

EU råkade skriva AML-branschens AI-strategi

AMLR dikterar inte att AI ska användas. Men kraven leder fram till exakt den arkitektur som AI behöver för att kunna göra nytta.

Peter Lange

Head of Sales, Pingwire

Under sommaren fick jag förmånen att läsa en artikel som Johan Övergaard, Manager Transaction Monitoring på Swish, delade med mig som publicerats i FinTech Global. Artikeln ställer frågan om försvaret hinner utvecklas i samma takt som den AI-drivna finansiella brottsligheten (se *Is financial crime entering an AI arms race*).

Artikeln svar är i korthet ja, kapprustningen pågår redan. Men det som var uppfriskande läsning är att artikeln inte landar i den enkla slutsatsen att autonom AI ersätter både systeminfrastruktur och människor samt löser AML och bedrägeribekämpning felfritt. Istället fokuserar den på den praktiska tillämpningen av AI, på hur tekniken faktiskt passar in i befintliga metoder och vad som sker just nu inom området för AML/fraud. Det är den här synen jag ville fördjupa mig i vilket resulterade i denna artikel.

Jag tror också att EU har skapat ett regelverk som driver fram AI-användning, sannolikt utan att ha avsett det. AMLR dikterar inte att AI ska användas. Men den kräver bredare kundkännedom, att fler datapunkter faktiskt används i den löpande uppföljningen och monitoreringen, synkron övervakning i realtid när förutsättningar finns och spårbarhet i varje led. De kraven råkar leda fram till exakt den arkitektur som AI behöver för att kunna göra nytta. Alltså data som är samlad, kopplad, nåbar i realtid och spårbar.

Som försäljningschef på Pingwire arbetar jag dagligen med AML- och bedrägerisystem, anpassade till företag som omfattas av penningtvätsregelverket. Det innebär att jag träffar många företag och institut som står inför utmaningar när man vill förnya sitt arbetssätt och sin systeminfrastruktur, för att mer effektivt bekämpa finansiell brottslighet.

Befintliga regler är inte oanvändbara, men de räcker inte

Statiska, icke-sekvensbaserade regler med fasta tröskelvärden (t.ex. rullande summor, beloppsgränser, nettovärde vid in- och utflyttning av medel) är inte tillräckliga mot upplägg som är byggda för att kringgå just dem. Men de tjänar fortfarande sitt syfte genom att de sätter ramarna. Det som måste till är smarta regler som löpande lär sig enskilda kunders beteende och flaggar avvikelser mot det. Alltså regler byggda på maskinlärning och som dessutom kopplar ihop data för att sätta ihop en profil. Detta är något många företag och institut som jag träffar efterfrågar.

Det är här också en central poäng i artikeln från FinTech Global, att brottsligheten designas för att smälta in. En transaktion som ser helt normal ut i isolering avslöjar sig först på andra sätt: mot kundens egen historik, mot jämförbara kunders beteende, eller när datan kopplas

ihop på nätverksnivå. Ett money mule account kan imitera en normal kund i en ögonblicksbild. Det är betydligt svårare att samtidigt fejka en konsistent historik över tid och hålla alla kopplingar rimliga, däribland transaktioner, device-enheter, IP-adresser, motparter, ägarförhållanden m.m.

AI gör redan verklig nytta i AML-processer

Vad marknaden också efterfrågar är AI-stöd i ärendehantering. Jag tror många har förstått att ärendehantering är en repetitiv, återkommande process där liknande typologier utreds, vilket är utmärkt för LLM:er att effektivisera. Både vad gäller förutredning som presenteras för analytikern och då också företagsspecifikt utifrån just deras utredningsbehov. Detta har flera steg som ökar effektiviteten men också kan göra utredningen mer rättssäker genom att minska manuella fel: 1. Komprimering av data, 2. Analys av data, 3. Identifiering av risker, 4. Rekommendation av utredningssteg och 5. Utfall. Det ger utredaren stöd i att snabbt förstå kontexten kring vad som har hänt, hur datan ser ut och hänger ihop samt vad som behöver utredas närmare. Det ger också bra, förklarbar utredningstext att spara i ärendet.

Men det stannar inte vid förutredningen. Redan nu ser vi AI-agenter användas bredare i det operativa arbetet. För att prioritera i ärendekön så att de larm som faktiskt bär störst risk hamnar högst, för att kalibrera regler och tröskelvärden samt för att djupdyka i data och plocka fram det underlag en analytiker annars hämtar manuellt ur flera olika vyer.

Hos oss på Pingwire tar det här två konkreta former. Den ena är vår AI-ärendeanalytiker, som läser ihop underlaget i ett ärende och levererar en kort beskrivning och en sammanfattning direkt i ärendet, anpassad till institutets riktlinjer. Den aktiveras per konto och styrs av behörigheter, så att bara de roller som ska ha funktionen använder den.

Den andra är en Copilot som följer dig i plattformen. Den kan svara på frågor om hur systemet fungerar, hur regler och riskklasser är uppsatta, och hämta t.ex. kunddata, ärenden, transaktionsstatistik och träffhistorik för PEP, sanktioner och negativ medieinformation. Copiloten arbetar med den inloggade användarens egna rättigheter, vilket betyder att den aldrig kan se mer än analytikern själv får se. Och varje svar passerar en ytterligare, isolerad AI-kontroll innan det visas för användaren.

Det är enligt mig så AI-stöd behöver byggas i den här domänen just nu. Med bred åtkomst till data, men snäva och spårbara befogenheter, kontroller, och ett beslut som ligger kvar hos människan. Utvecklingen går emellertid fort, och även om tillsynsmyndigheterna i dag strävar emot och håller hårt i principen att beslutet ska ligga hos människan tror jag att vi inom en snar framtid kommer att se beslut faktiskt överlåtas till AI. Alltså inte bara AI i en rådgivande roll, utan en reell ökning av automationsgraden i AML-arbetet. Det som gör den utvecklingen möjlig är att tekniken för att styra AI redan finns. AI governance i praktiken handlar om att kunna skriva policies, sätta tekniska guardrails, styra åtkomsträttigheter och säkerställa spårbarhet. Det begränsar inte AI:n, det styr den. Och framför allt gör det att man

kan definiera var gränsen går, alltså vilka beslut AI får fatta själv och vilka som fortfarande måste passera en människa. Det var också en insikt från Nordic Fintech Week (NFTW), där banker, advokater och branschfolk resonerade i just de banorna.



Det begränsar inte AI:n, det styr den."

En annan sak som har börjat diskuteras mer är kostnaden. Varje AI-session förbrukar tokens, oavsett om det handlar om en ärendeanalys, en fråga om kunddata eller en fråga om hur något fungerar i plattformen. I Pingwire mäts den förbrukningen per session, och det är medvetet. Utan mätning går det inte att svara på den enda fråga som egentligen betyder något. Vad kostar ett AI-handlagt ärende eller en fråga till AI om hur plattformen fungerar? Och vad kostade det tidigare, när ärendet analyserades manuellt och användaren fick leta i en manual?

Det är där nyttan blir konkret. Några kronor i tokens istället för tjugo minuters analytikerarbete är en kalkyl vem som helst kan räkna på och följa upp. Och kostnaden per ärende bör sjunka över tid i takt med att datamodellen, promptarna och arbetssättet mognar.

Den regulatoriska riktningen är tydlig

De uttalanden jag har fångat upp visar på en tydlig regulatorisk riktning. Såväl EU-övergripande myndigheter som AMLA som lokala tillsynsmyndigheter uppmuntrar användningen av AI, men trycker på AI governance och att beslutsfattandet ska ligga hos människan. Även om skäl 58 i AI-förordningen undantar AI-system som används för att identifiera bedrägerier från att definieras som "högrisk-AI" blir konsekvensen av lagstiftning såsom AI-förordningen, GDPR och DORA att AI inom AML-/fraudarbetet i praktiken behöver:

- **Risikanalys:** en dokumenterad bedömning av AI-systemets risker innan det tas i drift.
- **Dokumentation och spårbarhet:** utförlig beskrivning vad modellen gör, vilket underlag den bygger på och en logg som visar vad som legat till grund för respektive utfall.
- **Hög datakvalitet:** säkerställd kvalitet och representativitet i den data modellen tränas och verkar på.
- **Transparens och förklarbarhet:** möjlighet att i efterhand motivera varför ett specifikt utfall eller en specifik flaggning skedde.

- **Mänsklig översyn och involvering:** en människa fattar det faktiska beslutet, AI:n stödjer.

Hur mycket AI Omnibus och Digital Omnibus lättar på det återstår att se. De europeiska politikerna har nämligen insett att EU halkat efter i det globala AI-racet.

Inom överskådlig tid ser i vart fall inte jag en autonom AI-agent med begränsad mänsklig översyn som utför hela kretsloppet, dvs. gör den allmänna riskbedömningen, implementerar modeller och scenarier, automatiskt utreder och beslutar i ärenden med konsekvenser för betalningsgenomförande och enskilda kunders åtkomst till finansiella produkter, rapporterar SAR/STR:er till FIU:er, gör back-testing och sedan går tillbaka och justerar den allmänna riskbedömningen osv. Däremot behöver vi AI:s stöd för att omedelbart snabba på detta kretslopp för att komma i kapp de kriminella penningflödena. Kriminella kan nyttja AI-system ohämmat för att hitta och utvärdera nya sätt att tvätta pengar och utföra bedrägerier.

Kriminella agerar redan i AI-hastighet

Digitalisering och ny teknik har dessutom förändrat kundbeteendet: online banking har införts där KYC utförs digitalt på några minuter och betalningar genomförs internationellt inom sekunder. LLM:er kan skapa syntetiska identiteter, förfalskad KYC-dokumentation och skraddarsydda bortförklaringar. De kan dessutom sondera AML-system för att kartlägga tröskelvärden och hitta luckor att utnyttja. Tekniker som tidigare krävde tid, expertis och koordinering kan nu utföras snabbt, i stor skala och med hög grad av realism.

Traditionella system med statiska regler, fragmenterad arkitektur med datan i silon som konsekvens och som är baserade på dygnsvis batchkörning av transaktioner kan helt enkelt inte hänga med i AI-genererade kriminella flöden. AML-team drunknar i false positives och ser inte hela riskbilden. Den underliggande arkitekturen i traditionella AML-system som bygger på fragmenterade uppsättningar och data i silon, är inte längre ändamålsenlig.

Den frestande genvägen och varför den inte är tillräcklig

Det ligger nära till hands att inte byta ut infrastrukturen alls, utan lägga agentisk AI som ett intelligent lager ovanpå befintliga system för att effektivisera och förbättra ärendehantering genom att extrahera, komprimera och synliggöra den data som finns tillgänglig i dessa spridda system. För institut med inbäddad arkitektur, som förlitar sig på traditionella system, skulle det kunna ses som ett leapfrog. Analytiker slipper växla mellan en mängd system och webbläsarfönster, samla information manuellt och pussla ihop samband ur fragmenterade datamängder. En process med stor kognitiv belastning och som är tidskrävande. Man kommer dock inte åt roten till problemet, dvs. skalan, hastigheten och sofistikationen i den AI-genererade finansiella brottsligheten.

För att komma åt det behöver man börja i botten, med datamodellen. Den behöver vara flexibel, i betydelsen enkel att förändra, och kunna ta emot stora mängder datapunkter av olika slag utan att man bygger om systemet varje gång ett nytt dataunderlag tillkommer. Ovanpå den ligger ett API som speglar datamodellen, så att det blir enkelt för institutet att skicka in den data man har och faktiskt vill använda. Och i modellen måste datan gå att koppla ihop på entitetsnivå, så att en regelmotor kan räkna på sambanden snabbt nog för synkron övervakning i realtid.

Först då kan man verkligen dra nytta av agentisk AI i AML/fraud-system, tillämpa beteendeanalys och stoppa betalningar i realtid. Både beteendeanalys och att stoppa betalningar i realtid, då det är möjligt, kommer att bli ett krav enligt AMLR med tillhörande riktlinjer (se bland annat artikel 26 AMLR och AMLA:s riktlinjer för fortlöpande övervakning av en affärsförbindelse).

Traditionella system konstruerades när en kund var en rad i en databastabell och övervakningen kördes i batch över natten. Ett nytt system behöver inte ta hänsyn till decennier av ändringar i den strukturen, eller till alla integrationer som byggts ovanpå den och som i sin tur krävt lager av tvättning och omvandling av data för att hänga ihop.

Den obekväma frågeställningen

Artikeln från FinTech Global argumenterar för att nästa generations brottsbekämpning kommer att avgöras mindre av någon enskild banbrytande teknik och mer av förmågan att koppla ihop och operationalisera en bred uppsättning av tekniska förmågor på ett AI-native sätt. Jag delar denna uppfattning, men det tvingar fram en obekväm fråga för oss som bygger AML/fraud-system och tillhandahåller det som en SaaS-produkt. I en värld där agentisk AI effektiviserar och företag själva med hjälp av verktyg såsom Cursor, GitHub Copilot, Claude Code eller OpenAI Codex kan prompta fram funktioner på egen hand, vad är då vårt självberättigande?

Vårt svar och enligt mig ett do or die för all B2B SaaS, är att expertisen måste bli djupare inom det egna området, inte bredare över fler. Vi ska vara experter på AML, både det regulatoriska och det operationella. Experter på AI och ligga först i testning och tillämpning av de senaste LLM-modellerna för AML/fraud-arbete och experter på hur man på ett säkert och regulatoriskt hållbart sätt bäddar in dessa modeller i ett system som är byggt för AI från grunden. På så sätt vet kunden att vi alltid kommer att göra utvecklingen bättre och mer effektivt.

Detta för med sig en annan trend inom B2B SaaS: custom solutions, dvs. lösningar anpassade till kunden, långt ifrån den one-size-fits-all modell som B2B SaaS traditionellt kännetecknas av. När man med hjälp av ovan nämnda AI-verktyg kan utveckla, designa och lansera en prototyp på kort tid, kommer samma anpassningsbarhet att krävas av oss B2B SaaS-företag. För oss på Pingwire betyder det en produktvision bestående av en robust, icke förhandlingsbar kärna bestående av en flexibel datamodell med ett API som speglar den, och en re-

gelmotor som gör kraftfulla beräkningar och svarar anropande system på millisekunder. Ovanför kärnan ligger ett lager som är fullt anpassningsbart. Kunden kan beställa olika versioner av detta lager, eller koppla upp en egen AI-agent via Pingwires MCP och själv ändra det som behöver följa den egna processen, till exempel ärendestatusar, fält och arbetsflöden.

Samma MCP öppnar för det omvända, dvs. att arbeta med Pingwires struktur, processer och data direkt i gränssnittet hos den agent man själv föredrar. Så sent som på NFTW uttryckte flertalet banker i panelsamtal att **the best interface is no interface**.

Build vs Buy

Men om att bygga med hjälp av AI är lättillgängligt, varför inte göra det själv? Särskilt i en värld där AI ger omedelbar tillgång till specifik kunskap såsom syntax, API-dokumentation, reglering till en försumbar kostnad. Likväl som att köpa mjukvara, skulle man inte själv kunna förvärva nödvändig kunskap kring reglering och programmering för att bygga den AML-process man önskar, inbyggd med den spårbarhet och förklarbarhet som krävs för att försvara i myndighetstillsyn och revision?

Jag tror det finns tre argument mot detta: AI brister i konsekvent beteende, kontroll och tillräcklig kvalitet. Konsekvent beteende handlar om att AI-systemet bibehåller samma logik, ton och beteende över flera olika uppgifter. En utmaning eftersom AI:s output bygger på sannolikhetsbaserad textgenerering, vilket gör exakta, repeterbara resultat svårare att garantera. Kontroll avser det faktum att när vi använder AI-verktyg förlitar vi oss i grund och botten på prompter, vilket gör det svårt att kontrollera resultatet. Många har nog upplevt att när en mindre detalj i en AI-output ska justeras, förvandlas det snabbt till en tidskrävande och svår uppgift. Konsekvent beteende och kontroll är tekniska problem och utvecklingen går så snabbt att jag tror de kommer att lösas inom kort. Kvalitetsfrågan är av en annan sort, den handlar inte om modellens kapacitet utan om vem som gör avvägningarna.

När det gäller kvalitet kan AI imitera och använda existerande arbete, men den kan inte applicera genuint mänsklig smak eller omdömesförmåga. I brist på bättre ord och i linje med det uttryck som blivit vedertaget kan man säga att AI saknar personal taste.

Min övertygelse är att så länge en människa behövs för att göra avvägningar, välja rätt problemformulering och se helhet och vision, så behövs specialister i mjukvara/AI och i ämnesområdet. Förutsätter man detta har egentligen ingenting i frågan Build vs Buy förändrats sedan innan AI:ns intåg. Tidigare kunde man bygga själv om man rekryterade rätt specialister, eller välja att köpa mjukvara som redan har specialister på området.

Och det är här fördelen med att köpa in specialistkompetens blir tydlig. Det handlar inte bara om att skriva kod och tillämpa AI, utan om att någon redan har byggt, testat och försvarat riskanalysen, dokumentationen, spårbarheten och den mänskliga översynen som räknades

upp ovan inför flera tillsynsmyndigheter, i flera institut, över tid. Den erfarenheten går inte att prompta fram på en eftermiddag.



Den erfarenheten går inte att prompta fram på en eftermiddag."

Arkitekturen avgörande för nyttjande av AI och AMLR som katalysator

Kapprustningen är verklig och vi behöver nyttja AI för att stoppa kriminella från att tvätta pengar. Den som blir mest framgångsrik i detta avgörs inte av vem som har den mest autonoma AI-agenten, utan av vem som bygger den arkitektur och den kombination av människa och AI som faktiskt håller när penningflöden rör sig väldigt fort.

Företag och institut som lyder under penningtvättsregelverket behöver implementera AMLR senast den 10 juli 2027. Många har redan påbörjat arbetet, men för den som har erfarenhet av att implementera regelverk är tidsfristen snäv. Ikraftträdandet ligger i praktiken redan runt hörnet för ett regelverksprojekt av den här storleken.

AMLR innehåller mycket av det som nämnts i denna artikel. Kraven på att lära känna sin kund blir bredare och striktare, och uppföljning och monitorering kräver att fler datapunkter nyttjas. Till detta kommer kravet på synkron övervakning i realtid, så snart en organisation har förutsättningar för det, samt en utökad rapporteringsskyldighet där AMLA själva investerar mycket i infrastrukturen för att kunna ta emot mycket data.

Det jag uppfattar från möten med företag och institut är att de i sina AMLR-gapanalyser upptäcker att KYC-standarderna behöver breddas. Fler datapunkter måste hämtas in och kunna användas i uppföljning och monitorering på ett effektivt sätt. Många inser då att befintliga processer inte är ändamålsenliga och att systemstödet saknas.

Företagen och instituten söker därför system med en flexibel datamodell och ett API som speglar den, så att data kan tas emot och beräknas snabbt nog för övervakning i realtid. Och här händer något intressant. Som en bieffekt av regelefterlevnaden sätter man på plats precis den arkitektur som krävs för att kunna nyttja AI på bästa sätt.



Som en bieffekt av regelefterlevnaden sätter man på plats precis den arkitektur som krävs för att kunna nyttja AI på bästa sätt."

Databasen är nämligen mer än ett lagringsställe. En AI-agent kan inte arbeta med data den inte når, inte tolka samband som inte finns modellerade, och inte lämna spår efter sig i ett system som inte registrerar vad som hänt. Datamodellen med sitt API blir därför det lager agenterna måste gå igenom, deras operativsystem, minnet de hämtar sin kontext ur, och historiken som gör deras arbete granskningsbart i efterhand.

Det är i denna bemärkelse som AMLR fungerar som en katalysator för en bättre framtida tillämpning av AI, oavsett om AI stod högst på institutets agenda eller inte.

Jag är nyfiken på hur andra i branschen ser på detta. Hur tänker ni kring tillämpningen av AI i AML- och fraudarbetet och hur stora förändringar av processer och systemstöd tror ni att AMLR kommer att kräva av branschen som helhet? Dela gärna era perspektiv i kommentarerna eller hör av er direkt till mig.

Peter Lange

Head of Sales, Pingwire

>pingwire_

Källa: FinTech Global, "Is financial crime entering an AI arms race".