Fraud Rings: A Dangerous Trend Businesses Should Be Aware Of

Learn about fraud rings, the warning signs, and how businesses can protect themselves.

Despite the advancements in identity verification each year, online fraudsters persist in their innovation, resulting in a significant rise in fraud cases. Payment card fraud losses are expected to hit $49 billion by 2030. A primary catalyst for these concerning statistics is the proliferation of fraud rings, or fraud networks.

According to Sumsub's internal research, approximately one in every 100 users is associated with a fraud network. Fraud networks, or rings, are organized groups comprising multiple accounts engaged in criminal activities—with membership ranging from 3 to 750 individuals.

Fraud rings have emerged as a global fraud trend, akin to AI-powered deepfakes. Due to their organized nature, the impact of fraud rings surpasses that of individual scammers.

Let's dive into the most dangerous types of online fraud rings, preventive measures, and strategies to mitigate losses while maintaining compliance with anti-money laundering (AML) regulations.

What is a fraud ring?

A fraud ring, also known as a fraud network, are organized groups comprising multiple accounts engaged in criminal activities. These networks vary in size and structure; some may have thousands of members, others comprise only one fraudster controlling multiple accounts.

Multiple accounts are often used for fraud rings. The accounts themselves may be purchased from the dark web or created using fake identities. Ultimately, they're utilized to perpetrate a wide range of digital fraud, including money laundering, bonus abuse, fake reviews, and more.

Banking, trading, cryptocurrency, gambling (including betting and iGaming), e-commerce, and the social media industries suffer the most from fraud rings. This is partly due to their significant traffic and high volumes of applicants.

The fraud ring-related risks faced by these industries include:

- Multi-accounting, including mule networks and identity theft
- Deepfake scam networks

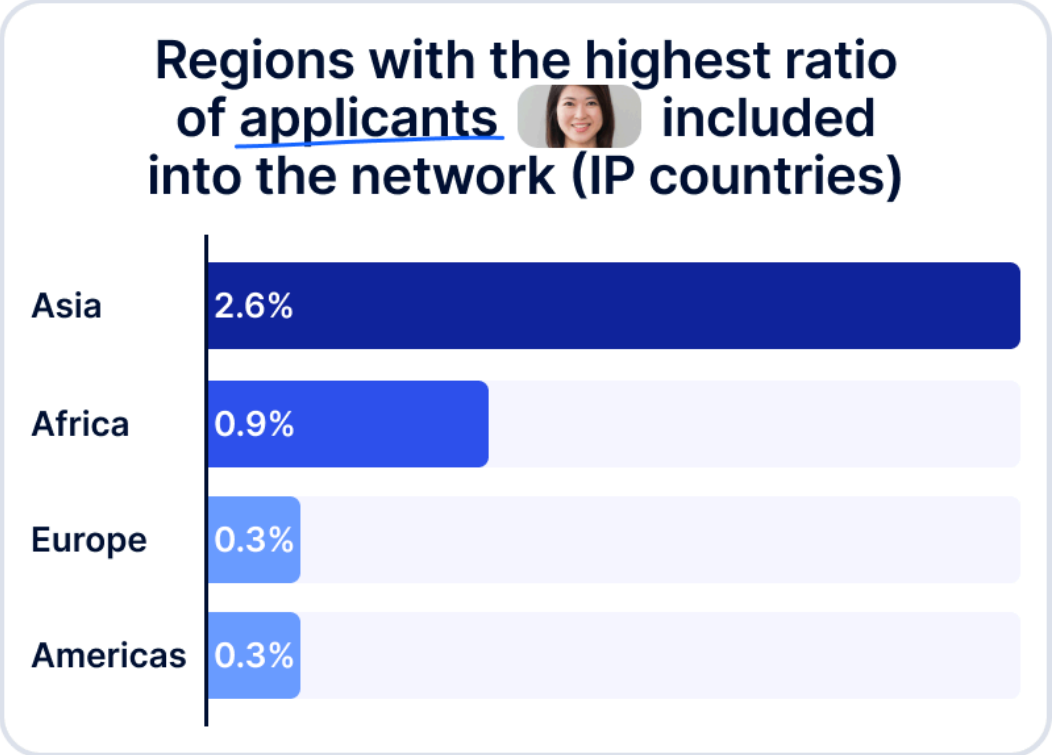
- Bot farms
- Incentivized traffic fraud networks.

High-risk regions

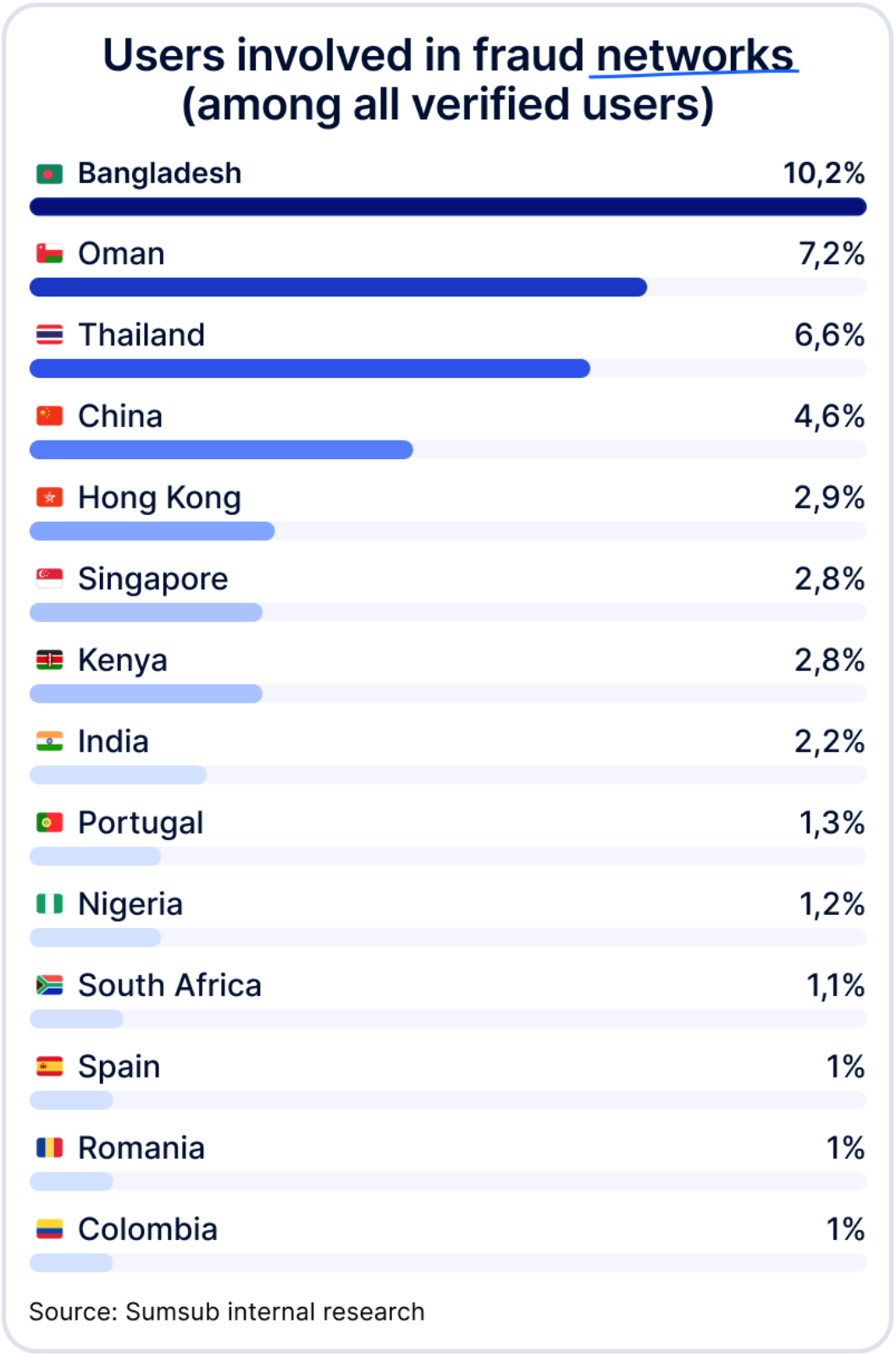
Fraud isn't bound by borders and can happen worldwide. However, specific regions may have characteristics that make them more vulnerable to certain types of fraud. Fraud networks therefore tend to thrive in areas characterized by:

- Economic and political instability
- Corruption
- Lack of regulatory oversight
- Poor cybersecurity infrastructure
- High internet accessibility and digitalization, as seen in the Asia-Pacific (APAC) region.

According to Sumsub's internal data, IDs registered in APAC are frequently utilized for fraudulent activities in countries such as the US, UK, Russia, Germany, and France.



Sumsub's internal research also shows the following statistics:



Countries on the Financial Action Task Force (FATF) blacklist or under the United Nations (UN) sanctions may also face risks associated with fraud rings.

Types of fraud rings

Identity theft rings

An identity theft fraud ring is an organized group of criminals who specialize in stealing personal information from individuals in order to commit various fraudulent activities. These activities can include opening fraudulent bank accounts, applying for credit cards in someone else's name, filing fraudulent tax returns, and other forms of financial fraud.

Members of an identity theft ring typically work together to obtain and exploit personal information, such as social security numbers, birth dates, and financial account details. They may use a variety of tactics, such as phishing scams, hacking into databases, or even stealing physical documents, to gather this information.

Once they have acquired the necessary personal information, they may use it themselves or sell it on the darkweb to other criminals. Identity theft fraud rings can cause significant financial and emotional harm to their victims, as well as damage to businesses and financial institutions.

Money mule networks

Money muling involves seemingly innocent individuals, known as money mules, who are recruited to transfer illegally obtained funds and disguise their origin. According to Sumsub's 2023 Identity Fraud Report, money muling networks are one of the top-5 global fraud trends. Just recently, Europol, Interpol and Eurojust identified 10,759 money mules and 474 recruiters, leading to the arrest of 1,013 individuals worldwide.

Money muling networks utilize the following techniques to launder acquired money through schemes including, but not limited to, investment scams, fake holiday rentals, middleman scams, phishing, messenger app fraud, help desk fraud, crypto fraud, counterfeit bank cards, and more:

- "Bank drops"

Money launderers need to deposit illicit funds without the bank's knowledge. To do this, they'll pay someone with a clean banking history—somewhere in the range of $50 to $100—to open up a bank on their behalf. Typically, online "neobanks" are preferred over traditional banks for this purpose.

- Online payment methods, including gift cards.

These are often furnished to money mules of a younger age demographic, who purchase items and deliver them to the criminals. These items are subsequently sold on popular e-commerce platforms, and a share of the illegal proceeds is provided in cash or goods to the mule.

- Social engineering attacks

Not all money mules are aware of their involvement. Criminals can use deceptive tactics, including bank impersonation, to compromise people's banking credentials—often those of more vulnerable populations, particularly seniors—which can then be used to open new accounts for money laundering.

- Fabricated identities

Not all money mules have to be real people. In fact, the perpetrators often fabricate identities—often through the use of AI—which can then be used to open up fraudulent bank accounts. These fake identities can be advanced enough to bypass KYC, underscoring the need for advanced security measures and monitoring beyond the onboarding stage.

Money mules are hard to identify because their activity often appears as legitimate transactions. Therefore, the right anti-fraud solution must have advanced transaction monitoring, anomaly detection algorithms, and behavior analysis to identify patterns indicative of money mule activities.

Deepfake fraud rings

A deepfake network refers to an individual or group that creates a collection of manipulated multimedia content using advanced artificial intelligence (AI) techniques. These deepfakes can then be used to create convincing yet entirely fabricated videos or audio recordings, as well as fake documents, for various fraudulent purposes, including:

– creating a non-existing applicant to pass verification

– manipulating public opinion and spreading misinformation

Since AI tools are getting cheaper and easier to use, they become an even greater threat. So, the solution is to fight fire with fire. **AI is the solution to this problem, as it can be used to detect certain visual or audio artifacts that are absent in authentic media, which can help successfully detect deepfake networks.**

Bot networks

Bot networks are automated software programs which mimic human behavior on the internet. These bots are strategically programmed to engage in various activities, including clicking on ads, visiting websites, and even simulating fake purchases.

Usually, the core objective of these networks is to mislead affiliate marketing platforms and advertisers by creating an illusion of genuine human interaction, thereby driving traffic and purportedly generating sales.

As a consequence, merchants find themselves paying commissions for engagement that doesn't translate into actual revenue.

Incentivized traffic fraud

Incentivized traffic fraud involves artificial interactions with digital content or services (such as e-commerce sites or social media) to manipulate user engagement figures. Fraudsters utilize various schemes to incentivize online users, such as offering rewards, bonuses, incentives to click on ads, visit websites, or engage with content.

These fraudulent activities aim to boost metrics and create a false impression of genuine user interest, often to deceive advertisers or manipulate rankings. Incentivized traffic fraud undermines the integrity of digital advertising and analytics, leading to inaccurate data and financial losses for businesses. The industries which suffer most from incentivized traffic fraud are digital advertising, social media, e-commerce, and online publishing.

Combatting this type of fraud requires robust monitoring, analytics tools, and preventive measures to identify and mitigate deceptive practices.

Fraud ring detection: The warning signs

If some of the following attributes are duplicated across multiple accounts, it could indicate a fraud ring:

- Devices
- Personal information
- Same selfie background during verification
- Action time
- IP addresses
- Documents
- Geolocation and home address
- Proofs of address (or registered location)
- Behavioral patterns (e.g. completion speed, gestures, the way users hold the device)

How to protect against fraud rings

You can uncover interconnected patterns of suspicious activity on your platform using Sumsub's AI-powered Fraud Network Detection solution. This tool provides you with the ability to **identify fraud rings before the onboarding stage** through AI, allowing you to apprehend **an entire**

fraudulent network rather than just a single fraudster, and protect your platform from online crime and money laundering.

With Sumsub's Fraud Network Detection, you'll be able to:

1. **Predict malicious behavior** through Graph neural network (GNN) analysis, which detects behaviors, patterns, and historical data using machine-learning algorithms.
2. **Analyze your entire client network** for suspicious patterns throughout the entire user journey with one solution
3. **Examine historical connections** among entities using ML/AI-powered algorithms
4. **Prevent multi-accounting** through IP address analysis, behavioral biometrics, and device fingerprinting
5. **Detect bot farms** by analyzing device fingerprints, completion speeds, and other non-human nuances.
6. **Monitor traffic** to distinguish genuine user engagement from artificially motivated traffic.

Sumsub's Fraud Network Detection elevates anti-fraud countermeasures by revealing hidden connections, detecting anomalies, and continuously analyzing user behavior at every stage of the user journey, including onboarding, AML-screening, and transactions.

sumsub

Start exploring Sumsub today.

Get started