# Finanspolisen informerar

INDIKATORER PÅ FINANSIERING AV TERRORISM • FEBRUARI 2024

## Finansiering av terrorism med kryptotillgångar

Inom Egmont Group[1] har det bedrivits ett projekt med utgångspunkt i hur kryptotillgångar kan används för att finansiera terrorism. Projektet tog fram ett antal indikatorer för kryptotillgångar och finansiering av terrorism.[2] Syftet med denna Fipo informerar är att dela indikatorerna med verksamhetsutövare.

Även om projektets fokus var kryptotillgångar är flera av indikatorerna även tillämpliga på andra typer av tillgångar och betalmedel samt för att upptäcka penningtvätt. Verksamhetsutövare som inte är berörda av kryptotillgångar bör därför ändå ta del av indikatorerna. För den som vill fördjupa sig i ämnet kryptovalutor rekommenderas rapporten Penningtvätt och finansiering av terrorism med kryptovalutor[3].

Vid tillämpning av indikatorer är det viktigt att ha i åtanke att det sällan är enskilda indikatorer som kan påvisa en misstanke om finansiering av terrorism eller penningtvätt. Ofta behövs det fler omständigheter för att stärka en misstanke.

Bild: MostPhotos

[1] Egmont Group är en global organisation vars medlemmar består av FIU:er. Egmont tillhandahåller bl.a. ett system för informationsutbyte mellan FIU:er rörande penningtvätt och finansiering av terrorism.
[2] På egmontgroup.org finns en sammanfattning av rapporten, den rapporten innehåll dock inga indikatorer.
[3] A433.555/2022, publicerad på https://polisen.se/om-polisen/polisens-arbete/finanspolisen/

# Finanspolisen informerar

Polisen

INDIKATORER PÅ FINANSIERING AV TERRORISM • FEBRUARI 2024

## Högriskland, allmän information

Flera av indikatorerna innehåller någon beröring mot högriskland. Med högriskland avses ett land där det bedöms föreligga en stor risk för penningtvätt eller finansiering av terrorism. Vissa organ, t.ex. EU och FATF[4] har publicerat sådana listor. Varför ett land bedöms som ett högriskland och på vilka premisser den bedömningen görs varierar, till exempel undermåliga funktioner för kontroll av det ekonomiska systemet eller en ökad aktivitet av terroristorganisationer i ett visst område. Det finns även officiella listor från andra organisationer på individer och aktörer som bedöms vara terrorister.

Omvärldsbevakning och att hålla sig uppdaterad om vilka länder eller områden som det råder oroligheter i skapar förutsättningar för verksamhetsutövare att fånga upp tecken på finansiering av terrorism. Det gäller inte bara transaktioner från Sverige till andra länder utan även transaktioner till Sverige från andra länder där personer kan vilja stötta terrorism eller rekryteringsverksamhet i Sverige. En transaktion i terrorfinansieringssyfte kan däremot studsa via något annat land som inte bedöms som ett högriskland, vilket gör att ha högriskland som enskild indikator i monitorering kan bli missvisande.

## Indikatorer relaterade till transaktioner

- Användning av en VASP[5] för att göra uttag eller insättning av kryptovaluta som direkt eller indirekt omsätts till kluster (en större mängd adresser/plånböcker) vilket kan kopplas till kända terroristorganisationer eller till organisationer som är kopplade till våldsbejakande extremism eller radikalisering.
- Transaktioner med kryptotillgångar kan länkas till ransomeware[6].
- Insättningar via bankomater för kryptotillgångar görs vid olika tider och på olika platser men till samma adress.
- Värdebevis används för att köpa kryptotillgångar.
- Kontanter används vid köp eller försäljning av kryptotillgångar, oavsett belopp.
- Ursprunglig tillgång som förs över till t.ex. bankkonto kan länkas till:
    - Falska eller bedrägliga sajter för kryptohandel
    - En okänd kryptovaluta som marknadsförts på sociala medier men där användare angett att det är en bluff
    - Dataspel där det går att köpa s.k. skins eller andra saker i spelet som kan säljas vidare till andra
- Flertalet transaktioner under en och samma dag mellan fiatvaluta och kryptotillgångar.
- Hög omsättning och många transaktioner mellan olika typer av kryptotillgångar.
- Kryptotillgång passerar en stor mängd olika mellanliggande adresser under väldigt kort tid innan den överförs till kundens plånbok.
- Små överföringar som kommer från flera plånböcker utan inbördes koppling och följs av transaktioner till annan plånbok kan tyda på insamlingsverksamhet.
- Användning av flera olika VASPs, adresser, betalplattformar och plånböcker i flera olika jurisdiktioner.
- Att det någonstans i samband med en transaktion hänvisas till hawala, t.ex. i meddelandetexten.

[4] Financial Action Task Force. Ett mellanstatligt organ som tar fram internationella standarder för bekämpning av penningtvätt och finansiering av terrorism.

[5] Virtual Asset Service Providers, verksamheter som erbjuder handel med kryptotillgångar

[6] I svensk betydelse utpressningsprogram, utpressningsvirus, gisslanprogram eller gisslanvirus. Är en typ av skadlig programvara vars syfte är utpressning, ofta genom att ta filer som gisslan via kryptering.

# Finanspolisen informerar



## Indikatorer relaterade till anonymisering

- Tjänster eller verktyg såsom darknet, mixers/tumblers eller Coinjoin används, vilka syftar till att dölja vem som utför en transaktion i kryptovaluta.
- Kryptotillgången går genom mixer/tumbler-tjänster och överförs via flera olika plånböcker innan den växlas till fiatvaluta.
- Kundens transaktioner utgörs av fler än en typ av kryptovaluta eller s.k. chain-hoppning[7], särskilt om kunden använder sig av s.k. privacy coins[8] såsom Monero, Dash eller Zcash.
- Kunden har tillgångar som enbart består av olika privacy coins eller har ett högt värde i privacy coins.
- Växling av kryptovalutor till privacy coins görs genom små betalningar eller genom stora summor.
- Kryptovalutor eller olika privacy coins härrör från en kryptomäklare eller -växlare som marknadsför sina tjänster som anonyma eller integritetsskyddade.
- Kundens uppgivna e-postadress är anonym och har erhållits genom en krypterad e-post-tjänst.

Bild: MostPhotos

## Indikatorer relaterade till avsändare eller mottagare

- Koppling finns till ett högriskland i den information som tillhandahålls när en kundrelation etableras eller när en initial transaktion genomförs. Kopplingen kan finnas exempelvis i uppgifterna om var personen är född, den nuvarande adressen, e-postadressen, telefonnumret, IP-adressen eller bostadsadressen.
- Vid etableringen av en ny kundrelation uppstår det misstankar kring kundens identitetshandlingar eller att identitetshandlingen i sig inte är tydlig eller läsbar.

[7] En typ av kryptovaluta konverteras/växlas till en annan kryptovaluta.
[8] Privacy coins är kryptovalutor som skapats för att tillhandahålla ökad anonymitet.

- En ideell organisation, stiftelse eller liknande använder sig av komplexa transaktionskedjor i form av t.ex. kontanter, betalinstitut och kryptovalutor när de genomför betalningar.
- Plånbok innehas av personer som kan kopplas till terrorfinansiering alternativt att det från plånboken gått transaktioner till insamling för terroristverksamhet.
- Av media och/eller cybersäkerhetsbulletiner framgår att kundens plånbok eller adress är kopplad till bedräglig verksamhet.
- Verksamhetsutövaren får träff på, eller hittar koppling till, organisationer som finns på offentliga listor som rör terrorism från organ såsom EU, FN eller OFAC[9].
- Flertalet olika kunder som under en kort tidsperiod registrerar sig hos en kryptoväxlare och använder sig av samma adress, mobilenhet, telefonnummer, IP-adress eller andra identitetsuppgifter.
- Medel skickas till eller från en plattform för kryptoväxling som är förknippad med hög risk (t.ex. att plattformen rekommenderas i forum där man kan få tips om kriminella tillvägagångssätt).

## Indikatorer relaterade till ursprunget till en tillgång eller en förmögenhet

- Kunden lämnar inga, eller säger sig sakna, underlag eller information för kundkännedom (inklusive tillgångens ursprung).
- Kunden är ovillig att, eller kan inte lämna information om ursprunget till privacy coins som kunden innehar eller har haft.
- Tillgångar (både i fiat-valuta eller kryptotillgångar) flyttas genom en serie komplexa transaktioner till flertalet adresser eller plånböcker vilket gör att det framstår som om kunden avser att dölja ursprunget till tillgångarna eller vad de ska användas till.
- Transaktioner sker till eller från en adress eller plånbok som har en direkt eller indirekt exponering till tjänster eller liknande som kan förknippas med hög risk. De kan utgöras av marknadsplatser på darknet, mixers eller tumbling-tjänster, tveksamma spelsajter, illegala aktiviteter såsom ransomeware eller rapporter om annan brottslig aktivitet.

## Indikatorer relaterade till geografiska risker

- En transaktion av en kryptotillgång kommer från ett högriskland eller kan kopplas till en VASP som har sin verksamhet i ett högriskland.
- Transaktioner av kryptotillgångar till eller från ideella organisationer, stiftelser eller liknande som agerar i högrisländer eller som erbjuder hjälp eller tjänster till personer som kan förknippas med ett högriskland.
- Användning en IP-adress som finns i en konfliktzon eller i ett geografiskt riskområde.
- Transaktioner i kryptotillgångar kommer från länder eller regioner som FATF har klassat som ej samarbetsvilliga.

Finanspolisen
Epost: fipo@polisen.se

[9] Office of Foregin Asset Control är en amerikansk myndighet som verkar för kontroll och efterlevnad av sanktioner mot länder, terrorister m.m.