Testimony of Ari Redbord, Global Head of Policy, TRM Labs

Before the House Judiciary Subcommittee on Crime and Federal Government Surveillance
Hearing on: “Artificial Intelligence and Criminal Exploitation: A New Era of Risk”
July 16, 2025 | Room 2141, Rayburn House Office Building

Introduction

Chairman Biggs, Ranking Member McBath, and Members of the Subcommittee, thank you for the opportunity to testify today on the urgent and evolving threat posed by artificial intelligence in the hands of criminal actors. I am honored to appear before you on behalf of TRM Labs, where we work every day with law enforcement, financial institutions, and national security agencies to detect, investigate, and prevent illicit financial activity in the digital asset ecosystem.

Before joining TRM, I spent about eleven years as a federal prosecutor at the US Department of Justice and later as an official in the US Treasury Department's Office of Terrorism and Financial Intelligence. In those roles — and now at TRM — I've seen one truth borne out time and again: criminals are often the earliest adopters of transformative technology. They were among the first to weaponize automobiles to move illicit goods across state lines, adopt pagers and cell phones to coordinate narcotics networks, utilize encrypted messaging apps to evade surveillance, and exploit cryptocurrencies to steal and transfer illicit proceeds at the speed of the internet. And now, they are embracing artificial intelligence (AI).

The FBI was created in 1908 — the same year the Model T was introduced — to pursue a new breed of criminal exploiting America's growing highway system to move faster and farther than ever before. Today, we find ourselves at a similar moment. Just as AI is revolutionizing medicine, education, and productivity, it is also unleashing an unprecedented era of speed, scale, and sophistication in criminal activity.

During my time at both DOJ and Treasury, I saw how quickly illicit actors adapted — using shell companies and darknet tools, exploiting gaps in global anti-money-laundering enforcement, and increasingly turning to cryptocurrency to move funds across borders. Now, at TRM, I see that adaptation accelerating. AI is removing human bottlenecks. It's not just enhancing traditional fraud — it's creating entirely new categories of criminal threat. And we are only beginning to understand the scale of this shift.

We are rapidly approaching a world in which the bottleneck for crime is no longer human coordination, but computational power. When the marginal cost of launching a scam, phishing campaign, or extortion attempt approaches zero, the volume of attacks — and their complexity — will increase exponentially. We're not just seeing more of the same; we're seeing new types of threats that weren't possible before AI. Novel fraud typologies, hyper-personalized scams, deepfake extortion, autonomous laundering — the entire criminal ecosystem is shifting.

That is why today's hearing matters. We must recognize that in the same way criminals are leveraging AI to disrupt and deceive, law enforcement and national security agencies must be empowered to use AI to defend and respond. This is not optional. It is foundational to preserving public trust — and the social contract itself. If adversaries are deploying large-scale, AI-enabled crime with impunity, and if the public no longer feels that government can protect them, we risk a breakdown of that trust. The consequences are not just individual harms — they are systemic, national security-level threats to our institutions and civic cohesion.

In the testimony that follows, I will walk through the state of AI-enabled crime across the ecosystem — from scams and fraud, to ransomware and cyberattacks, proliferation finance to disinformation and child exploitation. I will share what we are seeing at TRM through our investigations and data from Chainabuse, our open-source scam reporting platform. I will outline how TRM is leveraging AI to fight back. Finally, I will offer recommendations for how Congress can empower public-private collaboration, update legal frameworks, and help ensure that the tools of safety evolve as fast as the tools of harm.

The rise of AI-enabled crime and fraud

Artificial intelligence has revolutionized numerous industries, enhancing productivity and innovation at unprecedented speed. From increasing access to healthcare, to advanced climate modeling, to improving efficiency and security in workplaces — AI is enabling better, more sustainable outcomes across society.

However, this same transformative technology is also being leveraged for criminal purposes, posing significant threats to global security and societal stability. Malign actors are increasingly using AI to carry out hacks and fraud, create deepfakes for extortion and misinformation, and conduct cyberattacks at scale. As AI technology becomes more sophisticated, so too will the ways in which criminals exploit it for illicit gain.

TRM Labs has documented how AI removes the traditional bottlenecks that once constrained criminal activity. What used to require a team of humans — language translation, phishing email development, video editing, malware deployment — can now be accomplished by a single AI agent trained to operate at scale. Further, as at-home technology rapidly advances, powerful open-source LLMs and high-performance hardware will lower the barrier to entry and make it easier for an even wider range of illicit actors to operate independently without relying on expensive data centers.

We are watching, in real time, the industrialization of cyber-enabled crime.

How criminals are using AI

Criminals are increasingly incorporating AI into every stage of the illicit value chain. They use generative AI tools to write phishing emails in dozens of languages, create deepfake videos for extortion, develop synthetic identities for money laundering, and execute autonomous cyberattacks. TRM Labs categorizes this criminal adoption of AI across three phases:

- Horizon phase: AI use is possible but not yet operational. We see potential applications in areas like proliferation finance, where rogue states such as North Korea — already responsible for over USD 1.6 billion in crypto hacks in 2025 alone — could use AI agents to identify cybersecurity vulnerabilities or automate complex laundering schemes.

- Emerging phase: AI tools are deployed alongside human operators. This is where most AI-enabled fraud and ransomware operations exist today, with human actors directing large language models (LLMs) and deepfakes to scale their attacks. For example, the Internet Watch Foundation recently found over 3,500 AI-generated child sexual abuse images on a dark web forum, including content that overlaid children's faces onto adult actors. AI-generated deepfake voices are also increasingly used to impersonate executives or loved ones in extortion scams.

- Mature phase: AI dominates criminal activity. While no illicit domain has fully reached this point yet, we are moving toward it. AI systems are beginning to interface autonomously with email clients, databases, and cryptocurrency wallets, and they are being trained to optimize for outcomes such as revenue generation or influence. The recent "Terminal of Truths" case — in which an autonomous AI agent successfully interacted with users and bots to accumulate digital assets in a crypto economy — foreshadows this next frontier.

AI and ransomware

Ransomware actors are among those eagerly integrating artificial intelligence to enhance the efficiency, scale, and success rate of their attacks. AI-driven tools can generate highly personalized phishing emails and social engineering schemes that mimic trusted communications, often using deepfake audio or video to impersonate legitimate individuals.

On the technical front, ransomware developers are deploying AI to create polymorphic malware that continually adapts to evade detection by traditional security systems. Meanwhile, machine learning algorithms can identify and prioritize high-value targets based on their financial standing, cybersecurity posture, and likelihood to pay — making ransomware attacks more strategic and profitable.

Looking ahead, AI is poised to further transform how ransomware proceeds are laundered through blockchain ecosystems. Autonomous laundering agents could execute complex schemes involving mixers, tumblers, and rapid cross-chain swaps, while leveraging decentralized finance (DeFi) protocols to layer transactions and obscure fund origins. Advanced AI models may also simulate legitimate transaction patterns to evade detection, dynamically adapting to new compliance tools and analytics.

These advancements create profound challenges for law enforcement, demanding greater investment in technology, expertise, and cross-jurisdictional coordination to counter rapidly evolving threats.

AI-enabled cyberattacks

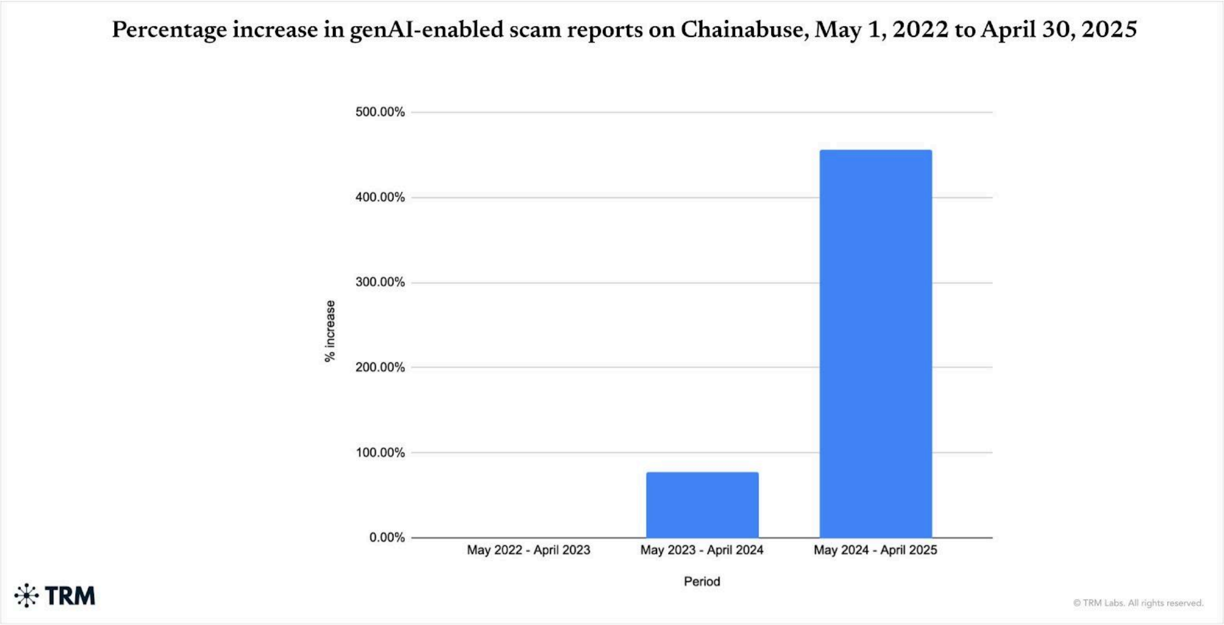
Like ransomware attacks, the intersection of AI and cyberattacks has the potential to dramatically increase the scale, speed, and sophistication of exploits targeting critical infrastructure and financial systems. AI enables cybercriminals and nation-states to automate vulnerability scanning and craft highly targeted, devastating attacks with minimal human oversight.

For instance, AI-powered tools can autonomously scan for weaknesses in critical sectors such as energy grids, hospitals, communication networks, and global financial systems. These vulnerabilities could include misconfigurations, unpatched systems, or gaps in security protocols, which can then be exploited with tailored malware or ransomware. Automating these processes significantly shortens the time it takes to breach security defenses, leading to a higher frequency and greater severity of cyberattacks. This presents serious risks, especially for sectors where AI-driven exploits could cause widespread disruption, affecting essential services and national security.

In the context of cryptocurrency and financial institutions, AI further enhances the ability of cybercriminals to identify and exploit weaknesses in security measures. By automating large-scale phishing campaigns and generating hyper-targeted exploits, criminals can more efficiently infiltrate systems and steal funds. The use of AI isn't just about increasing the volume of attacks; it amplifies their impact by enabling more precise and scalable efforts. Nation-state actors, like North Korean IT workers, could leverage AI to conduct automated scans of financial infrastructure, craft advanced exploits, and launder illicit funds,, making detection and attribution significantly more challenging. As AI technology continues to evolve, so too must our cybersecurity infrastructure. Strengthening defenses and ensuring better coordination between private and public sectors is critical to countering these rapidly advancing threats.

AI-enabled scams

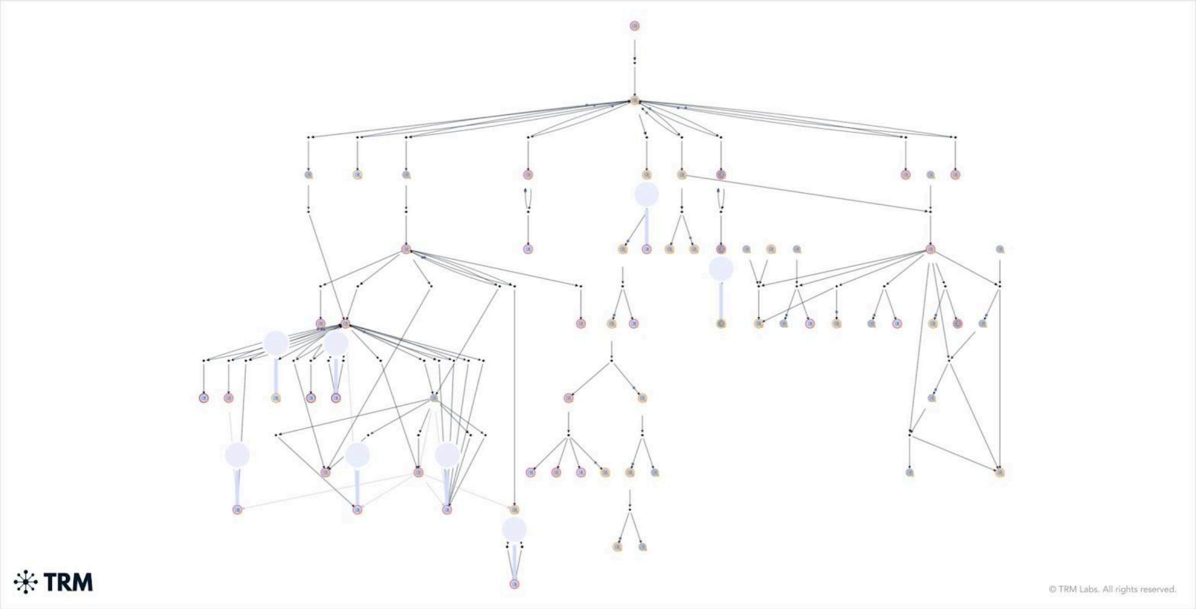
Perhaps the most widespread use of AI by criminals today is in perpetrating scams and fraud schemes against the public. In fact, data from Chainabuse — TRM Labs' open-source fraud reporting platform — shows that reports of generative AI-enabled scams between May 2024 and April 2025 rose by 456% compared to the same period a year earlier (which itself had seen a 78% rise over the year before). This explosion in readily available genAI tools has directly fueled a surge in AI-enabled fraud.


Percentage increase in genAI-enabled scam reports on Chainabuse, May 1, 2022 to April 30, 2025

The most commonly reported type of AI-enabled scam is the deepfake cryptocurrency giveaway scam.

In this scheme, fraudsters create a genAI-powered twist on the classic "double-your-bitcoin" ploy. They compromise popular YouTube channels and use them to stream manipulated videos — often repurposing real interviews or speeches by prominent crypto figures such as Elon Musk, Ripple CEO Brad Garlinghouse, MicroStrategy CEO Michael Saylor, or Ark Invest CEO Cathie Wood — with scam websites and QR codes overlaid on the video. Using deepfake technology, the scammers alter these videos to make it appear that the celebrity is personally endorsing a fraudulent giveaway or investment opportunity (for example, claiming they will double any cryptocurrency that users send in). These highly realistic streams are difficult to distinguish from authentic content, and they have tricked victims into sending millions of dollars in crypto to the scammers' addresses.

In June 2024, a Chainabuse report described a deepfake Elon Musk promoting a supposed AI-driven trading platform, which lured victims to scan a QR code causing the transfer of bitcoin. Funds from that address go to various destinations — but primarily to a few large exchanges, particularly MEXC. The scammers who defrauded this victim and others received at least USD 5 million between March 2024 and January 2025. TRM also observed small amounts of funds being sent to two darknet markets and a cybercrime entity.



TRM's Graph Visualizer has been used to map how scammers moved funds from these deepfake giveaway scams into exchange accounts like MEXC, illustrating the speed at which criminals can cash out once victims are duped

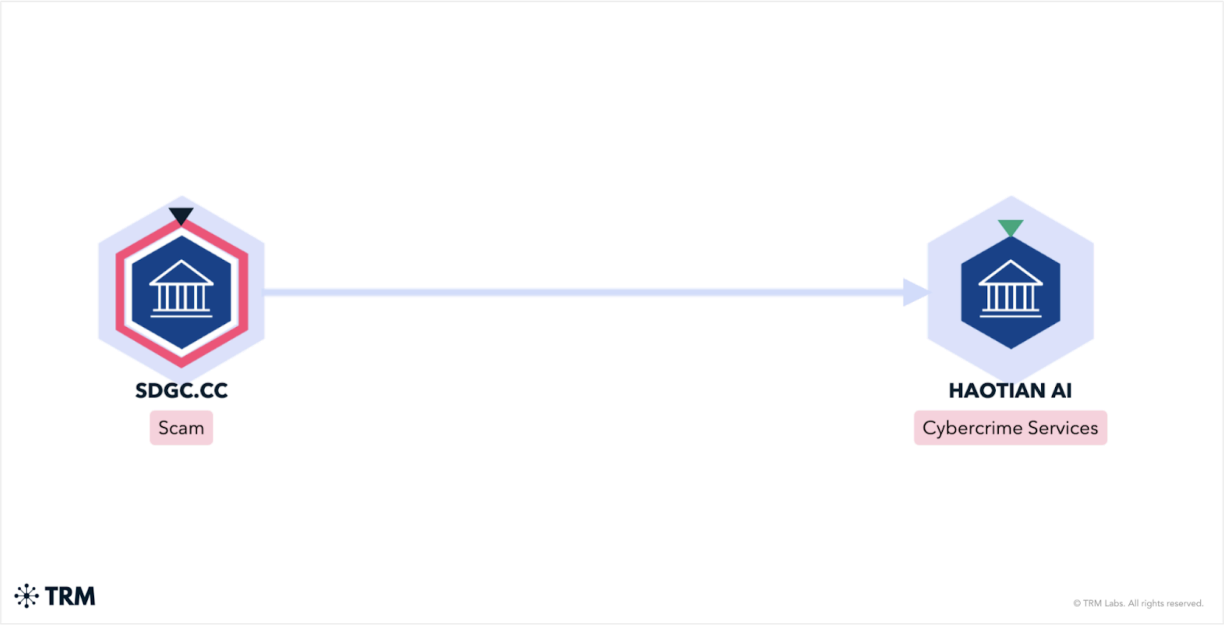
Deepfake impersonation scams and financial grooming

It is not only public figures who are being mimicked with deepfakes. Scammers are also using the technology to impersonate private individuals in real-time interactions.

Live deepfake technology (which can overlay one person's face onto another's in a live video call) means criminals no longer need large volumes of data to convincingly pose as someone else. For example, in February 2024, a multinational company in Hong Kong was defrauded out of millions of dollars after an employee joined a video meeting with individuals pretending to be the company's executives. The scammers used real-time face- and voice-swapping AI tools to perfectly mimic the executives' appearance and speech, tricking the employee into authorizing a large transfer of funds.

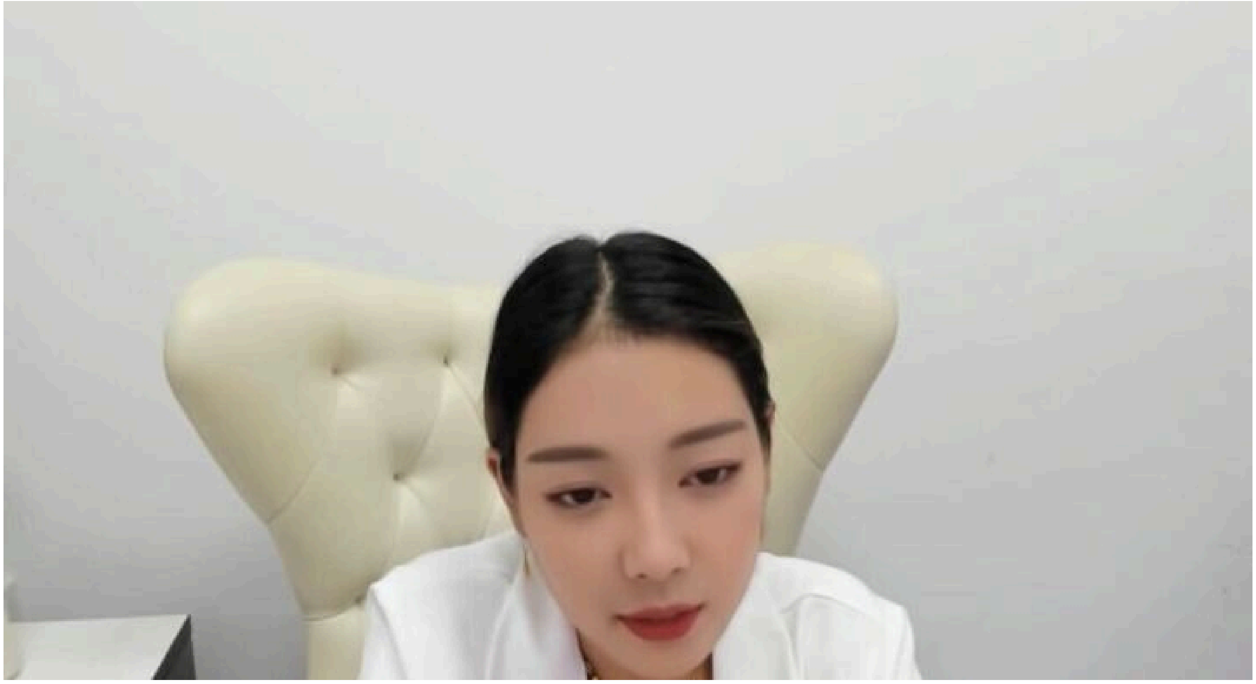
In another common scheme, criminals clone the voice of a victim's family member or friend and call with a plea for help. The impostor (speaking in a loved one's voice) might claim to be in an emergency that requires immediate cash, or urge the victim to invest in a "can't-miss" opportunity that the friend purportedly has made money from. These AI-voice scams have led to heartbreaking losses, preying on victims' trust in those closest to them.

Deepfakes are also being used to bolster long-term fraud operations like romance or investment scams (so-called "pig butchering" schemes). TRM has identified cases where scammers utilize deepfake-as-a-service providers to enhance their deception during months-long grooming of victims. In one operation we traced, crypto payments from victims of romance/investment grooming scams were sent directly to platforms offering AI-generated video tools — strong evidence that organized scam networks are paying for deepfake technology as part of their criminal toolkit.



As shown in TRM Graph Visualizer, a scam entity sends funds to an AI-as-a-service entity, demonstrating scammers' willingness to pay for such services

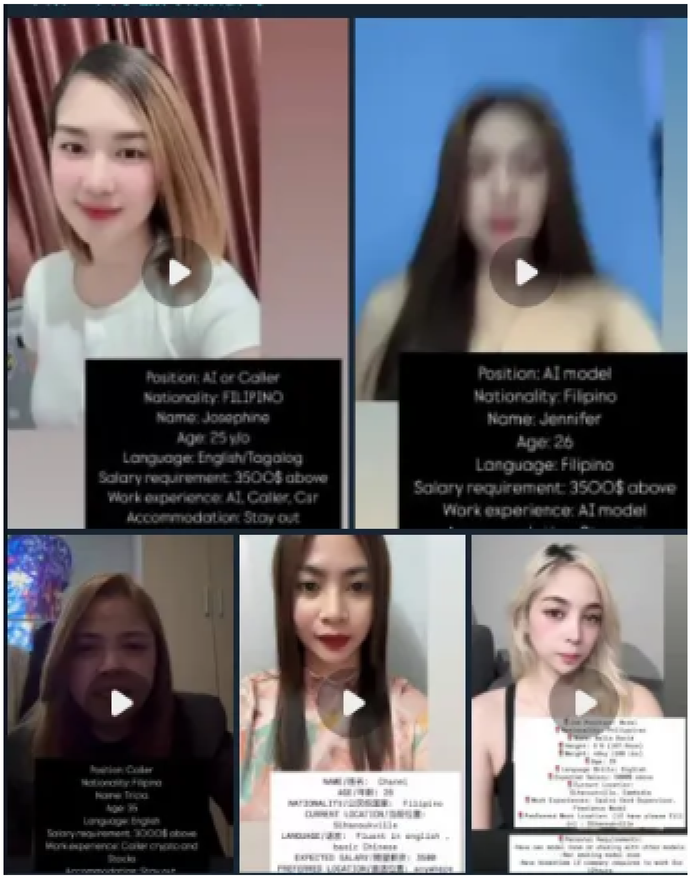
Our investigators even encountered a scammer who appeared on a video call using a deepfake face overlay — evidenced by the person's unnatural-looking hairline and other digital artifacts. AI detection software later confirmed that the video was likely manipulated. This specific scam — along with related schemes tied to the same group — has defrauded victims of at least USD 60 million. The potential financial gains of these AI-augmented "pig butchering" scams are staggering.



Likely live deepfake used in financial grooming scam

As generative AI becomes more prevalent, the general public is also becoming more aware that video or audio evidence can be faked. To counter rising skepticism and appear legitimate, some scam operations are now blending real people with AI technology.

For example, TRM found evidence of women in Cambodia advertising their services via Telegram as "real face models" (as opposed to purely AI-generated personas) for scam call centers and online casinos. In these operations — when a victim insists on a live video chat — the scammers will have one of these human accomplices appear on camera. The "model" might then use a subtle deepfake filter to alter her appearance — making herself look more attractive or even to resemble a specific person — thereby ensuring the victim remains convinced of her identity.



Position: AI or Caller
Nationality: FILIPINO
Name: Josephine
Age: 25 y/o
Language: English/Tagalog
Salary requirement: 3500$ above
Work experience: AI, Caller, Csr
Accommodation: Stay out

Position: AI model
Nationality: Filipino
Name: Jennifer
Age: 26
Language: Filipino
Salary requirement: 3500$ above
Work experience: AI model

Position: Caller
Nationality: Filipino
Name: Tricia
Age: 35
Language: English
Salary requirement: 3000$ above
Work experience: Caller crypto and Stocks

NAME/姓名: Chanel
AGE/年龄: 26
NATIONALITY/公民身份国家: Filipino
CURRENT LOCATION/当前位置: Sihanoukville
LANGUAGE/语言: Fluent in english , basic Chinese
EXPECTED SALARY/期望薪资: 3500
PREFERRED LOCATION/首选位置: anywhere

[illegible]
Language Skills: English
Current Location: Sihanoukville, Cambodia
Work Experience: [illegible] Freelance Model
Preferred Work Location: [illegible] Sihanoukville
Personal Requirements:
[illegible]

Women claiming to have experience working as "AI" and "real face" models

By using a real human presence augmented with AI visuals, criminals are attempting to overcome victims' suspicion of fully synthetic media.

AI agents and fully automated fraud operations

Autonomous AI agents are emerging as a powerful force-multiplier for both legitimate and illicit operations. Unlike a standard AI tool that only responds to individual prompts, an autonomous agent can proactively carry out complex, multi-step tasks with minimal human oversight. In the hands of bad actors, these agents are being weaponized to industrialize fraud at a scale not previously possible. Criminals program AI agents to scrape public data (names, social media profiles, job roles, interests) and then craft hyper-personalized scam messages targeting those individuals.

They also use agents to automate mass outreach across email and social media platforms, deploy LLM-powered chatbots and fake "customer support" desks to lure victims — often conversing with targets in their preferred language and cultural context to maximize credibility — and even run simulations to test different social engineering scripts in virtual environments to discover which are most convincing. Some fraudsters have begun using AI agents to manage the “back office” of their schemes as well: coordinating money laundering workflows, performing reconnaissance on law enforcement activity, and dynamically tweaking their scam strategies based on real-time feedback (for example, analyzing which phishing emails or scam websites are yielding the highest response rates from victims).

While many AI systems have built-in safeguards intended to prevent illicit use, criminals are finding ways around them. Through clever prompt engineering, offenders can manipulate AI models into revealing prohibited information or stratagems. For instance, a scammer might pose as an academic researcher or software developer when interacting with a large language model, coaxing it to provide step-by-step instructions for fraudulent schemes under the guise of legitimate inquiry.

This is no longer a theoretical concern — TRM researchers recently conducted an experiment by asking a supposedly restricted AI assistant how scammers might optimize their fraud operations using autonomous agents. Disturbingly, the tool responded with a surprisingly detailed set of illicit tactics, proving that current guardrails can often be circumvented. It is a stark reminder that as AI capabilities advance, so too must our vigilance against their malicious use.

AI in healthcare fraud

Earlier this month, the US Department of Justice (DOJ) announced the largest health care fraud takedown in US history — charging 324 defendants across 50 federal districts and 12 State Attorneys General’s Offices for schemes involving more than USD 14.6 billion in intended losses. The operation targeted organized networks exploiting health care systems and patient data at scale, with a renewed emphasis on the convergence of health care fraud and modern financial laundering techniques, including the use of cryptocurrency.

In one of the cases, charged in the Northern District of Illinois, Pakistani executives were accused of using artificial intelligence to generate fake beneficiary consent recordings to bill Medicare fraudulently for USD 703 million in services. The scheme involved nominee-owned medical supply firms, AI-generated patient data, and offshore laundering. Approximately USD 44.7 million was seized across domestic and international accounts.

The use of AI to create fraudulent documents to bypass KYC and other ID verification checks

A growing example of criminal use of AI is the creation of fraudulent state-issued IDs designed to bypass Know Your Customer (KYC) and other identity verification checks. AI-powered services now generate highly convincing fake driver's licenses and passports, making it easier for criminals to evade detection during KYC procedures. These counterfeit documents can mimic real state-issued IDs from multiple countries, allowing criminals to pass through KYC checks on financial platforms, including cryptocurrency exchanges, banks, and other financial institutions, which typically rely on such IDs to confirm a user's identity.

Terrorist financiers could use fake IDs generated by AI to open accounts on financial platforms, allowing them to anonymously raise and transfer funds for illicit activities without detection. Similarly, money launderers and North Korean IT workers could exploit these fake identities to bypass KYC checks, moving stolen or sanctioned funds across borders while evading law enforcement tracking.

One notable example is OnlyFake, an AI-driven service that creates fake IDs for as little as USD 15, including passports and driver's licenses from 26 countries. These IDs have successfully bypassed KYC controls on cryptocurrency exchanges, banks, and other financial institutions, enabling cybercriminals and illicit actors to open accounts and move funds anonymously. As a result, fraudsters can exploit these fake documents to launder money and hide their activities.

To combat this, companies like Get Real Labs are developing tools to detect AI-generated fake IDs, helping to strengthen security and prevent criminals from circumventing identity verification processes.

Sextortion and synthetic CSAM

One of the most disturbing developments in AI-enabled crime is the use of artificial intelligence to produce fake sexual content for exploitation and blackmail — specifically, the creation of synthetic child sexual abuse material (CSAM).

In 2024, the Internet Watch Foundation found over 3,500 AI-generated images of child sexual abuse on a single dark web forum. These ranged from fully AI-synthesized depictions of abuse to "deepfake" creations where a real child's likeness was digitally mapped onto adult pornographic content. Such images and videos are traded in underground forums and shared via encrypted messaging apps, making it very difficult for authorities to track their spread or identify the perpetrators. This is consistent with TRM's own investigations on the use of AI in creating CSAM.

AI-generated CSAM also exposes troubling gaps in our legal framework. Many child protection laws were written to address crimes involving real victims, and they struggle to account for imagery with no direct human victim that still causes harm. Even if no actual child was abused in the creation of an image, the material is psychologically damaging — both to the children whose likenesses are used and to society at large. Moreover, synthetic pornographic content is increasingly being weaponized in sextortion schemes: criminals threaten to distribute fake intimate images of someone (for instance, a doctored nude or a video that appears to show a minor) unless the victim pays them, often demanding cryptocurrency for its ease of transfer and anonymity.

Law enforcement must be equipped with the tools and authorities to investigate and prosecute these cases. That includes improved methods for tracing cryptocurrency flows associated with synthetic CSAM marketplaces and explicit legal provisions to charge those who produce or distribute AI-generated sexual abuse images — even if a loophole in current law means no real child was physically harmed.

Using AI to fight AI-enabled crime

The solution to the criminal abuse of AI is not to ban or stifle the technology — it is to use it, and use it wisely. We must stay a step ahead of illicit actors by leveraging the same innovations they use for bad, for good.

At TRM Labs, we embed AI at every layer of our blockchain intelligence platform to help fight financial crime. We use machine learning models and behavioral analytics to flag complex obfuscation techniques, trace illicit cryptocurrency transactions in real time, and discover novel criminal typologies before they can scale.

In practical terms, this means our tools are continuously becoming smarter and faster. For example, TRM's Signatures® recognizes on-chain patterns linked to known scam campaigns, money-laundering networks, and darknet market activity. And our interactive Graph Visualizer allows investigators to quickly follow digital money trails through hundreds of wallet hops, automatically highlighting and summarizing complex paths of funds a human analyst might struggle to unravel.

Today, TRM is developing and deploying AI "defense agents" at scale to map illicit networks, triage threats, and surface early warning signs to help global law enforcement agencies move faster, trace complex laundering schemes, and focus on the highest-risk activity. These are not theoretical ideas — they are operational tools currently being used in the field that help detect and dismantle illicit networks in real time, often stopping criminal schemes before they can do even more harm.

TRM Labs has actively partnered with law enforcement agencies around the world, providing advanced analytics and investigative leads that have directly contributed to arrests, indictments, and the recovery of victim funds. Through a combination of blockchain tracing, AI-driven pattern recognition, and human expertise, we've assisted in cases ranging from deepfake investment scams and romance fraud to illicit cryptocurrency exchanges laundering ransomware proceeds.

As threat actors scale up their schemes with AI, our collective defenses must scale up as well. It is crucial that law enforcement, financial institutions, and intelligence providers be equipped with cutting-edge investigative technology — and that they work in concert across jurisdictions and sectors to combat these threats. In parallel, we must continue to educate and alert the public about these new dangers. AI will undoubtedly shape the next generation of financial crime, but with collaboration and innovation, it can also become the key to preventing and defeating those crimes.

Guiding Principles for Safe and Effective AI in Law Enforcement

As we consider how to responsibly deploy AI in law enforcement and national security contexts, it's important to emphasize the foundational principles that must govern its use. At TRM Labs, we have learned firsthand that AI must not only be powerful but principled. We recommend the following design principles as a baseline for any AI used in investigative or intelligence settings:

- Guardrails: AI should be explicitly limited to predefined, auditable tasks. These systems must be designed with constraints that prevent unauthorized or unintended behavior.
- Compliance: AI must operate within the legal authorities of each agency and jurisdiction to ensure legal, targeted usage.
- Human Control: Human analysts remain in the loop for critical decisions, with AI initially focused on automating low-risk or repetitive tasks. As trust and oversight mechanisms

mature, selective autonomy could be introduced where mission-appropriate and policy-aligned.

- Transparency: Every action taken by an AI system should be fully traceable. Analysts must be able to understand how a result was generated, and audit logs should enable reproducibility for use in court.
- Flexibility: Law enforcement should not be locked into a single model or vendor. Modular architectures allow agencies to swap in best-in-class models for specific tasks, ensuring long-term adaptability.

These principles are not hypothetical. They reflect what we are already building into TRM's AI-driven tools to ensure they are safe, transparent, and effective for frontline investigators. If adversaries are using AI at scale, we cannot meet this moment with manual processes alone. We must respond with purpose-built AI—anchored in principles that protect both effectiveness and civil liberties.

Policy recommendations: Meeting the AI-enabled crime threat with urgency and coordination

The rapid rise of AI-enabled crime presents a national and global challenge that demands an equally swift and coordinated response.

The Department of the Treasury, alongside law enforcement partners at the FBI, HSI, IRS-CI, and the Department of Justice, as well as regulatory and intelligence agencies across the interagency, must invest in next-generation tools, update outdated legal frameworks, and build new mechanisms for information sharing.

Recommendation 1: Strengthen AI capabilities for financial crime detection and disruption

Congress should fund and prioritize the development and deployment of AI-powered tools for detecting and disrupting crime and national security threats. This includes machine learning models that surface behavioral anomalies, detect deepfake-enabled fraud, trace synthetic identities, and flag laundering typologies across the cryptocurrency ecosystem. These tools must be auditable, secure, and deployable across case management systems at IRS-CI, FinCEN, OFAC, FBI, DEA, USSS, HSI, as well at the defense and national security agencies.

Recommendation 2: Build real-time public-private alerting frameworks

Congress should encourage the development of real-time alerting systems that enable law enforcement, financial intelligence units, and vetted investigative partners to flag suspicious wallet addresses and, through the use of AI agents, notify participating exchanges, stablecoin issuers, financial institutions and other participants. These alerts can trigger temporary administrative holds — pending judicial process — to prevent illicit assets from being quickly moved or laundered. Bad actors, with the help of AI, are moving more quickly than ever, and so must we.

A real-time, AI-enabled alerting framework built on public-private coordination would allow all actors to respond faster, trace smarter, and disrupt more effectively.

Recommendation 3: Modernize legal frameworks to address synthetic crime

Congress should close statutory gaps to address AI-generated threats, including:

- Explicitly criminalizing deepfake impersonation fraud
- Defining and prohibiting synthetic CSAM (child sexual abuse material)
- Modernizing evidentiary standards for AI-altered media

These actions are essential to ensure prosecutors and investigators have the legal tools to pursue AI-driven crimes with the same intensity as traditional fraud, abuse, and exploitation.

Recommendation 4: Equip law enforcement with AI-enabled investigative infrastructure

Agencies at every level must have access to modern investigative capabilities, including blockchain analytics platforms with integrated AI, media authentication tools, and other AI-enabled investigative tools. Congress should allocate dedicated funding for these tools, along with specialized training programs in AI-enabled crime, forensic preservation, disruption techniques, network analysis and prosecutorial readiness.

This investment is not only about technology — but about building capacity in agents, officers, and analysts who must now navigate an increasingly complex threat landscape.

Recommendation 5: Promote public-private collaboration to counter AI threats

No single agency or company can address AI-enabled crime in isolation. TRM Labs partners with law enforcement globally, and victim reports through Chainabuse help surface new scam techniques in real time. These initiatives should be supported, formalized, and scaled through structured public-private partnerships that include technology companies, financial institutions, and community watchdogs.

These are the early warning systems of the AI era. Congress should ensure they are resourced, coordinated, and connected to national enforcement priorities.

AI is a vital tool on the side of good

Artificial intelligence is not inherently good or evil; it is a tool. In the hands of criminals, we have seen how it can enable harm at unprecedented speed and scale. But in the hands of law enforcement, innovators, and vigilant citizens, that same technology can be a powerful force for protection. Today's adversaries are moving fast to leverage AI's potential for exploitation. We must move faster.

Every day at TRM Labs, we witness both the dangers and the solutions inherent in AI technology. We see deepfake scams robbing families of their savings, grooming operations that leave victims devastated, and ransomware crews targeting hospitals and schools with AI-enhanced malware. But we also see how cutting-edge analytics, cross-sector collaboration, and an informed public can turn the tide.

Congress has a critical role to play in shaping a future where AI strengthens — rather than undermines — our financial system, our institutions, and our trust in one another. By updating laws, investing in law enforcement and technology, fostering public-private teamwork, coordinating internationally, and educating the public, we can ensure that the tools of safety evolve as fast as the tools of harm.

TRM Labs is proud to support this mission, and we look forward to continuing our work with the Subcommittee toward these goals.

Thank you again for your time and attention. I welcome your questions.