Finanspolisen informerar

FINANSIELLA FLÖDEN & PENNINGTVÄTT I NÄTVERKSMILJÖER • NOVEMBER 2023

Få nätverkskriminella misstankerapporteras

Med anledning av den pågående våldsvågen vill Finanspolisen uppmärksamma verksamhetsutövare på ett antal modus och finansiella kännetecken bland nätverkskriminella som kan indikera misstänkt brottlighet på bankkonton.[1]

En genomgång visar att en stor del av aktörerna inte tidigare har varit föremål för misstankerapportering till Finanspolisen trots att de ägnar sig åt penningtvätt. Nätverksaktörernas transaktionsmönster har inte alltid fångats i transaktionsövervakningen och föranlett en djupare granskning. För att upptäcka och stoppa penningtvätt i nätverksmiljöer behöver det proaktiva arbetet ytterligare förstärkas.

Centrala aktörer lämnar inga egna avtryck

Erfarenheter har visat att de mer centrala och etablerade aktörerna i nätverken sällan lämnar spår efter sig i form av transaktioner i eget namn för medel hänförliga till någon form av brottslig verksamhet. Däremot kan de använda sig av anhöriga eller andra bulvaner för att ta emot brottsvinster eller nyttja bankkonton för skiktning av medel. Aktörer i nätverkens periferi, ofta yngre personer under 25 år har däremot större benägenhet att genomföra transaktioner i eget namn där pengarnas ursprung kan ifrågasättas då merparten saknar regelbunden inkomst.

För att hitta aktörer som nyttjar det finansiella systemet, direkt eller indirekt genom målvakter eller bulvaner, behövs ett proaktivt arbete baserat på annan information än enbart transaktionsövervakningen. Ett led i arbetet kan exempelvis vara att ta del av och läsa domar eller annan öppen information för att på så sätt härleda aktörer som förekommer i kundbasen. En fördjupad granskning kan påvisa om aktören ska hanteras i bankens eget förebyggande arbete och misstankerapporteras till Finanspolisen.

Snabba förflyttningar

Ett av de mer typiska kännetecken på aktörernas bankkonton är hög omsättning av medel, främst avseende överföringar via Swish och ofta med ett stort antal motparter, såväl vid in- som utgående transaktioner. Beloppen är jämna och sällan högre än 5 000 kr. Inkomna medel står inte i paritet till taxerad inkomst eller uppgifter om inkomster som uppgetts i kundkännedomen. Trots höga transaktionsflöden, i flera fall uppåt en miljon kronor årligen, är kontobehållningen låg.

De snabba förflyttningarna av medel mellan olika parter är troligen ett led i en penningtvätt och ett sätt att försvåra spårning av pengarnas ursprung. Kontantuttag i samband med överföringarna är relativt vanligt och är troligen ett sätt att bryta spårbarheten av medel i omlopp.

Andra vanliga kännetecken

- *Resekostnader:* Trots inga eller låga inkomster förekommer resekostnader frekvent, främst för flyg och hotell, ofta till Spanien, Turkiet eller Förenade Arabemiraten. I vissa fall syns inga levnadskostnader utomlands trots tidigare köp av flygbiljett och hotell. Det förekommer även att aktörer har levnadskostnader utomlands men transaktioner för köp av flygbiljett och hotell saknas. Det indikerar att de antingen använder kontanta betalmedel för levnadskostnader utomlands eller att resorna emellanåt bekostas av andra inom nätverket.

[1] Privata transaktionskonton

- *Lyxkonsumtion:* Köp av dyrare varor förekommer där inkomna medel, främst från andra privatpersoner, bekostar en vara av dyrare karaktär, antingen i Sverige eller utomlands. Emellanåt förekommer återköp av varor köpta i Sverige, vilket kan tyda på penningtvätt där varor köps för kontanta medel med brottsligt ursprung och återköp istället görs till konto.

- *Färdmedel:* Kostnader för taxi och hyra av elsparkcyklar är relativt vanligt. Likaså nattklubb- och restaurangkostnader. Utgifterna bekostas i huvudsak med överföringar från andra privatpersoner eller kontanta insättningar. Utgifterna kan vara geografiskt spridda i flera delar av landet och inte enbart koncentrerade till den egna bostadsorten.

- *Kryptovaluta:* Enligt Finanspolisen är handel med kryptovaluta en vanlig metod för penningtvätt och kan handla om stora belopp. Köp av kryptovaluta görs dock sällan direkt från bankkontot. Däremot kan det finnas frekventa transaktioner till neobanker[1] där pengarnas slutdestination inte framgår. Det är troligt att transaktionerna i vissa fall avser köp av kryptovaluta.

Företagskonton som brottsverktyg

Nätverksaktörer eftersöker aktivt företagskonton i banker för att placera och skikta brottsvinster. Företagskonton används som brottsverktyg på grund av möjligheten att tvätta större belopp. För att upptäcka misstänkta flöden på företagskonton behövs god kännedom om de enskilda företagens verksamhet, deras företrädare och vad som kan förväntas i termer av motparter, motpartsländer och omsättning.

Det förekommer emellanåt transaktioner mellan företag och nätverksaktörer som inte kan hänföras till löneutbetalning eller utdelning. Beloppen är allt från några tusen till större belopp upp mot 100 000 kr och kan gå i båda riktningar. Transaktionsreferenser som *Lån* eller *Återbetalning lån* är vanligt vid denna typ av transaktioner. Branscher i vilka företagen är verksamma kan variera. Det finns företag som sannolikt nyttjas för att å ena sidan placera brottsvinster och å andra sidan betala svart arbetskraft. Relationen mellan omsättning och antalet anställda kan vara en faktor att beakta, liksom avvikande transaktioner från utlandet.

Ökat behov av möjliggörare på banker

Finanspolisen vill belysa att problematiken med möjliggörare på banker, så kallade insiders, som mot betalning nyttjas för att kringgå kontroller, bedöms öka. Det är troligt att nätverken får ett ökat behov av att använda sig av möjliggörare med strategiska funktioner i takt med att kontrollfunktioner och riskmedvetenhet för penningtvätt hos verksamhetsutövare ökar. En möjliggörare kan exempelvis värva kriminella kunder, bevilja kredit- och bolån på falska grunder samt möjliggöra överföringar som vanligtvis inte skulle ha beviljats. Finanspolisen tidigare påtalat behovet av ett intensifierat arbete bland annat kopplat till insiderproblematiken.[2]

Ett led i arbetet med att identifiera potentiella möjliggörare kan vara att titta på mönster när misstänkta oegentligheter väl upptäcks, exempelvis lån som inte borde ha beviljats eller transaktioner som inte borde ha gått igenom det finansiella systemet. Syftet med det är att utreda om det finns någon gemensam nämnare som kan föranleda misstanke om insiderproblematik.

[1] En neobank är en digital bank där användaren kan utföra alla sina tjänster via en mobilapp eller genom ett webbgränssnitt.
[2] Finanspolisen informerar – Banker och finansiella institut som brottsverktyg.

Finanspolisen informerar

Arbete framåt

Verksamhetsutövare bör verka för ett fortsatt proaktivt arbetssätt för att öka förmågan att identifiera individer och företag som nyttjas för penningtvätt i det finansiella systemet. Fördjupad kundkännedom liksom spetsigare transaktionsmonitorering kan utgöra delar i detta arbete. Som nämnts ovan kan även andra källor behövas för att upptäcka individerna.

Nedan exempel kan utgöra typiska transaktionsmönster i nätverksmiljöer som kan föranleda misstankerapportering till finanspolisen.

- Låg faktisk inkomst som inte stämmer överens med uppgifter som lämnats av kunden i kundkännedomen
- Höga transaktionsflöden, främst via Swish och med ett stort antal motparter
- Ständigt låga kontobehållningar på bankkonton
- Förhållandevis höga kontanta uttag eller insättningar
- Köp som bekostas av insättningar från andra privatpersoner, exempelvis varor av dyrare karaktär, resor, nattklubb- och restaurangkostnader samt kostnader för taxi och hyra av elsparkcykel
- Frekventa transaktioner till neobanker
- Överföringar till och från företag som personen i fråga inte har någon uppenbar koppling till där transaktionstext som *lån* och *återbetalning av lån* är vanligt förekommande

Finanspolisen
Epost: fipo@polisen.se

Diarienummer: A666.290/2023