ISSUE NO.26 03.11.2026

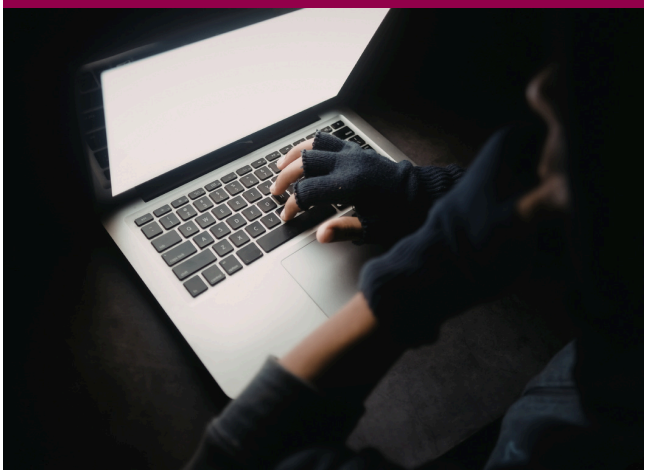
FINANCIAL CRIMES WATCH



INTERNATIONAL CRYPTOCURRENCY FRAUD: MADAGASCAR-BASED "*PIG BUTCHERING*" SCHEME TARGETING THE UNITED STATES

On October 27, 2026, the U.S. Department of Justice ("**DOJ**") publicly announced an investigation into six individuals suspected of conducting cryptocurrency investment fraud operations from Madagascar with links to China and Southeast Asia. The DOJ's Scam Center Strike Force (the "**Strike Force**") and the Federal Bureau of Investigation ("**FBI**"), in cooperation with foreign authorities, conducted an investigation into fraudulent non-fungible token (the "**NFT**") investment platforms targeting individuals in the United States. As part of the investigation, 74 cryptocurrency wallets believed to be associated with approximately 800 victims across the United States were identified.

The seized instructional guides reveal that workers at the scam centers were directed to gain victims' trust before encouraging them to invest.



I. Pig Butchering: From Emotional Manipulation to Cryptocurrency Theft

The activities under investigation involved a form of cryptocurrency investment fraud commonly known as "***pig butchering***" which relies on establishing relationships of trust with victims. Under this scheme, perpetrators typically contact potential victims through online dating applications, social media, or messaging platforms and gradually gain their trust by developing personal or romantic relationships. Victims are then directed to fraudulent cryptocurrency investment platforms through promises of high returns and encouraged to make further investments by being shown fictitious profits on these platforms. Once the perpetrators have obtained sufficient assets from the victims, they cease all communication.

In the case at hand, the suspects were found to have posed as attractive women on online dating platforms and continued communicating with victims through WhatsApp. Devices seized during the investigation contained fake identities, audio and video recordings used to support those identities, and written instructions directing employees to exploit victims' emotions. These findings indicate that the fraudulent activities were not isolated attempts but were carried out through a systematic and organized operation involving the identification of potential victims, the establishment of trust, the persuasion of victims to invest, and the encouragement of further investments.



The scammers created fake identities to gain victims' trust and had real individuals produce audio and video recordings to make these identities appear more credible.

In the case at hand, unlike traditional fraud schemes, victims were directed to connect their cryptocurrency wallets to fraudulent NFT investment platforms rather than transfer their cryptocurrencies directly to accounts controlled by the perpetrators. According to an affidavit prepared by the FBI, victims were asked to grant unlimited transfer authorization, allowing third parties to transfer USDT from their wallets without requiring separate approval for each transaction. In addition, small payments were made to certain victims to increase their trust in the fraudulent investment platforms.

II. Cross-Border Fraud and International Investigation

The investigation revealed that the alleged criminal organization had connections to organized crime networks in China and scam centers in Southeast Asia, operated from Madagascar, and targeted individuals in the United States. Witnesses stated that increased law enforcement activity in China and Cambodia had prompted the relocation of scam centers to Madagascar.

In August 2026, an FBI team conducted an on-site investigation in Madagascar at the invitation of the Malagasy Ministry of Justice. These efforts facilitated the examination of approximately 3,200 electronic devices seized from 13 scam centers, enabling investigators to identify additional suspects and significant evidence more effectively. However, according to the DOJ's announcement, numerous suspects were repatriated to China while the investigation was still ongoing, preventing investigators from obtaining their statements. U.S. authorities subsequently requested international cooperation to advance the investigation and secure the extradition of the suspects.

These developments highlight the challenges of effectively investigating cross-border fraud through the efforts of a single country's authorities. Identifying suspects, preserving electronic evidence, tracing cryptocurrency transactions, and obtaining witness statements require timely and effective cooperation among judicial and law enforcement authorities across multiple jurisdictions.

III. Criminal Allegations and Legal Assessment

During the investigation, some suspects claimed in their statements that they were victims of human trafficking and had been forced to work under poor conditions at scam centers. Furthermore, it was established that cryptocurrencies obtained through fraudulent activities had been transferred to various countries and converted into fiat currency abroad. Accordingly, the activities under investigation also warrant legal assessment in relation to human trafficking and money laundering offenses, in addition to fraud.

The data released by the DOJ illustrate the scale and cross-border nature of such fraudulent activities. According to data from the FBI's Internet Crime Complaint Center, reported financial losses resulting from cryptocurrency investment fraud increased by 89% between 2023 and 2025. The Strike Force also announced that, as part of its operations, measures had been imposed on more than USD 1 billion worth of cryptocurrency linked to fraudulent activities and that approximately 700 fraudulent investment websites had been seized. These figures, which are not limited to the Madagascar investigation, highlight the importance of international cooperation in investigating cross-border fraud. In this context, effective coordination of international investigations and mutual legal assistance mechanisms is essential for identifying perpetrators, tracing cryptocurrencies obtained through criminal activities, and recovering assets.

