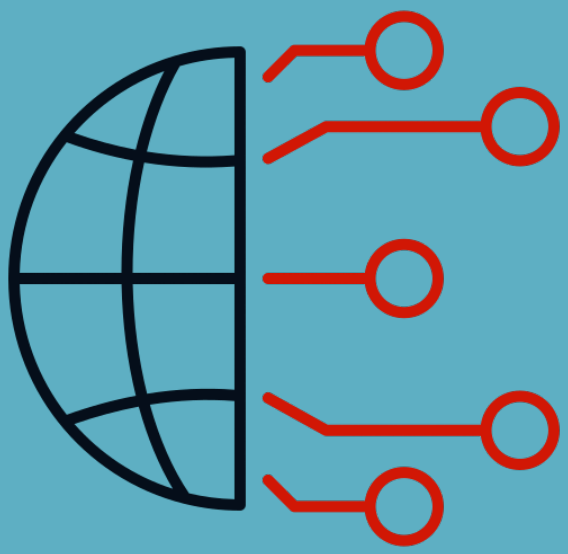
HORIZON SCAN

ARTIFICIAL INTELLIGENCE AND DEEPFAKES

IMPACTS ON MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING



FATF-GAFI.ORG

Background

This horizon scan provides a forward-looking perspective of current and potential Artificial Intelligence (AI) related risks and trends. It forms part of the FATF's staged approach to emerging technologies, with this study aiming to identify and explain developing risks and vulnerabilities associated with AI through the lens of Anti-Money Laundering, Countering the Financing of Terrorism, and Countering the Financing of Proliferation (AML/CFT/CPF). The report is also designed to raise awareness among national authorities, financial institutions (FIs), Virtual Asset Service Providers (VASPs), Designated Non-financial Businesses and Professions (DNFBPs), and other stakeholders, and to support the development of effective regulatory and operational responses within the AML/CFT/CPF framework. It explores the intersection of AI (including deepfakes) with some of the FATF Recommendations and seeks to inform discussion, strengthen understanding, and demonstrate FATF's commitment to stimulate discussion on new topics and to promote a forward-looking engagement on this evolving issue.

Introduction

AI is a disruptive force. From how we work and communicate to how we govern; it is transforming many aspects of modern life. But as with any powerful tools, its misuse is equally transformative—and dangerous. Two parallel narratives have emerged: (1) AI can be used to improve efficiencies in law enforcement, preventive measures, and compliance, and (2) AI is a powerful new tool for money launderers, terrorist financiers and sanctions evaders to circumvent existing ML, TF and PF frameworks with ever greater sophistication.

This paper builds on a roundtable meeting at the FATF's June 2025 Working Group and Plenary meetings exploring this topic. It explores the growing intersection between AI and ML, TF and PF in two parts:

Part I focuses on **AI deepfakes**, using recent expert FATF discussions on the challenges and opportunities of AI as a lens to explore broader vulnerabilities in the preventive systems of AML/CFT/CPF reporting entities, such as FIs, VASPs, DNFBPs.

Part II widens the scan to consider **other emerging AI risks and trends**. Drawing on current research and expert dialogue, it offers a snapshot of developments beyond deepfakes to help anticipate potential future challenges.

Section I: Deepfakes, AI and ML/TF/PF

A Rapidly Changing Landscape

Once a rare occurrence, deepfakes are now being used more widely. AI enabled deepfakes are synthetic media, typically videos, images, or audio, created using artificial intelligence techniques, especially deep learning, to convincingly mimic real people's appearance, voice, or actions[1]. These can be used to impersonate individuals, spread misinformation, or facilitate fraud and other illicit activities. Once rare, deepfakes are increasingly prevalent and can be used to bypass traditional AML/CFT/CPF controls and manipulate systems with alarming ease to commit Money Laundering, Terrorism Financing, Proliferation Financing, and predicate offences such as fraud.

AI-enhanced deepfakes pose a changing threat for the commission of multiple offences. In the context of ML, TF and PF, criminals can use deepfakes to circumvent AML, CFT and CPF preventive measures, particularly Customer Due-Diligence (CDD) systems, including digital ID verification. Sophisticated actors may exploit AI-generated deepfakes in complex securities fraud schemes. These technologies are also being used in consumer fraud schemes, phishing attacks, financial exploitation of vulnerable groups (such as the elderly), online romance scams, and online child sexual exploitation[2].

The risks from deepfakes are escalating rapidly. AI enabled deepfakes allow criminals to deploy increasingly sophisticated scams at scale. Until recently, producing deepfakes required significant technical expertise and resources. However, advances in AI technology and broader accessibility have dramatically lowered barriers to entry. Today, anyone with a smartphone and an internet connection can generate convincing deepfakes within minutes, posing urgent operational, and regulatory challenges for reporting entities and for governments in the fight against ML, TF and PF.

Deepfakes for Circumventing Preventive Measures

Recommendations 10 and 22 of the FATF 40 Recommendations require competent authorities to ensure that FIs, VASPs and DNFBs apply CDD measures to ensure that they can carry out effective checks and identify their customers using "reliable documents, data or information from independent sources (identification data)". As synthetic media tools grow more sophisticated and accessible, they provide new opportunities for organised crime groups[3]. Deepfakes can be deployed to impersonate individuals, manipulate biometric authentication, or support social engineering schemes, thereby amplifying the effectiveness of existing techniques of CDD circumvention and other security protocols established to protect banks and DNFBPs from ML, TF and PF risks. Their adaptability across diverse contexts makes them a versatile enabler of cyber-enabled crime and ML, TF ad PF, and a growing concern for law enforcement (evidence authentication, legal proceedings, victim identification, forensic etc.)[4].

By exploiting the ability to disguise, manipulate, and anonymise identities, criminals are increasingly using deepfakes to expand the complexity, scale, and reach of their operations. The experiences of several countries' law enforcement agencies who participated in the roundtable

---

[1] There is currently no universally accepted definition of "deepfakes," but the term generally refers to synthetic audio-visual content—videos, images, and voice recordings—designed to impersonate real individuals. See for example United States Government Accountability Office (GAO) 2020: 'Science and Tech Spotlight: Deepfakes'. (GAO-20-379SP Deepfakes)

[2] See FATF Report: *Detecting, Disrupting and Investigating Online Child Sexual Exploitation* (2025) https://www.fatf-gafi.org/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html

[3] Bateman, Jon. "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios." *Carnegie Endowment for International Peace*, 8 July 2020, website.

[4] INTERPOL. 2024. *Beyond Illusions: Unmasking the Threat of Synthetic Media for Law Enforcement*. Website

discussion further underscore these concerns, giving concrete examples of how AI-generated deepfakes are actively used to circumvent safeguards and exploit vulnerabilities in financial systems.

The risks from deepfakes are amplified in three key areas:

1) the growing **reliance on biometric verification**, where widespread adoption of facial recognition and video-based KYC creates opportunities for deepfake manipulation;
2) the persistent **lag in technology adoption**, as many AML systems remain ill-equipped to detect synthetic content and compliance frameworks have yet to address these vulnerabilities; and
3) the challenge of **cross-border complexity**, as the interconnection of global financial systems complicates digital identification or the acceptance of remote identity verification, allowing criminals to exploit weaknesses in Anti-Money laundering regimes.

These risks impact the financial sector, notably banks and payment service providers, but also the wider financial sector and DNFBPs, particularly as services (financial, legal, and others) and other activities (such as gambling, gaming, etc.) increasingly take place entirely online. The acceleration of digitalisation since the COVID-19 pandemic has also contributed to an even greater acceleration of financial and commercial interactions taking place online. Moreover, the widespread accessibility of AI systems has amplified the 'dual-use' risk, enabling both highly skilled and less experienced actors to exploit these technologies in ways that pose distinct threats:

Box 0.1. Threat of dual-use of AI for high and low-complexity attacks – (Europol)

Europol highlighted the use of their "innovation hub" echoing other discussions on the AI "Arms Race" against criminals and professional ML schemes.

In regard to trends and emerging risks, Europol highlighted how Artificial intelligence is being exploited for fraudulent purposes in two manners, by both low-skilled criminals, using the opportunity of AI-enhanced deepfakes to easily commit offences, and highly skilled, professionalised individuals operating ML and fraud schemes on behalf of organised crime, thus creating a multiplier effect of crime.

- **Low-skilled offenders** increasingly benefit from the widespread availability of off-the-shelf AI tools, which enable them to carry out sophisticated criminal activities without requiring advanced technical expertise. These technologies—often viewed as general-purpose applications—include AI and deepfake tools that are easily accessible and usable without specialised training. Criminals can exploit them for a range of illicit purposes, such as phishing and fraud, generating synthetic images for child sexual abuse material, impersonation to bypass security systems, and other forms of deception.

- **Highly skilled cybercriminals** are using AI to boost their capabilities—by automating complex attack methods and quickly spotting weaknesses in computer systems. At the same time, expert-level use of AI and deepfake technology enables more sophisticated impersonation techniques. For example, professionals can now replicate fingerprints, browser behaviour, and login credentials to hijack accounts. "Infostealer" malware can copy key parts of a victim's digital identity, helping attackers bypass two-factor authentication and other security measures to maintain unauthorised access.

New types of AI-driven cybercrime are also emerging, such as "typosquatting" attacks that exploit errors made by AI coding assistants. These assistants sometimes suggest software packages that don't actually exist. Malicious actors monitor these suggestions, and when they see a fake package name being suggested repeatedly, they create a real—but malicious—package with that name and upload it to public repositories. If developers trust the AI and use the suggested code without verifying the package, their systems may unknowingly install malware, leading to a software supply chain compromise.

The Expert use of AI also amplifies existing threats by automating the criminal process. Cybercriminal networks use machine learning algorithms to scan for vulnerabilities in target systems. This allows them to scale up attacks significantly while reducing the need for human involvement.

This dual-use dynamic broadens the threat landscape, as AI enables a wider range of actors to operate with greater efficiency, precision, and impact.

The following case study highlights the varying impact from AI-enabled deepfakes and the use of synthetic ID, illustrating the growing complexity to CDD authentication processes. It highlights the continued importance of human and technological expertise in detecting inconsistencies that automated systems may overlook.

Box 0.2. Case Studies: AI deepfake synthetic identity

AI technologies are increasingly being integrated into financial services to enhance customer experience and security. However, criminal actors are exploiting these same technologies to perpetrate sophisticated fraud schemes. An emerging tactic witnessed in one jurisdiction involves the collection of stolen identity documents and the creation of "hybrid" synthetic identities—merging elements of both victims' and suspects' information. These fabricated identities are used to open bank accounts, bypass Customer Due Diligence (CDD) controls, and circumvent facial recognition systems, significantly increasing the risks of fraud, identity theft, and other predicate offences.
Authorities of this jurisdiction shared two notable cases illustrating the misuse of AI and deepfake technologies:

- **Case 1: Deepfake Video Conference Scam**
  Criminals used AI-generated deepfakes to simulate a video conference involving a multinational advisory firm. Impersonating senior executives, they instructed the firm's CFO to transfer USD 25 million to a fraudulent project account. While a portion of the funds was successfully frozen, investigations are ongoing to trace the remaining assets.
- **Case 2: Romance and Investment Scam Operation**
  Police uncovered a scam call centre operated by highly skilled individuals. The centre orchestrated romance scams, luring victims into fraudulent cryptocurrency investments and other deceptive schemes.

Authorities explained how deepfake images and synthetic identities were used to bypass CDD processes. In response, the police have implemented a multi-layered strategy to combat deepfake-enabled financial crimes:

Preventive Measures at the CDD Stage

- Deployment of advanced ID verification tools, including advanced "liveness checks" with hardware-based and other forms of biometric authentication, coupled with more advanced multi-factor authentication.

- Strengthening Know Your Customer (KYC) protocols with AI-driven detection systems.

Investigative Measures

- Integration of traditional investigative techniques (e.g., forensic accounting, intelligence gathering) with advanced technologies, such as:
  - AI-powered forensic tools
  - Deepfake detection software
  - Blockchain analytics to trace virtual asset flows
- Establishment of specialised cybercrime units to dismantle cross-border networks and track illicit financial activity
- Appointment of dedicated prosecutors and introduction of enhanced sentencing measures for technology-enabled financial crimes.

These cases underscore the continued importance of human expertise in detecting anomalies that automated systems may miss. In response, financial institutions have begun collaborating with academic institutions and industry partners to:

- Share intelligence
- Test detection methodologies
- Deepen understanding of evolving technological risks

The cases also highlight the critical role of public-private partnerships in maintaining resilience against emerging threats and ensuring that countermeasures evolve in step with technological advancements.

In 2020, the FATF issued specific Guidance on Digital ID to respond to the rapid growth in digital and online payments and the movement of financial services into the digital space. The guidance responded to the evolving vulnerabilities from virtual onboarding and CDD, by suggesting an "informed risk-based approach to relying on digital ID systems" to ensure that financial and other services covered by the FATF Standards guarantee adequate and standardised level of assurance for KYC and CDD. It is now more vital than ever for institutions to implement a sound CDD framework that considers this new threat landscape through this informed risk-based approach.

Addressing the challenge from AI Deepfakes

Detection and good practices for financial institutions and reporting entities

The unpredictable and evolving nature of AI-driven threats demands foresight, innovation, and cross-sector collaboration. The rapid evolution of AI deepfakes fuels a constant technological "arms race", forcing institutions to invest heavily in advanced detection tools and specialised expertise, sometimes external providers of technological solutions. The expansion of digital services requires security measures that are both scalable and seamless, ensuring robust protection without undermining user experience, all while protecting and expanding financial inclusion. Institutions must also navigate a complex regulatory environment, balancing effectiveness with compliance on issues of privacy, consent, and accountability.

Distinguishing between authentic and falsified content now requires advanced technical expertise. Detection can also be enhanced by adopting technological support tools capable of identifying inconsistencies in video and audio content, enhancing multi layered verification, but also by educating compliance teams working closely with technological service providers. The below case study shows how authorities can use different sources to identify AI-enabled deepfakes and their fraud:

Box 0.3. Identification of Deepfake-enabled Securities Fraud

In one country a "deep fraud" case was identified through a series of sources, including reporting from banks, Virtual Asset Service Providers and the public (via judicial complaints) to the Financial Intelligence Unit (FIU).

Conducting operational and strategic analysis, the FIU uncovered a sophisticated fraud involving AI and deepfake technologies, exploited to produce a lifelike video broadcast of a "deepfake" news report involving reputable news anchors reporting on an initial public offering of a fraudulent firm. Deepfakes also included other reputable individuals in the business and academic space.

The perpetrators employed these synthetic videos in two separate investment and stock market fraud schemes using the identifies of specific corporations, including a state-owned enterprise.

Investigations revealed that the software deployed in this incident was procured from a foreign supplier, and that the internet infrastructure used was based in a European jurisdiction outside of the country. Two major financial institutions have been linked to the case, and, according to the national risk assessment, both banking channels and cryptocurrency mechanisms are considered to pose elevated risk exposure.

Authorities have traced the funds and activity of the perpetrators. Funds from the fraud are sent into a central account and then funnelled into virtual assets (VA), using un-hosted wallets which also relied on deepfakes for CDD to authenticate their virtual asset wallets. The identification of the ultimate beneficial owner of these wallets and accounts has been further complicated by the obfuscation techniques using synthetic digital ID for registration with the VA wallet provider (which is itself listed under foreign sanctions regimes).

Authorities involved highlighted the use of new technologies – such as content verification, trainings and special software to identify deepfakes. Authorities also highlighted the requirement for the FIU and other competent authorities to continually monitor and evolve with ongoing risks to tackle the changing risks from new technologies.

AI may also be used by reporting entities to improve effectiveness and CDD measures. As artificial intelligence becomes increasingly embedded in financial services, a growing number of financial institutions offer a compelling example of its transformative potential. AI can be seamlessly integrated into core banking functions. Their embedded technological approach positions them to rapidly adapt to emerging risks and opportunities, making them key players in future public–private cooperation and dialogue on AI-enabled financial services.

Good practices from law enforcement agencies:

The rapid technological evolution of AI presents many challenges for law enforcement agencies, underscoring the need for robust internal capabilities, advanced training, and continuous technological development to effectively prevent, detect, and respond to AI-enabled crime.

The following case study highlights how national authorities are responding to a surge in AI-driven cyber fraud. These developments have prompted a range of countermeasures, from advanced biometric verification and enhanced transaction monitoring to legal reforms and public awareness campaigns, as authorities and financial institutions work to keep pace with the evolving threat landscape.

Box 0.4. Case Study: Deepfakes involving cyber fraud

Recent reports from national authorities from a jurisdiction indicate a surge in cyber fraud incidents involving AI technologies. These attacks are frequently intertwined with traditional methods such as phishing, social engineering, and other forms of digital deception.

A particularly concerning trend is the increased use of voice-based deepfakes and manipulated video content, which are being deployed to impersonate individuals and deceive financial institutions and consumers alike.

Authorities describe the current landscape as a "technological arms race", with both regulators and reporting entities striving to keep pace with rapidly evolving AI capabilities. In response, several key measures have been introduced:

- FIs are encouraged to adopt advanced biometric identification systems and advanced forms of "liveness checks" (e.g. use of hardware, passive and active liveness detection in conjunction, etc.) to verify user authenticity and prevent AI impersonation.
- FIUs are enhancing transaction monitoring systems and leveraging data analytics to detect suspicious patterns linked to AI-driven fraud.
- LEAs have initiated technological reforms, including the establishment of specialised cybercrime units dedicated to investigating and countering AI-related threats.
- Across all sectors, awareness-raising campaigns are being prioritised to educate stakeholders and the public about the risks and indicators of AI-enabled fraud.

The jurisdiction is also reviewing its criminal code to formally recognise the use of AI tools in criminal activity. Proposed amendments would classify such use as a distinct form of criminality and potentially an aggravating factor in sentencing, reflecting the seriousness and sophistication of these offences.

Some FIUs have developed best practices to assist obliged entities in detecting deepfakes in financial activity, focusing on behavioural and transactional anomalies[5]. Key indicators include suspicious patterns such as coordinated activity, rapid transactions to newly opened accounts, and immediate fund withdrawals following deposits. FIUs also monitor for incoherence—such as mismatches between IP addresses and customer profiles or use of a same device by different counterparts—and unusually high transaction volumes, whether originating from high-risk payees or reflected in elevated rates of chargebacks and rejected payments. These practices help strengthen detection frameworks against AI-enabled fraud.

However, detection techniques can quickly become obsolete in this rapidly evolving space. To address this, participants in the June 2025 FATF roundtable emphasised the importance of partnerships between public authorities, the private sector[6], and operational agencies. Given this trend, the need for trained experts in investigations and for specialised expert witnesses is critical.

---

[5] See for example United States FINCEN *'Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions'* https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial ; See also Luxembourg FIU (CRF) *'Trend Aler #1: Use of Deepfakes and AI to circumvent AML/CFT Measures'*

[6] Including technological services providers

Building a pool of qualified experts and witnesses is a necessary first step. Prosecutors must also receive specialised training, not only in the use of AI but also in detecting and mitigating AI-generated forgeries during fraud proceedings.

The creation of robust public–private partnerships, combined with collaboration with think tanks and local networks, is indispensable for sharing knowledge, exchanging good practices, and improving detection capabilities Strengthening these connections is essential to enhancing the collective capacity to combat AI-driven fraud.

To effectively counter the growing threat of AI-enabled deepfakes, financial institutions and law enforcement agencies must not only strengthen detection capabilities but also embrace AI as a proactive tool. Innovative applications—such as AI-driven content verification, biometric analysis, and behavioural anomaly detection—can help identify synthetic media and fraudulent identities in real time. By integrating AI into CDD, transaction monitoring, and investigative workflows, institutions can enhance resilience against deepfake-enabled fraud.

Section II: Horizon Scan: Generative AI and ML - Evolving ML/TF/PF Vulnerabilities

Generative AI, AI agents, General AI and ML/TF/PF

Section II below is a rapid initial forward-looking exploration of emerging trends and risks associated with the misuse of AI which highlights evolving challenges for law enforcement and operational authorities such as FIUs. Conducting a rapid horizon scan, several distinct forms of AI technologies (categorised by deployment style) present new risks for ML, TF, and PF, particularly through tools like:

1) **Discriminative/Predictive Models**[7], which uses data-driven algorithms to detect patterns and make predictions and can be exploited by criminals, terrorist financiers and PF actors to bypass traditional detection systems or automate illicit financial activities.
2) **Generative AI**, which can create realistic synthetic content (see for example section on deepfakes above), fake documents or artifacts that facilitate fraud and deception using diffusion models (image/video generation).
3) **AI agents**, autonomous systems capable of making decisions and taking actions without human intervention, potentially enabling scalable financial manipulation or fraud.

In addition, other technologies on the horizon can be considered. This includes **General AI**, a still-theoretical form of AI with broad, human-like reasoning capabilities, which could pose unpredictable risks if ever realised could strategically design entire laundering pipelines and adapt in real time at a level that may exceed human operators.

All of these technologies pose varying degrees of risk based on likelihood and consequence, and these are shifting constantly with new evolutions in AI.

Potential risks (known-unknowns)

- As outlined above, one ongoing, high impact scenario is the use of **generative AI** (text, image, video, and voice models) to create highly convincing fake people or events that scammers deploy to trick victims into sending money, revealing credentials, or approving transactions.

- **Discriminative / predictive AI** also poses a significant risk, by deploying algorithmic pattern mimicry, where humans (or AI agents) are trained using machine learning to replicate legitimate financial behaviour with high precision. Future money launderers could use machine learning models trained on vast datasets of normal customer transactions (legally and illegally obtained)—such as payroll distributions or trade payments—to generate synthetic transaction sequences that statistically resemble genuine activity. This makes illicit transactions harder to detect, as they blend seamlessly into the broader stream of legitimate commerce, hence, ensuring the security of information systems and safeguarding the data of institutions within the financial sector constitute critical next challenges.

- Another potential high-impact risk is the emergence of fully automated laundering pipelines operated by **AI agents**[8], with minimal human oversight. Criminal organisations could deploy these

[7] These models are widely used in AML/fraud (risk scoring, SAR prediction, anomaly detection), so attackers have strong incentive to target or exploit them.
[8] IBM: '*What are AI Agents*?' https://www.ibm.com/think/topics/ai-agents

agents at scale to overwhelm systems and exploit vulnerabilities in detection and enforcement mechanisms. These agents may be capable of identifying system-wide weak points, rerouting transactions in real time to avoid scrutiny, and adapting dynamically to compliance controls. To mitigate such threats, financial institutions will need to deploy advanced detection systems capable of identifying and responding to these sophisticated, automated behaviours[9].

- A further concern lies in the potential future development of **General AI**—a form of artificial intelligence with broad, human-like reasoning and decision-making capabilities. While still theoretical, General AI could pose unpredictable and systemic risks if leveraged by criminal actors. Its ability to autonomously learn, strategies, and adapt across domains could enable the orchestration of complex financial crimes, including cross-border laundering schemes, manipulation of financial markets, or exploitation of regulatory loopholes. The lack of transparency in how such systems operate would further complicate detection and accountability, underscoring the need for proactive horizon scanning and regulatory preparedness.

Potential Scenarios involving AI:

AI poses a multi-faceted and highly complex threat to the way that LEAs tackle ML, TF and PF. There are a wide range of ways that AI could be used by bad actors to commit or facilitate the commission of ML. Below are some "scenarios" (including several drawn from real-world cases) that elicit how AI may be used to facilitate professional ML and evade prosecution:

Scenario 1: Use of Generative AI to automate and facilitate layering to legitimise proceeds of crime

Perpetrators use a suite of generative and agentic AI systems to produce a convincing documentation "paper trail" that supports a complex fraud and layering scheme. Criminals may generate fake invoices for professional services to generate illicit or convincingly fake billing of services in the layering of funds from fraud. The use of AI in this case is used to create documentation to deceive obliged entities and authorities (or auditors, etc.) so that transactions or economic activities appear real, when in fact it is a complex layering system.

Scenario 2: Agent-AI-assisted professional ML (third-party ML)

Professional ML actor designs/creates a series of AI agents. The agents automatically conduct a set of tasks such as completing online purchases, depositing funds into accounts and other activities (e.g. online gambling, gaming, small purchases) and deploys AI bots scheduling and executing micro-transactions, moving money through a series of accounts when risk is lowest. This can also be enabled by fraudulent synthetic or co-opted IDs to perform these as part of a complex layering and smurfing operation.

Scenario 3*:* AI-facilitated Agent in transnational ML using straw account holders.

This describes an ML scheme that automates recruitment/management of straw account holders (mules) and executes high-volume micro-transactions into hundreds of mule accounts to launder large sums (e.g., via online gaming/gambling platforms). To layer the funds, AI agents automate transactions into hundreds of mules' bank accounts, used to launder millions of USD a month through online gaming / gambling platforms. The perpetrators also bypass digital ID verifications using AI-generated deepfakes when checks are conducted.

[9] Advanced detection approaches could include graph/network analytics to uncover hidden laundering rings; real-time ML transaction monitoring with anomaly detection; adaptive customer profiling; consortium intelligence sharing; adversarial-robust ML with continuous red-teaming; hybrid human-in-the-loop review pipelines; synthetic-data testing of agent behaviours; and explainable AI governance to ensure regulatory oversight.

Scenario 4: Professional ML/TF and sanctions evasion AI advisor

A sanctions-evasion specialist at a small trust & company service provider (TCSP) leverages a professional, agentic AI system to research, compile and operationalise weak-jurisdiction strategies for evading targeted financial sanctions (TFS) for proliferation and terrorist-financing (PF/TF) controls. The stack combines large language models (LLMs) with retrieval-augmented search over legal/regulatory texts, structured knowledge-graphs of jurisdictions and corporate vehicles, and automated planning agents. It automatically gathers and synthesises public and legal sources, ranking and suggesting the best routes for funds and goods to evade scrutiny and controls.

Relatedly, it is also conceivable that sanctions evaders may use a similar agent to that described in Scenario 4 combining aspects of the three other scenarios above (e.g. creating synthetic AI documentation in scenario 1, and potentially using AI agents noted in scenario 2) to commit document fabrication in trade-based money laundering and sanctions evasion by creating falsified invoices and incorporate shell import-export firms with fake business records in jurisdictions with few CDD measures in place. It may even use AI to develop fake websites and virtual suppliers, with fake product catalogues, shipping documents, email correspondence between non-existent actors, etc.

Outlining ongoing and future challenges for LEAs

The integration of AI into financial and commercial systems introduces significant new risks for AML/CFT/CPF regimes. While AI holds promise for enhancing monitoring and detection capabilities, it simultaneously empowers illicit actors with sophisticated tools to obscure their activities, fabricate documentation, and exploit regulatory blind spots.

AI enables criminals to generate transactional patterns that closely mimic legitimate behaviour, effectively bypassing conventional monitoring systems and FIU detection. Adversarial AI can be trained to recognise and avoid red flags by analysing typology reports, guidance documents, and other regulatory materials—deliberately evading detection. By leveraging large-scale historical and public datasets, AI systems can develop adaptive countermeasures that evolve in response to law enforcement strategies.

Investigative processes are equally vulnerable. Criminal networks can deploy AI-powered bots to mine regulatory intelligence, mutual evaluation reports, and open-source data to identify weak jurisdictions, under-regulated sectors, and exploitable gaps. These agents can map optimal laundering routes, pinpoint areas with low enforcement risk, and even innovate laundering techniques through coordinated darknet "hackathons" or automated experimentation. Advanced obfuscation tactics—such as synthetic trade flows and AI-generated shell company networks—can mislead or delay law enforcement efforts.

In the realm of asset recovery, AI accelerates the concealment and movement of illicit funds. AI-enabled mixers, autonomous wallets, and dynamic routing systems can fragment and transfer assets across multiple jurisdictions in near real time. These tools can also generate convincing but fraudulent documentation to obscure the origin of funds, complicating asset tracing and freezing efforts.

Finally, prosecution can also face unique hurdles from AI. The complexity of AI-assisted financial crime can outpace the technical understanding of investigators and courts. The sheer volume of synthetic or falsified evidence generated by AI may overwhelm authorities and obscure the chain of custody. Moreover, the "black box" nature of many AI systems can undermine the evidentiary value of their outputs if the underlying decision-making processes cannot be clearly explained or audited.

While the challenges outlined above illustrate the growing complexity of AI-enabled financial crime, some jurisdictions have begun to respond with innovative solutions. The following example from demonstrates how tools such as Generative AI can also be harnessed to strengthen detection and verification capabilities.

Box 0.5: Financial Institutions' utilisation of AI as a tool to detect patterns

Financial institutions in one jurisdiction have begun implementing practices to address risks associated with Generative AI. These include the development of advanced systems for document verification and anti-counterfeiting, as well as collaboration on industry standards to detect tampering in digital content.

Through transaction monitoring, a financial institution identified a company exhibiting several patterns of suspicious transactions, such as abnormal volumes, timings, and amounts. In order to verify the authenticity of its business activities, the financial institution requested the company to provide relevant photographic evidence of its business premises. Using its intelligent anti-counterfeiting system, combined with big data analysis to analyse the photos, the institution detected that the background elements of the photo of the company's storefront and interior bore a strong resemblance to a counterfeit document from a customer previously identified as high risk. As a result, the company was deemed highly suspicious of engaging in fictitious business activities, with the use of artificial intelligence, enabled the early detection of fraud.

Regulatory approaches to AI

There is currently no consistent or enforceable global standard on the regulation of AI. Several jurisdictions and intergovernmental bodies are developing regional or global guidance[10]. However, there is currently no overarching framework for integrating AI into a broader regulatory system. While some jurisdictions are actively developing rules to ensure AI is used safely and aligns with existing or new legal standards, other jurisdictions—particularly those with limited regulatory capacity and lower capacity—are less likely to do so.

Past FATF work on Generative AI and ML/TF/PF

The FATF's 2021 report, '*Opportunities and Challenges of New Technologies for AML/CFT*', highlighted the significant potential of AI and machine learning to support Financial Intelligence FIUs, supervisors, and other law enforcement agencies. The report notes that these technologies can replicate human analytical processes and uncover novel methods for detecting ML, TF and PF, emphasising that AI can "*enhance the capabilities of actors to respond to risks and implement requirements more effectively.*"

Since then, AI has rapidly evolved. Once limited to specialised institutions, these tools are now widely available, offering enormous benefits but also creating new and complex risks when misused. This shift underscores the importance of ongoing dialogue and joint efforts by the FATF

[10] See for example the **EU's** *AI Act*, a legal framework on AI to harmonise laws and develop a set of risk-based rules on AI and foster "trustworthy AI". The AI act prohibits a series of practices for AI services offered by platforms.
China has also issued regulations and technical standards for compliance of service providers with regulations such as the *Interim Measures for the Management of Generative Artificial Intelligence Services*.
In 2019, **Singapore** was the first nation to launch a Model AI Governance Framework, and in 2024 released a proposed *Model AI Governance Framework for Generative AI*.
See also the **OECD's** 2024 updated *Open AI principles* ,an intergovernmental standard on AI.

and the wider global community to better understand and address both the opportunities and challenges that come with these technologies.

FATF's Standard on emerging technologies

The FATF has adopted a broad and inclusive approach to "New Technologies," (FATF Recommendation 15) requiring reporting entities to identify and assess risks associated with emerging products. As AI advances, this approach provides a strong foundation for further collaboration—helping countries and stakeholders explore how technologies such as deepfakes and autonomous agents create new vulnerabilities, and how these risks can be effectively managed. There is an opportunity for the FATF and its global partners to work together in ensuring that the benefits of AI are harnessed, while the associated risks are addressed in line with FATF Standards.

Overall Conclusion and Recommendations

Artificial intelligence and deepfake technologies are reshaping the financial crime landscape, introducing both unprecedented risks and new opportunities for detection and prevention. As these tools become more accessible and sophisticated, they challenge existing AML/CFT/CPF frameworks, particularly in areas like customer due diligence, identity verification, and transaction monitoring. The FATF's horizon scan on this topic underscores the need for enhanced vigilance and continuous innovation. To stay ahead of evolving threats, stakeholders must not only strengthen safeguards but also harness AI responsibly to reinforce the integrity of the global financial system.

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit www.fatf-gafi.org.