# AI-Enabled Transnational Fraud: Risk Evolution, Governance Dilemmas, and Regulatory Pathways

**Jingjing Zheng**
*School of Finance and Accounting, Fuzhou University of International Studies and Trade, Fuzhou, Fujian, China*

**Abstract: Generative artificial intelligence has rapidly changed the technical conditions under which cross-border fraud is produced, distributed, and concealed. Unlike traditional fraud, which relies heavily on manual scripts, fake identities, phone calls, and fraudulent websites, generative AI enables criminals to create realistic text, cloned voices, synthetic images, deepfake videos, and personalized deception strategies at low cost and large scale. This article examines the emerging risks of generative AI-enabled cross-border fraud and analyzes why such fraud is difficult to govern under existing regulatory frameworks. The study argues that generative AI increases the credibility, precision, scalability, and concealment of cross-border fraud by combining identity impersonation, data misuse, automated content generation, platform-based dissemination, and complex financial transfer channels. It further proposes a governance framework based on risk classification, platform accountability, financial monitoring, enterprise internal control, personal data protection, public awareness, and international cooperation. The article concludes that the governance of generative AI-enabled cross-border fraud should not rely only on post-event punishment. Instead, it requires a preventive, coordinated, and technologically adaptive regulatory system that balances AI innovation with digital security.**

**Keywords: Generative AI; Cross-Border Fraud; Deepfake; Data Security; Financial Crime; Digital Governance**

## 1. Introduction

Generative artificial intelligence has become one of the most influential technologies in the current stage of digital transformation [1]. Large language models, voice cloning systems, image generation tools, synthetic video technologies, and automated content production platforms are increasingly used in business communication, education, financial services, media production, and international trade. These technologies improve efficiency, reduce communication costs, and create new opportunities for digital economic development. However, the same technologies can also be misused by criminal actors. When generative AI is applied to cross-border fraud, it changes not only the tools used by fraudsters but also the scale, speed, credibility, and complexity of fraudulent activities [2,3].

Traditional cross-border fraud usually depends on relatively simple methods. Fraudsters use fake websites, forged emails, phone calls, fraudulent investment platforms, false customer service accounts, or social engineering scripts to deceive victims. Although such methods remain common, they often leave visible signs of deception, such as poor language quality, unnatural communication, inconsistent identity information, or suspicious payment instructions. Generative AI weakens these traditional warning signals [4]. It can produce fluent multilingual texts, imitate professional writing styles, generate realistic voices, fabricate images and videos, and personalize fraudulent messages according to the victim's background. As a result, victims may find it increasingly difficult to distinguish real communication from synthetic deception [5,6].

The cross-border nature of this problem makes it even more serious. Fraudulent actors, servers, accounts, platforms, data sources, payment channels, and victims may be located in different jurisdictions. A scam message may be generated by an AI tool hosted in one country, distributed through a platform registered in another country, sent from an anonymous account controlled elsewhere, and linked to a payment channel that transfers funds through multiple financial institutions or virtual asset wallets. This fragmentation makes evidence collection, fund

 

tracing, responsibility identification, and law enforcement coordination extremely difficult. Generative AI therefore does not merely improve the technical capacity of fraudsters. It intensifies existing weaknesses in data governance, platform regulation, financial monitoring, and international legal cooperation [7,8].

The issue should not be understood as a reason to reject artificial intelligence. Generative AI itself is a general-purpose technology with enormous positive potential. It can improve productivity, support public services, enhance financial inclusion, assist language communication, and promote innovation across industries. The key question is how to govern its misuse without suppressing legitimate development. A balanced governance approach should recognize both sides of the technology. On one side, generative AI is a driver of digital economic growth. On the other side, it can be used to produce deception at a scale and quality that traditional governance tools were not designed to handle.

This article focuses on the risks and governance pathways of generative AI-enabled cross-border fraud. It argues that this new type of fraud is characterized by realistic identity impersonation, personalized targeting, automated content production, data-driven manipulation, complex fund transfer channels, and jurisdictional fragmentation. Effective governance requires a shift from fragmented and reactive enforcement to systematic prevention. Regulators, digital platforms, financial institutions, enterprises, individuals, and international organizations all need to play coordinated roles. The governance objective should be clear: to reduce the misuse of generative AI in fraud while preserving its legitimate value for economic and social development.

## 2. The Changing Nature of Cross-Border Fraud in the Age of Generative AI

Cross-border fraud has always adapted to new communication and financial technologies [9,10]. When email became widely used, phishing scams expanded rapidly. When social media platforms grew, romance scams, fake investment groups, and impersonation fraud became more common. When digital payment and virtual currency systems developed, fraudsters gained new channels for moving and laundering funds. Generative AI is another turning point because it does not simply provide a new communication channel. It enhances the content, identity, and psychological manipulation capacity of fraud itself [10].

The first major change is the professionalization of fraudulent communication. In the past, many scams could be identified through language errors, inconsistent writing style, or poorly designed materials. Generative AI can now produce convincing emails, contracts, customer service messages, investment proposals, legal notices, and business documents in different languages. This is particularly relevant for cross-border fraud because language barriers used to limit the ability of criminals to target foreign victims. With generative AI, criminals can produce natural and culturally adapted messages for different countries and groups. A scam targeting international students can use one style, while a scam targeting import-export companies can use another. This greatly increases the reach of fraud.

The second change is the rise of synthetic identity. Fraudsters can now create fake profile pictures, synthetic business representatives, AI-generated video calls, and cloned voices. In corporate fraud, criminals may imitate a senior executive and instruct financial staff to make urgent payments. In family-related scams, they may clone the voice of a relative and request emergency funds. In investment scams, they may create a fake financial adviser using synthetic images and automated conversations. These methods make identity verification far more difficult. Trust, which used to be based on voice, appearance, or writing style, becomes vulnerable when all these signals can be artificially generated.

The third change is personalization. Generative AI allows fraudsters to tailor messages according to the victim's personal information. Public social media data, leaked databases, shopping records, professional profiles, and business information can be used to create highly targeted deception. For example, a cross-border e-commerce seller may receive a fake customs notice that includes realistic product details. A university student abroad may receive a message pretending to be from an embassy or school office. A company accountant may receive an AI-generated instruction that imitates internal corporate language. Personalized fraud is more dangerous than generic fraud because it appears relevant, urgent,

 

and trustworthy.

The fourth change is automation and scale. Traditional scams require human labor to write messages, answer questions, build trust, and persuade victims. Generative AI can automate parts of this process. Chatbots can maintain long conversations with victims, generate answers in real time, and adjust tone according to the victim's emotional response. Fraudsters can operate many fake identities simultaneously and target large numbers of people across countries. This reduces the cost of fraud and increases its potential scale.

The fifth change is the combination of AI with financial and data infrastructure. Generative AI-enabled fraud often works together with illegal data markets, anonymous communication tools, digital payment channels, virtual assets, and offshore accounts. AI helps create trust and persuasion, while financial technologies help move funds quickly. This combination creates a full fraud chain from data acquisition to content generation, psychological manipulation, payment transfer, and money laundering.

## 3. Main Risks of Generative AI-Enabled Cross-Border Fraud

Generative AI-enabled cross-border fraud creates multiple layers of risk. These risks affect individuals, firms, platforms, financial institutions, regulators, and the broader digital economy. The following table summarizes the main risk types (as is shown in Table 1).

**Table 1. Main Risks of Generative AI-Enabled Cross-Border Fraud**

| Risk Type | Main Manifestation | Potential Harm |
|---|---|---|
| Identity impersonation | AI voice cloning, deepfake videos, synthetic avatars, forged documents | Makes fraud more credible and induces transfers, authorization, or disclosure |
| Precision targeting | Personalized scripts based on social media, leaked data, and professional profiles | Increases fraud success rates and weakens traditional awareness |
| Data misuse | Illegal collection and processing of personal and business information | Enables profiling, manipulation, and targeted attacks |
| Financial security risk | Use of offshore accounts, virtual assets, account splitting, and fast transfers | Makes fund tracing, freezing, and recovery more difficult |
| Platform governance risk | Fraudulent content spread through social media, email, messaging apps, and short-video platforms | Expands fraud reach and increases platform compliance pressure |
| Corporate fraud risk | Fake executive instructions, supplier account changes, forged contracts, and synthetic meetings | Causes corporate payment losses and internal control failures |
| Cross-border enforcement risk | Actors, servers, funds, victims, and evidence located in different jurisdictions | Complicates investigation, prosecution, and accountability |

Identity impersonation is perhaps the most visible risk. Voice cloning and deepfake technologies allow criminals to imitate people whom victims already trust. The psychological effect is powerful because people are often more likely to believe a request when it appears to come from a familiar voice or face. In cross-border settings, where communication often relies on remote channels, this risk is especially serious. Family members, business partners, school officials, embassy staff, or corporate executives may all be impersonated [11].

Precision targeting is another critical risk. Many victims do not fall for scams because they are careless, but because the scam is designed around their real situation. Generative AI makes this easier. It can transform scattered data into coherent, persuasive narratives. A fraudster who knows that a victim recently applied for a visa can generate a fake visa problem. A fraudster who knows that a company works with a foreign supplier can generate a fake payment update. A fraudster who knows that someone invests in digital assets can generate a personalized investment opportunity [12,13]. When fraud becomes context-specific, traditional public warnings become less effective.

Data misuse is the foundation of many AI-enabled scams. Generative AI becomes more dangerous when combined with personal and business data. Data leakage, illegal data trading, weak corporate data protection, and excessive collection of user information all create opportunities for fraud. The more detailed the data, the more convincing the deception. This means that anti-fraud governance must be connected to data governance. Without stronger control over personal information and business data, fraudsters will continue to have the raw material needed for targeted manipulation.

Financial security risks arise after the victim is

 

persuaded. Cross-border fraud often depends on rapid fund movement. Funds may pass through multiple accounts, payment platforms, virtual asset wallets, or offshore institutions. Criminals may split transfers into smaller amounts, convert them into virtual currencies, or move them across jurisdictions before victims realize what happened [14]. This creates pressure on banks, payment institutions, and regulators to detect suspicious patterns in real time.

Corporate fraud deserves special attention. Enterprises involved in foreign trade, cross-border e-commerce, international education, overseas investment, and global supply chains may face AI-generated fraud in daily operations. Fake supplier emails, forged invoices, synthetic video meetings, and impersonated executive instructions can lead to large financial losses. In many cases, the weakness is not only technological but procedural. If internal payment approval depends too much on email or verbal instructions, AI impersonation can exploit this gap.

## 4. Governance Challenges

Generative AI-enabled cross-border fraud is difficult to govern because it combines technological, institutional, and jurisdictional complexity. Traditional anti-fraud systems were not designed for a world in which voices, faces, documents, and conversations can be generated automatically and convincingly.

The first challenge is the low technical threshold. Many AI tools are easy to access and use. Criminals no longer need advanced programming skills to create realistic fraudulent content. A simple prompt can generate a professional email, a fake customer service response, a legal warning, or an investment message. Voice cloning and image generation tools are also becoming more accessible. This democratization of technical capability creates a governance problem because the number of potential fraud actors increases.

The second challenge is speed. AI-generated fraud can be produced and modified quickly. Once one script is blocked, another can be generated. Once one account is suspended, new accounts can appear. Traditional manual review systems struggle to keep up with this speed. Even keyword-based detection may fail because generative AI can rewrite the same fraudulent meaning in many different ways.

The third challenge is the uncertainty of responsibility. A fraud case may involve an AI model provider, a social media platform, a messaging service, a telecom operator, a bank, a payment provider, a virtual asset exchange, and several offshore entities. Each actor may claim that it only provides neutral infrastructure. This makes accountability fragmented. Without clear responsibility rules, fraud prevention becomes weak at every point in the chain [14].

The fourth challenge is evidence collection. AI-generated content may be deleted quickly, accounts may be anonymous, and servers may be overseas. Deepfake and voice cloning evidence also require technical verification. Law enforcement agencies may need platform logs, payment records, IP addresses, device information, model usage data, and cross-border cooperation. The process is often slow, while fraudulent funds move quickly.

The fifth challenge is regulatory imbalance. Different jurisdictions have different rules for AI governance, data protection, digital platforms, financial monitoring, and virtual assets. Fraudsters exploit these differences by locating different parts of their operations in places with weaker enforcement. This creates a regulatory arbitrage problem. If one country strengthens governance but others do not cooperate, cross-border fraud networks can simply shift their operations.

## 5. Governance Pathways

The governance of generative AI-enabled cross-border fraud requires a multi-layered framework. No single measure can solve the problem. Effective governance must connect AI regulation, data protection, platform responsibility, financial monitoring, enterprise compliance, public education, and international cooperation.

### 5.1 Risk-Based AI Regulation

Regulators should classify AI applications according to risk. Not all uses of generative AI require the same level of oversight. Low-risk uses, such as general writing assistance or entertainment content, should not be regulated in the same way as high-risk uses involving identity verification, financial transactions, legal documents, voice cloning, or video synthesis. High-risk AI applications should be subject to stronger traceability, security testing, user verification, and audit requirements.

 

Deepfake content should be labeled where appropriate, especially when it involves public communication, commercial transactions, political messaging, or financial instructions. AI service providers should also maintain records that help identify misuse while respecting legitimate privacy and data protection requirements. The goal is not to prevent all synthetic content, but to reduce anonymous and harmful use in high-risk settings.

### 5.2 Platform Accountability

Digital platforms are major channels for AI-enabled fraud. Social media platforms, messaging applications, short-video platforms, email services, online marketplaces, and advertising systems can all be used to distribute fraudulent content. Platforms should therefore strengthen detection of synthetic fraud content, abnormal account behavior, fake customer service accounts, suspicious links, and mass messaging patterns.

Platform governance should not rely only on user reporting. Real-time risk detection is necessary. Platforms can use behavioral signals, account history, link reputation, content similarity, user complaints, and financial risk warnings to identify fraud campaigns earlier. They should also establish fast response channels with financial institutions and law enforcement agencies. When a fraud pattern is identified, platforms should be able to suspend accounts, preserve evidence, notify affected users, and share relevant information with authorized authorities.

### 5.3 Financial Monitoring and Fund Interception

Fraud ultimately seeks financial gain. Therefore, financial monitoring is a key part of governance. Banks, payment institutions, and virtual asset service providers should strengthen real-time monitoring of abnormal transfers, account splitting, rapid fund movement, virtual currency conversion, and high-risk cross-border transactions.

Financial institutions should also improve warning mechanisms for users. When a transaction shows signs of fraud, such as unusual destination accounts, sudden large transfers, or urgent payment instructions following suspicious communication, users should receive clear warnings. Enterprises should have stronger verification procedures for supplier account changes, overseas remittances, executive payment instructions, and emergency transfers.

### 5.4 Enterprise Internal Control

Enterprises are increasingly exposed to AI-enabled cross-border fraud. Companies engaged in international trade, supply chain management, cross-border e-commerce, overseas education services, and foreign investment are particularly vulnerable. Internal control systems must adapt to AI impersonation risks.

Enterprises should avoid relying on a single communication channel for financial decisions. Payment instructions from executives, suppliers, or overseas partners should be verified through independent channels. Video calls should not be treated as automatically reliable because deepfake technology can create synthetic appearances. Supplier account changes should require formal documentation and multi-person approval. Employees in finance, procurement, legal, and customer service departments should receive training on AI-generated fraud.

### 5.5 Personal Data Protection

Personal data protection is central to preventing precision fraud. Many AI-enabled scams succeed because fraudsters already know the victim's name, job, family situation, transaction history, school, company, or travel plan. Reducing data leakage reduces the effectiveness of personalized deception.

Governments should strengthen enforcement against illegal data collection and data trading. Enterprises should limit unnecessary data collection and improve data security. Platforms should reduce excessive exposure of personal information. Individuals should also be cautious about sharing sensitive information online. Public education should explain that AI fraud often uses real personal details to create trust.

### 5.6 International Cooperation

Cross-border fraud cannot be governed effectively by one country alone. International cooperation is needed in evidence sharing, suspicious account freezing, virtual asset tracking, data requests, extradition, and joint action against fraud networks. Countries should also work toward common technical standards for AI-generated content labeling, deepfake detection, and digital evidence preservation.

Cooperation should be practical rather than

 

symbolic. Law enforcement agencies need faster channels to request digital evidence. Financial regulators need mechanisms to freeze suspicious funds before they disappear. Platforms operating globally need consistent procedures for responding to cross-border fraud. International organizations can help coordinate standards and information sharing (as is shown in Table 2).

**Table 2. Governance Framework for Generative AI-Enabled Cross-Border Fraud**

| Governance Actor | Governance Focus | Main Measures |
|---|---|---|
| Government regulators | AI risk classification and legal standards | Regulate high-risk AI uses, require traceability, strengthen deepfake governance |
| Digital platforms | Content and account governance | Detect synthetic fraud content, suspicious links, fake accounts, and mass messaging |
| Financial institutions | Fund monitoring and interception | Monitor abnormal transfers, virtual asset conversion, and cross-border fund flows |
| Enterprises | Internal control and verification | Strengthen payment approval, supplier verification, identity checks, and staff training |
| Individuals | Data protection and awareness | Recognize voice cloning, deepfakes, personalized scripts, and urgent payment scams |
| International partners | Cross-border enforcement | Share evidence, freeze funds, track virtual assets, and coordinate legal standards |

## 6. Policy Implications

The governance of generative AI-enabled cross-border fraud should follow the principle of balancing innovation and security. Overly strict restrictions may harm legitimate AI innovation, while weak regulation may allow fraud to expand. A risk-based approach is therefore more appropriate. High-risk applications should face stronger obligations, while low-risk and beneficial applications should continue to develop.

Governance should also move earlier in the fraud chain. Many current systems focus on post-event investigation and fund recovery, but AI-enabled fraud moves too quickly for this approach to be sufficient. Prevention, detection, and early intervention are more important. This means improving data protection before fraud scripts are generated, strengthening platform detection before fraudulent content spreads, and monitoring payments before funds disappear.

Another implication is that enterprises must become active governance participants. Cross-border fraud is not only a matter for police or regulators. Companies may be victims, channels, or data sources. Weak internal controls can create opportunities for fraud. Stronger corporate governance, employee training, payment verification, and cybersecurity management are necessary.

Public education also needs to evolve. Traditional warnings such as “do not trust strangers” are no longer enough. AI-enabled fraud may come from a familiar voice, a realistic video, or a message containing accurate personal details. The public must understand that seeing or hearing is no longer always believing. Verification through independent channels should become a normal habit.

## 7. Conclusion

Generative AI-enabled cross-border fraud represents a new stage in the evolution of digital crime. It increases the realism of deception, improves the precision of targeting, expands the scale of fraudulent communication, and complicates cross-border enforcement. Its danger lies not only in the technology itself but in the combination of AI-generated content, personal data misuse, platform dissemination, financial transfer channels, and jurisdictional fragmentation.

The solution is not to reject generative AI. The technology has significant value for economic development, business communication, public services, and innovation. The real challenge is to build governance capacity that matches technological progress. This requires risk-based regulation, platform accountability, financial monitoring, enterprise internal control, personal data protection, public awareness, and international cooperation.

In the future, the competition between fraud and governance will increasingly become a competition of speed, coordination, and technological adaptability. Fraudsters will continue to use new tools, but regulators and institutions can also use technology to detect, trace, and prevent misuse. A secure digital economy depends not only on innovation capacity, but also on the ability to govern

 

innovation responsibly. Only by combining technological development with strong governance can society reduce the misuse of generative AI and preserve trust in cross-border digital communication and financial systems.

**References**

[1] Alt, T., Ibisch, A., Meiser, C., Wilhelm, A., Zimmer, R., Ditz, J., Dresen, D., Droste, C., Karschau, J., & Laus, F. (2024). Generative ai models: Opportunities and risks for industry and authorities. arXiv preprint arXiv:2406.04734.

[2] Bail, C. A. (2024). Can generative AI improve social science? Proceedings of the National Academy of Sciences, 121(21), e2314021121.

[3] Banh, L., & Strobel, G. (2023). Generative artificial intelligence. Electronic markets, 33(1), 63.

[4] Button, M. (2012). Cross-border fraud and the case for an “Interfraud”. Policing: An International Journal of Police Strategies & Management, 35(2), 285–303.

[5] Ferrari, F., Van Dijck, J., & Van den Bosch, A. (2025). Observe, inspect, modify: Three conditions for generative AI governance. New Media & Society, 27(5), 2788–2806.

[6] Fui-Hoon Nah, F., Zheng, R., Cai, J., Siau, K., & Chen, L. (2023). Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration. In (Vol. 25, pp. 277–304): Taylor & Francis.

[7] Guo, Y., Bao, Y., Stuart, B. J., & Le-Nguyen, K. (2018). To sell or not to sell: Exploring sellers' trust and risk of chargeback fraud in cross-border electronic commerce. Information systems journal, 28(2), 359–383.

[8] Heinemann, M., & Stiller, W. (2025). Digitalization and cross-border tax fraud: evidence from e-invoicing in Italy. International Tax and Public Finance, 32(1), 195–237.

[9] Holmström, J., & Carroll, N. (2024). How organizations can innovate with generative AI. Business Horizons.

[10] Ibitoye, J. S. (2025). Multi-agent AI systems for secure, transparent, and compliant fraud surveillance in cross-border FinTech operations. Int J Res Publ Rev, 6(6), 9724–9740.

[11] Janssen, M. (2025). Responsible governance of generative AI: conceptualizing GenAI as complex adaptive systems. Policy and Society, 44(1), 38–51.

[12] Joshi, R., Pandey, K., & Kumari, S. (2025). Generative AI: A transformative tool for mitigating risks for financial frauds. Generative artificial intelligence in finance: Large language models, interfaces, and industry use cases to transform accounting and finance processes, 125–147.

[13] Kaswan, K. S., Dhatterwal, J. S., Malik, K., & Baliyan, A. (2023). Generative AI: A review on models and applications. 2023 international conference on communication, security and artificial intelligence (ICCSAI).

[14] Ricker, J., Assenmacher, D., Holz, T., Fischer, A., & Quiring, E. (2024). AI-generated faces in the real world: A large-scale case study of Twitter profile images. Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses.

 