladu sa članom 83 Zakona.

### 7.2. Detekcija prekograničnog odliva kroz konverziju u digitalnu imovinu i platforme za digitalne donacije

S obzirom na to da su instant transakcije ograničene na domaću jurisdikciju, sistem monitoringa mora pratiti lanac transakcija koji slijedi neposredno nakon akumulacije sredstava na domaćem računu:

- Hibridni monitoring (instant-to-crypto/global) - obveznik postavlja indikatore sumnje na klijente koji, nakon serije primljenih instant mikro-uplata, vrše hitno usmjeravanje tih sredstava (često u roku kraćem od 24h) putem deviznih naloga ili platnih kartica ka međunarodnim berzama virtuelne imovine (VASP platforme), globalnim platformama za grupno finansiranje (Crowdfunding) i digitalne donacije, provajderima digitalnih novčanika koji omogućavaju dalju anonimizaciju traga novca;
- Identifikacija situacija gdje klijent prima veći iznos sredstava sa inostranih platformi, a potom ta sredstva u realnom vremenu (instant) disperzuje na veći broj računa fizičkih lica u Crnoj Gori, što može ukazivati na operativno finansiranje lokalnih ćelija ili radikalizovanih pojedinaca.

### 7.3. Provjera prema listama sankcija i sistem za preventivnu zaštitu integriteta platnog prometa

U domenu sprečavanja finansiranja terorizma, brzina reakcije je ključna zbog neopozivosti instant naloga:

- Svaki nalogodavac i primalac u domaćem instant platnom sistemu mora proći automatizovanu provjeru prema nacionalnim i međunarodnim listama sankcija (UN, EU) prije nego što nalog uđe u kliring;
- Re-screening i ažurnost - obveznik je dužan osigurati implementaciju izmjena u listama sankcija u roku od 60 minuta, a ne kasnije od 24 časa od momenta izmjene relevantnih lista, kako bi se spriječilo da sankcionisano lice iskoristi 24/7 dostupnost sistema prije ažuriranja baze klijenata banke u odnosu na relevantne sankcione liste;
- Operativni sistem za preventivnu zaštitu integriteta platnog promet („Kill-switch“) mehanizam - u situacijama visoke bezbjednosne situacije (npr. objave novih međunarodnih sankcija velikog obima ili prepoznavanja koordinisanog mrežnog napada na sistem banke ili finansijski sitem u cjelini), obveznik mora imati mogućnost da aktivira protokol za hitno suspendovanje instant kanala za specifične grupe klijenata ili kategorije transakcija. O aktivaciji ovog mehanizma obveznik momentalno obavještava finansijsko-obavještajnu jedinicu i Centralnu banku Crne Gore, uz dostavljanje detaljnog obrazloženja o razlozima hitne obustave, čime se obezbjeđuje osnov za privremeno neizvršavanje obaveza iz instant platnog prometa.

## 8. OPERATIVNA KONVERGENCIJA: INTEROPERABILNOST ANTI FRAUD I SPN/FT SEKTORA BANKE

8.1 Uvođenje kanala instant plaćanja, zbog svoje brzine i nepovratnosti sredstava, imperativno zahtijeva brisanje operativnih silosa između odjeljenja zaduženih za prevenciju prevarnih aktivnosti (IT/Anti-Fraud) i odjeljenja za SPN/FT banke. Preporučuje se uspostavljanje integrisanog pristupa kroz sljedeće mehanizme:

- Jedinstveni profil rizika i korelacija podataka – obveznik uspostavlja sistem u kojem zaključci Anti-Fraud (AF) sektora o sumnji na kompromitaciju klijentovog uređaja, „phishing“ napade ili aktivnosti „money mule“ (novčanih mula) automatski postaju integralni dio SPN/FT profila klijenta. Banka ne smije dozvoliti izolovanu obradu incidenata; svaka detekcija prevare na digitalnom kanalu mora inicirati trenutnu provjeru klijenta sa aspekta sprječavanja pranja novca i finansiranja terorizma, sprečavajući situacije u kojima se klijent tretira isključivo kao žrtva prevare dok se istovremeno omogućava nesmetan protok sumnjivog kapitala bez produbljene analize.
- Praćenje vođeno događajima podrazumijeva da svaki bezbjednosni incident, prijava prevarnih aktivnosti od strane klijenta ili treće strane, kao i svaka privremena blokada inicirana od strane nadležnog organa, predstavlja „okidač“ koji automatski pokreće postupak vanredne, produbljene provjere klijenta. Ovaj mehanizam osigurava da se klijentov profil rizika ažurira u realnom vremenu na osnovu konkretnih operativnih saznanja, a ne samo u periodičnim ciklusima;
- Interoperabilnost podrazumijeva da digitalni metapodaci prikupljeni od strane AF sektora (IP adrese, digitalni otisak uređaja – device fingerprint, geo-lokacija) moraju biti dostupni ovlašćenom licu za SPN/FT prilikom analize neuobičajene, složene ili sumnjive transakcije . Ova sinergija omogućava bržu identifikaciju mreža povezanih lica koje koriste brzinu instant sistema za koordinisano izvlačenje sredstava ili finansiranje nedozvoljenih aktivnosti.

## 9. POSTUPANJE PO NALOZIMA NADLEŽNIH ORGANA I KONTINUIRANO PRAĆENJE

### 9.1. Naredba o privremenoj obustavi transakcija (Član 93 i 94 Zakona)

Shodno **članu 93**, obveznik je dužan da bez odlaganja postupi po naredbi finansijsko-obavještajne jedinice o obustavi izvršenja transakcije. U ambijentu instant plaćanja, ovaj proces se operacionalizuje na sljedeći način:

- Hitno postupanje po usmenoj naredbi (član 93 stav 7 i 8) - zbog brzine instant transakcija kreditna institucija je dužna da obezbijedi realizaciju momentalne tehničke blokade kanala po prijemu poziva, dok ovlašćeno lice bez odlaganja sačinjava službenu zabilješku, uz obavezu prijema pisane/elektronske potvrde naredbe u roku od 24 časa;
- Prestanak mjere obustave izvršenja transakcije (član 94) - ako po isteku zakonskog roka od 72 časa (ili produženog roka) ne stigne obavještenje o daljem postupanju, sistem aktivira protokol za deblokadu sredstava, čime se eliminiše rizik od regulatorne neusklađenosti prema klijentu.

### 9.2. Kontinuirano praćenje finansijskog poslovanja (član 95)

Na osnovu zahtjeva finansijsko-obavještajne jedinice za kontinuiranim praćenjem klijenta (koje može trajati do 6 mjeseci), obveznik prilagođava instant platni sistem sljedećim mehanizmima:

- Izvještavanje prije izvršenja (stav 3) - za klijente pod mjerom kontinuiranog praćenja, obveznik postavlja sistemski „marker“ koji svaku iniciranu instant transakciju stavlja u status privremenog zadržavanja radi dostavljanja podataka finansijsko-obavještajnoj jedinici prije finalne realizacije instant naloga, uz navođenje procjene roka izvršenja;
- Ex-post izvještavanje i obrazloženje (stav 4 i 5) - ako zbog specifične prirode instant naloga (automatizam i brzina od 10 sekundi) ili realizacije van radnog vremena obveznik nije mogao postupiti preventivno, dužan je da podatke dostavi bez odlaganja, a najkasnije sljedećeg radnog dana. U ovom slučaju, obveznik dostavlja detaljno obrazloženje o tehničkim razlozima nemogućnosti zadržavanja instant transakcije u realnom vremenu.

### 9.3. Operativna i sistemska spremnost banke na zahtjeve nadležnih organa u režimu 24/7

Shodno članu 11 stav 1 tačka 9 Zakona, obveznik je dužan da uspostavi i kontinuirano prati funkcionisanje sistema koji omogućava potpun i blagovremeno dostupan odgovor na zahtjeve finansijsko-obavještajne jedinice i drugih nadležnih organa.

- U kontekstu instant platnog prometa, ova zakonska obaveza se operacionalizuje tako što obveznik implementira tehničko rješenje koje omogućava da se naredbe o privremenom obustavljanju transakcija (shodno članu 93) izvrše bez odlaganja. Sistem se postavlja tako da omogućavajući da se tehnička blokada računa ili specifičnog digitalnog kanala sprovede u realnom vremenu po prijemu naloga od nadležnog državnog organa;
- Kontinuirano praćenje funkcionalnosti sistema (24/7) - kako bi se osigurala potpuna usklađenost sa zakonom, sistem za prihvat i obradu zahtjeva nadležnih organa mora biti funkcionalan neprekidno. Obveznik obezbjeđuje da tehnički protokoli za blokadu sredstava budu dostupni i van radnog vremena, vikendom i praznicima, čime se sprječava rizik da klijent iskoristi brzinu instant plaćanja prije nego što banka odgovori na zahtjev organa;

- Sveobuhvatnost odgovora i digitalni dokazi - obaveza potpunog odgovora iz člana 11 podrazumijeva da banka, osim obustave realizacije transakcije I kontinuiranog praćenja poslovanja klijenta, na zahtjev nadležnog organa hitno dostavlja i sve prateće podatke definisane članom 117 Zakona;
- Ovlašćeno lice za SPN/FT dužno je da redovno prati i testira efikasnost ovih sistema, osiguravajući da automatizovani procesi i dežurni protokoli komunikacije sa finansijsko-obavještajnom jedinicom garantuju izvršenje naredbi u rokovima koji ne ugrožavaju svrhu hitne obustave transakcija I kontinuiranog praćenja klijenta.

## 10. STRUČNO OSPOSOBLJAVANJE I USAVRŠAVANJE ZAPOSLENIH

### 10.1. Programi obuke prilagođeni instant okruženju (Član 78)

Shodno **članu 78 Zakona o SPNFT**, obveznik je dužan da obezbijedi redovno stručno osposobljavanje i usavršavanje svih zaposlenih koji učestvuju u procesima sprječavanja i otkrivanja PN/FT. Uvođenje instant plaćanja zahtijeva nadogradnju standardnih programa obuke specifičnim modulima:

- Prepoznavanje tipologija u realnom vremenu - edukacija o novim metodama pranja novca i finansiranja terorizma karakterističnim za instant kanale, kao što su npr. "money mule" mreže, zloupotreba brzine transfera za brzo iznošenje kapitala na eksterne platforme isl.
- Simulacije incidentnih situacija - praktične vježbe postupanja u uslovima vremenskog pritiska, sa fokusom na donošenje odluka o blokadi ili realizacije transakcija u roku od nekoliko minuta, kao i postupanje po hitnim usmenim naredbama nadležnih organa;
- Razumijevanje značaja metapodataka (IP adrese, VPN korelacije, Device ID) u procesu analize sumnjivih obrazaca i šema. Obuka mora osigurati da zaposleni u sektoru SPN/FT mogu efikasno tumačiti tehničke logove u bliskoj saradnji sa IT i Anti-Fraud odjeljenjima.

### 10.2. Obuhvat i planiranje obuka (Član 78 stav 2 i 3)

U skladu sa zakonskim zahtjevima, program usavršavanja obuhvata:

- Upoznavanje zaposlenih sa listama indikatora sumnjivih transakcija (čl. 82 i 83), te internim procedurama koje regulišu rad u režimu 24/7;
- Obuka se obavezno proširuje na zaposlene koji su u direktnom kontaktu sa klijentima, radi prepoznavanja obrazaca socijalnog inženjeringa (phishing, vishing isl.) koji često prethode instant transakcijama povezanim sa pranjem novca.

### 10.3. Vanredne obuke i kontinuirano usavršavanje

S obzirom na visok stepen inovativnosti u metodama kriminalnih aktivnosti unutar instant šema, obveznik uvodi mehanizam **ad-hoc obuka**:

- U slučaju identifikacije nove tipologije prevare ili pranja novca specifične za domaći instant platni sistem, ovlašćeno lice je dužno da sprovede vanrednu obuku relevantnih zaposlenih u roku od 48 sati od detekcije negativnih obrazaca;
- Ovaj mehanizam osigurava da operativni timovi budu trenutno informisani o novim indikatorima, čime se minimizuje rizik od sistemskog propusta tokom neradnih dana.

- Obveznik vodi preciznu evidenciju o svim sprovedenim obukama, testovima znanja i prisustvima.

**Prilog A: Indikatori rizika za CEF (Cyber-Enabled Fraud) u instant okruženju**

Postojanje pojedinačnog indikatora ne mora nužno značiti prevarne aktivnosti i sa njim povezeane aktivnosti pranja novca i finansiranja terorizma ali u kontekstu instant plaćanja, ovi slučajevi zahtijevaju pojačanu pažnju odgovornih lica u instituciji.

**1. Indikativni obrasci transakcija**

1. Visoka frekfencija ili neposredna realizacija transakcije (visoke ili niske vrijednosti) odmah nakon otvaranja računa, koje nisu u skladu sa svrhom računa;
2. Brzo podizanje gotovine ili transferi značajnih iznosa odmah nakon priliva sredstava kako bi se račun ispraznio ("cash-out");
3. Česte transakcije u iznosima koji ne odgovaraju ekonomskom profilu klijenta (npr. iznenadni međunarodni transferi, transferi ka visokorizičnim jurisdikcijama ili transakcije putem platnih kartica na inostranim ATM uređajima, plaćanje u korist nelicenciranih inostranih platnih institucija, značajne kupovine virtuelne imovine nakon realizovanih instant plaćanja) ;
4. Izvršenje transakcije male vrijednosti (testna transakcija), nakon koje u kratkom vremenskom intervalu slijede uplate znatno većih iznosa istom primaocu;
5. Kupovine u zaokruženim iznosima koje su česte ili značajne u okruženju instant plaćanja (može ukazivati na kupovinu poklon kartica).

**2. Indikativne instrukcije i ponašanje klijenta**

1. Ponovljeni zahtjevi za plaćanje neposredno nakon uspješno izvršene transakcije u korist primaoca sa kojim klijent ranije nije imao poslovnu saradnju.
2. Instrukcije klijenta koje odstupaju od ranije verifikovanih obrazaca u pogledu jezika, stila pisanja, vremena slanja ili uobičajenih iznosa realizovanih transakcija;
3. Odstupanje u podacima o računu primaoca (IBAN) u odnosu na prethodno korišćene podatke za istog primaoca;
4. Neslaganje između naziva primaoca u opisu i stvarnog vlasnika računa u banci primaoca;
5. Nalozi fizičkih lica bez adekvatnog finansijskog iskustva u korist subjekata uz navođenje investicionih proizvoda kao svrhe plaćanja (npr. penzioneri ili osobe mlađeg doba iniciraju transfere ka licima koji nude nerealne profite i po indikativnim osnovama/ulog radi brzog profita);
6. Iniciranje instant naloga sa lokacija koje su fizički previše udaljene da bi klijent mogao biti prisutan na obje (npr. prijava iz Crne Gore, praćena nalogom sa IP adrese iz druge vremenske zone u razmaku od nekoliko minuta), što predstavlja primarni alarm za tzv. Account Takeover (ATO) i neovlašćeno raspolaganje sredstvima - geografski i biometrijski nesklad (Impossible Travel);
7. Odstupanje u vremenskoj zoni uređaja (device time zone mismatch) sa kojeg se inicira nalog u odnosu na geografsku lokaciju klijenta;

**3. Sumnja u validnost klijentskog profila i identiteta korisnika**

1. Klijent izbjegava ili nije u mogućnosti da pruži podatke u okviru mjera poznavanja klijenta (CDD);

2. Klijent ne posjeduje adekvatna saznanja o izvoru sredstava ili navodi da vrši transakcije u ime trećeg lica;
3. Indikatori potencijalne krađe identiteta klijenta su korišćenje zajedničkih, falsifikovanih ili otuđenih identifikacionih podataka (broj telefona, e-mail adresa);
4. Učestale promjene kontakt podataka klijenta neposredno nakon uspostavljanja poslovnog odnosa;
5. Anomalije u online ponašanju kao što su neobična dinamika unosa podataka, kašnjenje pri kucanju (keystroke delays), indikatori automatizacije (botovi) ili višestruki neuspješni pokušaji prijave;
6. Nedostatak osnovnih saznanja klijenta o prirodi, predmetu, iznosu ili svrsi transakcije (ili poslovnog odnosa), uz pružanje nerealnih, kontradiktornih ili konfuznih obrazloženja, što ukazuje na sumnju da klijent djeluje kao posrednik u transferu nelegalnih sredstava (finansijska mula);
7. Više IP adresa ili uređaja povezanih sa jednim nalogom, ili jedna IP adresa povezana sa mnogo različitih korisnika;
8. Pristup nalogu putem Remote Desktop aplikacija (npr. TeamViewer), što sprečava uvid u stvarnu lokaciju.

**4. Negativne informacije o klijentu**

1. Postojanje zahtjeva za povrat sredstava (recall) uslijed sumnje na prevaru od strane druge kreditne institucije;
2. Relevantne negativne informacije iz javno dostupnih izvora o klijentu ili saugovorniku (npr. klijent identifikovan kao prethodna žrtva prevare ili "mula").

**Prilog B: Najbolje prakse za konvergenciju Anti-Fraud (AF) i SPN/FT funkcija**

Ovaj prilog objedinjuje primjere dobre prakse o tome kako finansijske institucije mogu efikasno integrisati funkcije sprečavanja prevara (Anti-Fraud – AF) i sprečavanja pranja novca i finansiranja terorizma (SPN/FT). U kontekstu instant plaćanja, tradicionalni silosi između ovih sektora postaju prepreka brzoj reakciji, zbog čega je uspostavljanje sinergije između AF i AML okvira ključno za očuvanje integriteta platnog sistema. Cilj ovih praksi je stvaranje holističkog pristupa identifikaciji i suzbijanju finansijskog kriminala, gdje se podaci iz AF sistema koriste kao kritičan input za SPN/FT monitoring i obrnuto.

1. Uspostavljanje rigoroznih procesa identifikacije klijenta (KYC) ili procesa provjere poslovnih partnera (Know-Your-Business), implementacija biometrijskih karakteristika tokom procesa digitalnog zasnivanja poslovnog odnosa (on-boarding) i identifikacija jednog mobilnog ili sigurnog uređaja za autentifikaciju transakcija putem elektronskog bankarstva (dok se drugi uređaji blokiraju ili podliježu mjerama pojačanog ublažavanja rizika);
2. Uvođenje perioda mirovanja (cooling-off period) prilikom prve aktivacije usluga elektronskog bankarstva ili sigurnih uređaja (tj. pun spektar bankarskih usluga nije odmah dostupan po otvaranju računa), uz ograničavanje broja ili vrijednosti finansijskih transakcija klijenta;
3. Razvijanje standarda očekivanih i uobičajenih transakcija klijenta (broj transakcija, iznosi, vrste saugovornika, uključene zemlje) radi lakše detekcije sumnjivih transakcija, kao i pooštravanje pravila i okidača za detekciju prevara u cilju preventivnog blokiranja nedozvoljenih transakcija;

4. Korišćenje servisa za verifikaciju primaoca (verification of payee), koji nalogodavcu/platiocu/ omogućavaju da provjeri da li se primalac/povjerilac naveden u platnim porukama podudara sa nazivom vlasnika računa;
5. Razvijanje analitičkog modela koji mapira odnose između računa unutar banke. Ako više računa iznenada šalje sredstva na isti "novi" račun koji je otvoren u kratkom vremenskom periodu, to ukazuje na koordinisanu "mule" mrežu (tzv. money mule ring detection), što omogućava preventivno blokiranje svih povezanih transakcija;
6. Svođenje komunikacije putem elektronske pošte i društvenih mreža sa klijentima isključivo na opšte informacije, uz izričito navođenje da se identifikacioni ili lični podaci ne smiju razmjenjivati sa finansijskom institucijom putem elektronske pošte;
7. Zahtijevanje mehanizama višefaktorske autentifikacije za verifikaciju klijenata i izvršenje finansijskih transakcija, kao i za dodavanje ili aktivaciju primaoca putem različitih kanala;
8. Autentifikacija identiteta korisnika tokom daljinskog podešavanja i sprječavanje kriminalaca da steknu pristup višestrukim računima korišćenjem podataka o računima „finansijskih mula“ ili žrtava putem:
   -Unapređenja pouzdanosti procesa identifikacije klijenata kroz testove živosti (tj. osiguranje da je riječ o živom i stvarnom licu), uključujući provjeru da li je pojedinac izložen socijalnom inženjeringu tokom testova živosti; ili
   -Monitoringa IP adresa koje se koriste za povezivanje sa web sajtovima za elektronsko bankarstvo i sl., uključujući detekciju korišćenja alata za udaljeni pristup (Remote Access Tools);
9. Proširenje vrsta podataka koje obveznici prikupljaju i analiziraju o klijentima, uključujući brojeve mobilnih telefona, IP adrese, GPS koordinate, ID uređaja itd. U svrhe prevencije prevara, finansijske institucije bi mogle ponoviti navedene identifikacione provjere primjenom pristupa zasnovanog na riziku (npr. sprovođenje provjera kada se detektuje indikativno ponašanje);
10. Implementacija sistema za monitoring transakcija u realnom vremenu zasnovanog na riziku, kako bi se osiguralo da se svaka abnormalna aktivnost može brzo detektovati, istražiti i, gdje je relevantno, prijaviti podnošenjem izvještaja o sumnjivoj transakciji**.**

**Sofisticiranost sistema za AF/SPN/FT monitoring treba da bude srazmjerna obimu instant transakcija koje finansijska institucija realizuje.**