Combating Digital Crime in the Age of Generative AI

Nami Ueda

10 July 2026

Iakyara vol.417

Nomura Research Institute, Ltd.

Nami Ueda
Senior Associate
Security Solutions Planning & Consulting Department

Executive Summary

Digital crime is evolving rapidly in the age of generative AI. Sophisticated forgeries are increasingly being used to bypass eKYC authentication processes, while phishing sites can now be created and deployed at unprecedented speed and scale. As a result, organizations must strengthen defenses against the exploitation of vulnerabilities and loopholes in system specifications. Online services now require multilayer defenses encompassing security precautions designed into the services from the outset, dynamic anomaly detection and cyber business continuity planning to ensure resilience against emerging threats.

GenAI's emergence and loopholes lurking in official specifications

The digital crime prevention environment is at a critical turning point in the wake of generative AI's ascendance. In this context, "digital crime" does not refer to attacks intended to impair, disable, or otherwise tamper with software systems. Rather, it refers to acts such as unauthorized fund transfers, theft of loyalty points, and account takeovers that exploit legitimate service functions, operational processes, or loopholes embedded within service specifications.

Historically, cybercrime primarily involved hacking activities aimed at identifying and exploiting software vulnerabilities. Today, however, attacks targeting weaknesses in legitimate business processes and service designs are becoming increasingly prevalent alongside traditional cyber threats. (The "GenAI" referred to herein means maliciously used AI models released prior to the advent of frontier models such as Claude Mythos.)

Misuse of GenAI for digital crime is progressing faster than anticipated by the cybersecurity community against a backdrop of two trends. The first trend is technological advancement as exemplified by deepfakes. The second is that attack processes are becoming increasingly efficient by virtue of AI's code- and text-generation capabilities. Below we highlight specific schemes that notably capitalized on these two trends and service specification loophole mechanisms.

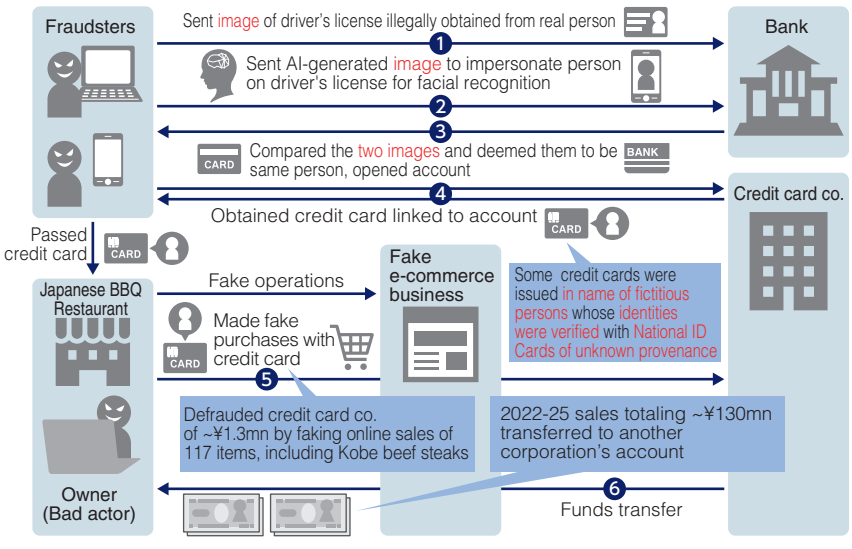
One notable example involved the use of advanced impersonation technology to exploit vulnerabilities in an online eKYC identity verification process that relied on ID photographs and biometric facial recognition. The fraudulent activity occurred from April 2022 to September 2025, during which time eKYC facial recognition logic was designed to process only static images.

Attackers opened bank accounts by combining AI-generated facial images with stolen or fabricated identity documents. They apparently then obtained lines of credit using these newly opened accounts or credit information under a fictitious name. They regularly generated cash proceeds from the credit lines by fabricating fake e-commerce transactions as detailed in the accompanying diagram.

Another scheme involved misappropriating and monetizing information across multiple platforms. The schemers circumvented eKYC authentication to open fake accounts by using GenAI to generate dynamic facial images (selfies) based on driver's license photos fraudulently harvested by phishing sites. Phishing schemes targeting images of victims' IDs have been ongoing since at least January 2024. Misappropriation of information across platforms has also become common. Such schemes have become markedly more sophisticated.

Phishing sites are becoming increasingly effective at harvesting personally identifiable information, driven by GenAI's advanced code generation capabilities. Phishing site features that previously aroused suspicion (e.g., non-native Japanese text, unnatural designs) have been eliminated through optimization of textual

Fraud scheme that exploited GenA



Source: NRI

content and UIs, making it difficult for even security-conscious users to detect the ruse.

New safeguards required in GenAI era

To combat digital crime in the GenAI era, the cybersecurity community must transition to multi-layer defenses that integrate upgraded organizational defenses with granular safeguards deployed at the IT system level, placing priority on automated, AI-powered responses instead of relying on human judgment.

The first priority is addressing the increasing efficiency of digital crime schemes. Successful attack methods are rapidly replicated and deployed across the entire financial services industry. Late responders are prone to incur huge costs and reputational damage. Financial institutions accordingly must perform exhaustive risk analyses that assume mass deployment of automated, AI-powered fraud schemes and assess their service specifications' susceptibility to malicious exploitation. Such due diligence should be incorporated into the specification design stage. Additionally, financial institutions must continuously monitor the latest digital crime trends on an industry-wide basis and share information with other financial institutions to upgrade their own defenses to industry standards.

The second priority is countering the growing technological sophistication of digital crime. Detection logic must be continuously augmented, primarily with technologies based on GenAI and machine learning. Specific safeguards that should be adopted include risk-based authentication and behavioral biometrics. These two technologies utilize GenAI to comprehensively assess risk based on continuity of user behavior, transaction details and access-device usage patterns such as how the user holds her smartphone and how fast she types. If anything suspicious is detected, the system would automatically require additional authentication or lock the account in real time. Additionally, a common online method for biometric identity verification currently in use[1] is slated to be essentially abolished by a pending amendment to the Act on Prevention of Transfer of Criminal Proceeds. In its place, technologies such as Japanese Public Key Infrastructure or IC chip readers will be required to be used.

The third priority is establishing a cyber business continuity plan that assumes cybersecurity incidents will occur and defines how services should respond during a disruption. The plan must include explicit criteria for deciding which functions

NOTE

1) Stipulated in the enforcement regulations of the Act on Prevention of Transfer of Criminal Proceeds, this method for identity verification requires that users to photograph their ID (e.g., driver's license, National ID Card) with a smartphone and then send the photograph together with a selfie video that features motion (e.g., blinking, nodding). The selfie is biometrically compared to the ID photo to verify the user's identity.

should be shut down and when. Another necessity is establishing a framework capable of swiftly restricting functionality and deploying patches without hesitation.

In May 2026, the Japanese Financial Services Agency issued a request regarding the risks posed by frontier AI models. Advancements in AI technology could lead to an increasingly vicious cycle of cat and mouse that would tend to favor the criminals. The aforementioned malicious exploitation of legitimate specifications may be exacerbated by frontier AI. Service design that prioritizes user-friendliness above all else could give rise to loopholes that leave the service vulnerable to an onslaught of AI-generated fake requests. The cybersecurity community must therefore respond by embracing advanced AI technologies of its own. Financial institutions must build a sophisticated AI defense that swiftly and autonomously upgrade diagnostic and detection logic as threats evolve.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $5.1 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including Tokyo, New York, London, Beijing and Sydney, with over 16,800 employees.

For more information, visit https://www.nri.com/en

Inquiries to : Business Planning Department, Financial Technology Solution Division
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

https://www.nri.com/en/knowledge/publication/list.html#lakyara