5. Privatejede pengeautomater

Produkt

Privatejede pengeautomater

Sektoren

Der er en stigende anvendelse af privatejede pengeautomater i hele Unionen, og de retshåndhævende myndigheder er blevet gjort opmærksom på det mulige misbrug heraf til hvidvask af penge. Ifølge de modtagne oplysninger skaber private parters mulighed for at købe og leje pengeautomater hos engrosleverandører et smuthul, som kriminelle drager fordel af.

For mange ejere af diskoteker, barer og restauranter, der installerer en af disse pengeautomater, har det vist sig at være en forretningsorienteret beslutning — kunden tilbydes den bekvemmelighed at kunne hæve kontanter, og den forretningsdrivende maksimerer sandsynligheden for, at nogle af disse kontanter vil blive brugt i vedkommendes forretning.

Private pengeautomater er ofte placeret i kontantintensive virksomheder. Desuden kan privatejede pengeautomater også findes i pengeoverførselsvirksomheder (MSB). I betragtning af at tilstedeværelsen af en pengeautomat i en MSB er ulogisk på grund af en MSB-tjenestes karakter og det forhold, at mange hawaladarer driver en MSB som en lovlig sidebeskæftigelse (38) eller en valutaomvekslingstjeneste, kan risikoen for misbrug klart identificeres. Desuden kan privatejede pengeautomater anvendes til at købe virtuelle valutaer (39).

Beskrivelse af risikoscenariet

a) ATM-indlæsningsmuligheder

For at fylde maskinen med kontanter er én mulighed at benytte kontanthåndterings-/kontantleveringsvirksomheders tjenester.

En anden mulighed for den forretningsdrivende er at fylde op med kontanter fra sit kasseapparat. Dette giver erhvervsdrivende yderligere muligheder for at begå skatteunddragelse ved at sælge varer til gengæld for kontanter uden at udstede kvitteringer. Derefter placerer de blot deres sorte kontanter i deres pengeautomat og venter på, at de tages af almindelige kunder. Ved årets udgang anmeldes sådanne salg aldrig til skattemyndighederne.

Den tredje og mest bekymrende mulighed er blot at fylde pengeautomater op med kriminelle midler (40). Indsamlede efterretninger viser, at i sager, hvor der anvendes kriminelle kontanter, er modus operandi følgende: en kurer leverer kriminelle kontanter til automatejeren/den forretningsdrivende. Kontanterne kan stamme fra forskellige kontantgenererende aktiviteter såsom narkotikahandel, illegal migration, menneskehandel, arbejdskraft og seksuel udnyttelse, salg af forfalskede varer, tyveri, røveri osv. De kriminelle kontanter fyldes derefter i maskinen. Når intetanende kunder eller forbipasserende, der har brug for kontanter, anvender deres kort til at hæve kontanter, debiteres det samme beløb på deres bankkonti og krediteres kontoen tilhørende ejeren af pengeautomaten/den handlende. Derefter kan han blot overføre pengene til en given konto, der kontrolleres af den kriminelle, med fradrag af den aftalte provision.

38 Se afsnittet "Illegal transfer of funds — Hawala".
39 https://www.justice.gov/usao-cdca/pr/oc-man-admits-operating-unlicensed-atm-network-laundered-millions-dollars-bitcoin og
40 Enten er en kriminel organisation tjenesteudbyderen, og pengeautomaterne lastes udelukkende med udbytte fra kriminalitet, eller der er et samarbejde mellem tjenesteudbyderen og den kriminelle organisation, eller der er tale om infiltration.

b) Afkobling af bankkonti og internationaliseringsrisici

Der opstår et internationaliseret, potentielt langt farligere risikoscenarie, når nationale regelsæt kræver, at en privat enhed, der køber en pengeautomat, ved købet skal angive et nationalt bankkontonummer, som er knyttet til pengeautomaten og dens aktiviteter, men der er ikke noget krav om, at den forretningsdrivende skal anmode om kontanter til pengeautomaten fra den samme bankkonto, som denne har knyttet til sin pengeautomat eller endda fra den samme bank. Dette hæmmer bankers korrekte overvågning.

En gennemgang af de virksomheder, der tilbyder private ATM-tjenester, viser, at der er flere store britiske og amerikanske (41) leverandører, som har formået at gøre deres forretninger internationale (42).

Der opstår vigtige spørgsmål vedrørende de konti, som disse pengeautomater (som sælges af virksomheder i EU og USA og er til stede i EU-lande) er knyttet til. Hvis de er knyttet til en bankkonto i EU, men fysisk befinder sig i et andet land, er det praktisk talt umuligt at fastslå oprindelsen af de kontanter, der indsættes i dem.

c) Skatteunddragelse og skattesvig

Private pengeautomater anvendes også til skatteunddragelse og skattesvig, især da nogle kontantintensive forretningsdrivende tilskynder deres kunder til at hævekontanter for tjenester, der ikke er faktureret eller registreret. Det beløb, der går tabt i skatteindtægter fra skatteunddragelse og skattesvig gennem private pengeautomater, er større end den mængde, der hvidvaskes.

d) Mikrostrukturering efter organiseret kriminalitet

Med hensyn til hvidvask af penge anvendes private pengeautomater ofte til "mikrostruktur" — deponering og hævning af små pengebeløb, der er i overensstemmelse med normale beløb for hævning i pengeautomater, og som ikke opdages af bankkontroller. Organiserede kriminelle vil foretage omfattende små daglige kontante indskud på 100 eller flere bankkonti ved hjælp af private pengeautomater for at undgå at udløse indberetningskrav i forhold til bekæmpelse af hvidvask af penge.

Trussel

Finansiering af terrorisme

Der findes i øjeblikket kun få specifikke vurderinger af terrorfinansieringstruslen i forbindelse med privatejede pengeautomater. Ikke desto mindre viser den kombinerede vurdering af kontantbetalinger og analysen af pengekurerer, at denne modus operandi er bredt tilgængelig og billig. Der kan også være en trussel om transport af kontanter til EU fra et tredjeland, navnlig fra lande, der er eksponerede over for terrorfinansieringsrisici eller fra konfliktområder. Der er konstateret tilfælde af lave beløb, som involverer integration af kontanter, der transporteres fra tredjelande ind i det finansielle system/den lovlige økonomi i EU (analyseret i et særskilt afsnit i denne rapport).

Konklusioner: på grundlag af feedback fra de retshåndhævende myndigheder og FIU'erne anses terrorfinansierings-trusselsniveauet for at være meget betydeligt (niveau 4).

Hvidvask af penge

41 Som eksempel kan nævnes: YourCash Europe — en virksomhed, der kontrollerer 32 % af det frit tilgængelige ATM-marked i Det Forenede Kongerige — har filialer i Nederlandene, Belgien og Irland samt pengeautomater i andre jurisdiktioner. Derudover opererer Cardtronics (nogle filialer, der opererer under varemærket DC Payments) i 11 lande. Ud over de nævnte filialer ud af Europa (Sydamerika og Nordamerika, New Zealand og Australien, Sydafrika) og den britiske filial opererer de i Irland, Tyskland, Polen og Spanien.

42 Som et yderligere eksempel er afsnittet ATM-lokalisator på LINK's websted: (https://www.link.co.uk/consumers/locator/) viser, at der findes privatejede britiske pengeautomater, der er fysisk til stede i Belgien, Tjekkiet, Frankrig, Tyskland, Gibraltar, Italien, Nederlandene, Irland og Schweiz samt Guernsey, Isle of Man og Jersey.

Vurderingen af hvidvasktruslen i forbindelse med privatejede pengeautomater viser, at denne modus operandi udnyttes af kriminelle, da den udgør en realistisk mulighed, som er ganske attraktiv og sikker. Den udgør en let måde, hvorpå man kan undgå at betale skat og skjule ulovligt udbytte fra strafbare forhold. For så vidt angår terrorfinansiering, kræver det imidlertid et moderat ekspertiseniveau for at kunne drive virksomheden og undgå at blive opdaget. Denne modus operandi anvendes også til at købe virtuel valuta som rapporteret af FIU'er og bekræftet af Europol: Da der ikke findes nogen harmonisering af eller kontrol med krypto-pengeautomater, er det let at deponere kontanter i disse krypto-pengeautomater for at omdanne kontanter til kryptoaktiver (43).

Konklusioner: på grundlag af feedback fra de retshåndhævende myndigheder og FIU'erne anses hvidvask-trusselsniveauet for at være meget betydeligt (niveau 4).

Sårbarhed

Finansiering af terrorisme

a) risikoeksponering

Sårbarhedsvurderingen af terrorfinansiering i forbindelse med privatejede pengeautomater er uløseligt forbundet med vurderingen vedrørende anvendelsen af/betalinger i kontanter generelt og kan følge samme rationale. Privatejede pengeautomater gør det muligt at behandle et stort antal anonyme transaktioner, som kun kræver en indledende investering. Det har derfor en høj iboende risikoeksponering.

b) risikobevidsthed

Risikobevidstheden synes at være temmelig lav.

c) retlige rammer og kontroller

I henhold til EU's retlige ramme kan tjenester i form af hævning af kontanter tilbydes af ureguleredе enheder (dvs. ikke underlagt AML/CFT-krav). De gældende retlige rammer varierer fra den ene medlemsstat til den anden, og der kan derfor potentielt mangle kontrol.

Konklusioner: privatejede pengeautomaters sårbarhed er uløseligt forbundet med sårbarhederne i forbindelse med brugen af kontanter generelt. Den udbredte brug af kontanter i EU's økonomier, og det faktum at sektoren tilsyneladende ikke er klar over denne risiko, gør, at terrorfinansierings-sårbarheden anses for at være meget betydelig (niveau 4).

Hvidvask af penge

a) risikoeksponering

Sårbarhedsvurderingen af hvidvask af penge i forbindelse med privatejede pengeautomater er uløseligt forbundet med vurderingen vedrørende brugen af/betalinger i kontanter generelt og kan følge samme rationale. Privatejede pengeautomater gør det muligt at behandle et stort antal anonyme transaktioner, som kun kræver en indledende investering. Det har derfor en høj iboende risikoeksponering.

b) risikobevidsthed

Risikobevidstheden synes at være temmelig lav.

43 De såkaldte "krypto-ATM's" er dramatisk blomstrende i hele verden: https://coinatmradar.com/

c) retlige rammer og kontroller

I henhold til EU's retlige ramme kan tjenester i form af hævning af kontanter tilbydes af uregulerede enheder (dvs. ikke underlagt AML/CFT-krav). De gældende retlige rammer varierer fra den ene medlemsstat til den anden, og der kan derfor potentielt ikke være kontrol.

Konklusioner: privatejede pengeautomaters sårbarhed er uløseligt forbundet med sårbarhederne i forbindelse med brugen af kontanter generelt. Den udbredte brug af kontanter i EU's økonomier og den kendsgerning, at sektoren tilsyneladende ikke er klar over denne risiko, gør at sårbarheden for hvidvask af penge anses for at være meget betydelig (niveau 4i).

Risikoniveau

Med hensyn til **finansiering af terrorisme** er trusselsniveauet blevet vurderet til at være meget betydeligt (4), mens sårbarhedsgraden er blevet vurderet som meget betydelig (4).

RISIKO	
1-1,5	Mindre signifikant LAV
1,6-2,5	Moderat signifikant MEDIUM
2,6-3,5	Signifikant HØJ
3,6-4	Meget signifikant MEGET HØJT

Med hensyn til **hvidvask af penge** er trusselsniveauet blevet vurderet til at være meget betydeligt (4), mens sårbarhedsgraden er blevet vurderet som betydelig/meget betydelig (niveau 4).

RISIKO	
1-1,5	Mindre signifikant LAV
1,6-2,5	Moderat signifikant MEDIUM
2,6-3,5	Signifikant HØJ
3,6-4	Meget signifikant MEGET HØJT

Konklusioner: det anslåede risikoniveau for både finansiering af terrorisme og hvidvask af penge er MEGET HØJT.

Risikobegrænsende foranstaltninger

Private pengeautomatvirksomheder udgør en øget risiko for banker og bør behandles som højrisikovirksomheder i forbindelse med bankers risikovurderinger. Risiciene for banker er ikke kun finansielle, men omdømmemæssige.

- For det første bør kunder, der ejer eller driver private pengeautomater, identificeres behørigt.
- Når banken har identificeret en ATM-ejer eller -operatør, bør den indhente yderligere oplysninger for at få en forståelse af ATM-ejeren/-operatøren samt en forståelse af ATM-ejerens procedurer.
- Når der er indhentet tilstrækkelige oplysninger, bør den tilknyttede bank implementere en procedure for overvågning af pengeautomatejernes konti. De oplysninger, der indhentes under due diligence-processen, bør sætte banken i stand til at bestemme omfanget og hyppigheden af den nødvendige overvågning.
- Medlemsstaterne bør garantere forpligtelsen til at registrere, begrænse ejerskabet, overvåge eller undersøge privatejede pengeautomater — til og med forpligtelsen til at knytte pengeautomater til en bankkonto i den medlemsstat, som de fysisk befinder sig i.
- Et styrket samarbejde med toldmyndighederne vil bidrage til at indhente yderligere oplysninger om import af AML-maskiner.
- I betragtning af den grænseoverskridende karakter af hvidvask af penge og finansiering af terrorisme bør medlemsstaterne tilstræbe internationalt samarbejde og tilskynde de relevante myndigheder med ansvar for forebyggelse og bekæmpelse af hvidvask af penge og finansiering af terrorisme til at anmode om støtte fra agenturer såsom Europol.