

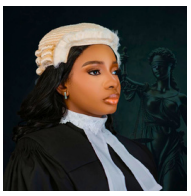
CRYPTOCURRENCY FRAUD IN NIGERIA: LEGAL REMEDIES FOR VICTIMS UNDER THE ISA 2025

August 2026

SYNTEGRAL LEGAL PRACTICE



Oladiran Falore
Senior Partner



Ifunanya M. Igwebuike
Associate Counsel

For many years, Nigeria's cryptocurrency market operated within a fragmented and uncertain legal and regulatory landscape. Although digital assets enjoyed widespread adoption, there was little legislative certainty regarding their legal status, regulatory oversight or the rights and protections available to investors. That position has changed significantly with the enactment of the Investments and Securities Act 2025 ("ISA 2025").

For the first time, the ISA 2025 expressly recognises digital and virtual assets within Nigeria's securities regulatory framework and places qualifying activities involving those assets under the supervision of the Securities and Exchange Commission ("SEC"). This represents a significant milestone in the development of Nigeria's digital asset ecosystem. It provides a clearer legal foundation for cryptocurrency-related businesses, enhances regulatory oversight and offers greater protection to investors participating in the market.

However, increased legitimacy has been accompanied by increased risk. As investment in cryptocurrencies and other digital assets continues to grow, so too has the sophistication of fraudulent schemes targeting unsuspecting investors. Cybercriminals increasingly exploit the anonymity, speed and cross-border nature of blockchain transactions to perpetrate investment scams, Ponzi schemes, phishing attacks, fake trading platforms and wallet theft. Nigeria has also experienced a significant rise in cyber-enabled financial crime, making investor protection an increasingly important aspect of the country's evolving digital asset framework.

Against this backdrop, understanding both the opportunities and the risks associated with digital assets has become essential for investors, businesses and legal practitioners alike. This article examines the legal meaning of cryptocurrency fraud, scams and Ponzi schemes, identifies the most common forms of crypto-related fraud, analyses the regulatory framework introduced under the ISA 2025, considers the remedies now available to victims, and provides practical guidance on the steps victims should take where fraud occurs, together with recommendations for promoting a safer and more resilient cryptocurrency ecosystem in Nigeria.

The Concept of Cryptocurrency Fraud, Scams and Ponzi Schemes:
Although the terms cryptocurrency fraud, crypto scam and crypto Ponzi scheme are often used interchangeably, they describe different forms of unlawful conduct within the digital asset ecosystem. Understanding the distinction is important, as the legal consequences and available remedies may differ depending on the nature of the misconduct.

Cryptocurrency fraud refers to any intentional deception involving digital or virtual assets designed to induce another person to part with money, cryptocurrency or other property. It encompasses a wide range of fraudulent conduct, including fake cryptocurrency exchanges, phishing attacks, wallet theft, impersonation scams, rug pulls (where project developers abandon a project after raising investors' funds), market manipulation and other deceptive practices intended to unlawfully obtain or misappropriate digital assets.

Cryptocurrency scams constitute a broader category of deceptive investment schemes in which fraudsters make false representations or unrealistic promises of returns to persuade individuals to invest in non-existent or illegitimate cryptocurrency projects. Common examples include fake Initial Coin Offerings (ICOs), fraudulent investment platforms, pump-and-dump schemes, romance and investment scams, and social media promotions falsely endorsed by celebrities or reputable institutions.

Crypto Ponzi schemes are a specific form of investment fraud in which purported returns paid to existing investors are financed not from genuine investment profits but from contributions made by new participants. Such schemes are inherently unsustainable and inevitably collapse once the inflow of new investors declines. Within the cryptocurrency market, Ponzi schemes frequently disguise themselves as high-yield investment programmes, cloud mining ventures, staking platforms, liquidity pools or yield farming opportunities promising guaranteed or exceptionally high returns with little or no investment risk.

Although these schemes differ in their structure and operation, they share a common characteristic, they rely on deception, misrepresentation and the exploitation of investors' limited understanding of digital assets. As cryptocurrency adoption continues to grow, so too has the sophistication of these fraudulent schemes, making regulatory oversight and investor due diligence more critical than ever.

Types of Crypto Fraud, scams and Ponzi Scheme
There are a lot of ways crypto scammers have deployed to defraud their victims and notable among these are:
• **Romance Scams:** Romance scams in the crypto space typically begin on dating apps or social platforms, where fraudsters build emotional connections under fabricated identities. Once trust is established, victims are manipulated into sending cryptocurrency to cover supposed emergencies or urgent expenses, often under strict instructions to keep the relationship secret.

• **Pig-butchering**: Pig-butchering scams, often disguised as crypto investment opportunities, involve prolonged grooming by fraudsters posing as romantic partners or successful traders. Over weeks or months, victims are persuaded to deposit funds into fraudulent platforms that simulate legitimate profits, only to face escalating demands for additional deposits to “unlock” their money. These schemes typically begin with outreach via SMS or social apps, rely on fake trading interfaces showing fabricated returns, and culminate in devastating financial losses once the deception unravels.

• **Fake investment platforms, projects, and ICOs:** Fraudulent investment platforms and token sales entice investors with promises of guaranteed returns and polished marketing, butlack any genuine project or roadmap. Victims are shown fabricated profits through slick apps or websites, sometimes allowed to withdraw small amounts to build confidence, before suddenly facing frozen accounts or locked withdrawals. These scams thrive on buzzwords without substance and ultimately end with the disappearance of investor funds once trust has been secured.

• **Rug Pulls and Exit Scam:** Rug pulls and exit scams occur when developers deliberately abandon a project after attracting investor funds, often by draining liquidity from a newly launched token or DeFi protocol. These schemes typically involve anonymous teams, lack of audits or code transparency, and culminate in sudden token price collapses once liquidity is removed. The result is that investors are left with worthless assets while the perpetrators vanish with the proceeds.

• **Ponzi and Pyramid Schemes**: Ponzi and pyramid schemes remain some of the most enduring forms of crypto fraud, relying on new deposits or recruits to sustain the illusion of profitability. In Ponzi models, early investors are paid with funds from later victims, while pyramid schemes emphasize aggressive recruitment with promises of referral payments. Both structures are inherently unsustainable, collapsing once new deposits slow, leaving participants with losses and no transparency around how funds were managed.

• **Phishing Scams:** Phishing scams exploit trust by impersonating reputable crypto services, tricking users into revealing private keys or signing malicious contracts. Victims are often lured through fake login portals, typosquatteddomains, or fraudulent QR codes, and may even receive spam tokens designed to redirect them to drainware contracts. Once credentials are compromised, scammers swiftly remove funds from wallets, leaving users with irretrievable losses.

• **Mining scams:** Mining scams entice victims with promises of effortless passive income through fraudulent cloud mining operations or hardware schemes. In reality, these ventures often lack any genuine mining infrastructure, instead pocketing deposits or operating as disguised Ponzi models. Hallmarks include fake dashboards showing fabricated yields, pressure to upgrade to higher “hash power” tiers, and a complete absence of transparency about actual facilities or partners.

• **Tech and IT support scams:** Tech and IT support scams exploit fear by impersonating exchange, wallet, or antivirus support teams to gain remote access to user devices. Victims are typically targeted through fake pop-ups, phishing emails, or unsolicited calls claiming urgent account compromise, and then pressured into installing remote desktop software. Once access is granted, scammers can seize control of accounts and drain funds, leaving users with significant losses.

Legal and Regulatory Framework

• **The ISA 2025:** The ISA 2025 marks a turning point in the regulation of digital assets, formally recognisingcryptocurrencies, tokens, and other blockchain-based instruments as securities. By expanding the definition of securities to include virtual assets, the Act subjects Virtual Asset Service Providers (VASPs), Digital Asset Operators, and Digital Asset Exchanges to the oversight of the SEC. This statutory recognition places digital assets under the same compliance obligations as traditional securities, including registration, capital adequacy, Know Your Customer protocols, Anti-Money Laundering measures, and mandatory reporting of suspicious transactions.

The ISA enhances investor protection by outlawing fraudulent schemes such as Ponzi models and granting the SEC broad enforcement powers. The SEC can seal prohibited operations, freeze and forfeit assets, and impose penalties of at least ₦20 million (approximately $12,430) or prison terms of up to ten years on offenders. It also has authority to access telecom and internet data to investigate market manipulation and insider trading, while Section 123 ISA introduces a legal entity identifier system to strengthen transparency and reduce systemic risk.

Dispute resolution has also been strengthened through the expansion of the Investments and Securities Tribunal (IST), which now has jurisdiction to hear cases involving digital assets and cryptocurrencies. This provides aggrieved investors with a formal channel to seek redress against the SEC or market operators, a development expected to boost confidence in Nigeria's capital markets. However, the effectiveness of the ISA will depend on robust enforcement and improved inter-agency coordination, ensuring that the promise of statutory recognition translates into real investor protection.

• **Central Bank of Nigeria Act 2007**: The Central Bank of Nigeria (CBN), established under the 2007 Act, issues Nigeria's legal tender and oversees financial stability. While the Act does not explicitly cover digital assets, CBN has historically restricted banks from dealing directly with cryptocurrencies. In 2023, however, CBN introduced guidelines for VASPs, requiring compliance with AML, CTF, and consumer protection standards. These guidelines marked a shift from outright prohibition toward structured oversight, aligning with the SEC's proactive stance on digital asset regulation. By 2024, the SEC began amending its Digital Assets Rules to explicitly include cryptocurrencies, signaling Nigeria's move toward formal recognition and regulation of crypto markets.

• **Money Laundering (Prevention and Prohibition) Act 2022:** The Money Laundering (Prevention and Prohibition) Act, 2022 explicitly includes virtual assets in its scope. Section 30 defines them as digital representations of value used for payment or investment, excluding fiat and securities. It also classifies VASPs as financial institutions, subjecting them to AML obligations like customer due diligence, record-keeping, and suspicious transaction reporting. VASPs must report transfers above certain thresholds to enhance transparency and oversight of crypto transactions. Penalties for violations are severe, with individuals facing at least four years imprisonment or heavy fines, and corporate bodies fined no less than five times illicit profits.

• **National Information Technology Development Agency Act 2007:** The National Information Technology Development Agency (NITDA) Act 2007 underpins Nigeria's tech regulatory framework. In 2023, NITDA introduced the National Blockchain Adoption Strategy to encourage blockchain use across sectors like finance and healthcare. While focused on blockchain innovation, the strategy indirectly supports cryptocurrency by promoting blockchain infrastructure. A key feature is the regulatory sandbox, which allows startups to test blockchain applications in a controlled environment. This initiative balances innovation with oversight, fostering safe experimentation and regulatory compliance.

Legal Remedy Available to Victims:
For victims of cryptocurrency fraud, investment scams and Ponzi schemes, the difficulty of tracing digital transactions does not place the wrongdoer beyond the reach of Nigerian law. The ISA, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended, the Proceeds of Crime (Recovery and Management) Act 2022 ("POCA"), and the general powers of the courts provide a number of regulatory, criminal and civil avenues through which victims may pursue redress.

The fact that crypto transactions may be pseudonymous or cross-border can make recovery more complicated, but it does not make recovery impossible. In appropriate cases, transactions can be traced, assets restrained, operators prosecuted and civil proceedings commenced against persons responsible for the loss.

• **Regulatory intervention under the ISA 2025:** - The ISA 2025 significantly strengthens the regulatory position of digital assets in Nigeria. The ISA expressly includes virtual assets, digital assets and other distributed ledger technology offers, tokens and products among recognised forms of investment, while empowering the SEC to regulate virtual and digital asset exchanges and related market activities.

This is particularly important in relation to fraudulent investment and Ponzi schemes. Section 196 empowers the SEC to enter and seal premises used for prohibited schemes and to seek an order of the Tribunal or a court freezing and forfeiting their assets. Operators of prohibited schemes also face substantial criminal sanctions. Victims should therefore consider making a formal complaint to the SEC where the fraud involves an investment platform, digital asset operator or unregistered investment scheme.

• **Criminal investigation and prosecution**: - Crypto scams are no longer "untraceable" crimes in the eyes of the state. Traditional statutes against fraud, money laundering, and embezzlement now apply to digital assets just as they do to cash. The Cybercrimes Act is the primary tool used to prosecute hackers and identity thieves, with penalties including prison terms of up to ten years. Victims may report suspected offences to the Economic and Financial Crimes Commission ("EFCC") and other appropriate law-enforcement agencies. The EFCC has developed specialized units to investigate these digital crimes, tracking the flow of "tainted" coins to bring scammers to justice.

• **Civil proceedings and preservation of assets** - A victim may pursue civil remedies against the persons or entities responsible for the loss. Where there is a real risk that identifiable assets will be dissipated before judgement, the court may, in appropriate circumstances, grant interim preservatory relief, including Mareva Injunction to "freeze" assets pending determination of the substantive claim. This was established the Supreme Court in the case of Sotuminu v Ocean Steamship (Nig) Ltd. A Mareva order prevents a scammer from disposing of or moving their assets (including crypto in Nigerian exchanges) until the court decides who the money belongs to.

Where the identity of the wrongdoer is unknown, it may also be possible, depending on the circumstances and the parties before the court, to seek disclosure orders against intermediaries such as banks or regulated exchanges to assist in identifying the persons behind relevant accounts or transactions. Such remedies are discretionary and will depend upon the evidence presented to the court. They should therefore not be described as automatic mechanisms for recovering cryptocurrency.

• **Recovery of proceeds of crime: -** The Proceeds of Crime (Recovery and Management) Act 2022 (POCA) provides an additional framework for tracing, restraining, confiscating and managing property representing the proceeds of unlawful conduct. This may be particularly relevant where fraud proceeds have been converted into cryptocurrency, transferred through several accounts or mixed with other property.

Importantly, asset recovery proceedings are distinct from an ordinary civil claim by the victim. The fact that assets are frozen or forfeited does not necessarily mean that they will automatically be returned to an individual complainant. Victims should therefore obtain advice on whether to pursue civil recovery alongside any regulatory or criminal investigation.

The practical lesson is that victims should act quickly. Transaction hashes, wallet addresses, screenshots, emails, payment records, bank statements and communications with the suspected operator should be preserved immediately. Where assets remain within a regulated exchange or identifiable bank account, early legal and regulatory intervention may significantly improve the prospects of preventing further dissipation.

Immediate Steps: What to Do If You Are Scammed

Victims of cryptocurrency fraud should act promptly, as delays may significantly reduce the prospects of tracing or recovering stolen assets. The following steps should be taken immediately upon discovering the fraud:

• **Secure your accounts:** Change the passwords to your cryptocurrency exchange accounts, email accounts and digital wallets without delay. Where available, enable multi-factor authentication and make use of any account suspension or wallet lock features provided by the exchange or wallet provider to prevent further unauthorised transactions.

• **Preserve evidence:** Record and retain all relevant evidence relating to the fraudulent transaction. This should include the transaction hash or Transaction ID (TxID), wallet addresses, screenshots, emails, text messages, chat histories, payment confirmations and any communications with the suspected fraudster. These records may prove critical during investigations and any subsequent legal proceedings.

• **Notify the cryptocurrency exchange or service provider:** Where the stolen assets have been transferred to or through a recognised cryptocurrency exchange, notify the exchange immediately. Although blockchain transactions are generally irreversible, exchanges may be able to freeze the recipient's account or wallet where the assets remain within their platform, thereby assisting law enforcement agencies in tracing or preserving the assets.

• **Report the matter to the appropriate authorities:** Victims should promptly report the incident to the relevant law enforcement agencies, including the Nigeria Police Force National Cybercrime Centre (NPF-NCCC) and the EFCC. The report should be accompanied by all available documentary evidence to facilitate investigation and possible asset tracing or recovery.

• **Seek legal advice:** Given the complexity of cryptocurrency transactions and the evolving regulatory framework, victims should obtain legal advice as early as possible. Depending on the circumstances, legal counsel may assist in pursuing civil remedies, seeking interim preservatory orders, engaging with cryptocurrency exchanges or coordinating with law enforcement agencies to maximise the prospects of recovery.

Conclusion

Nigeria's approach to cryptocurrency regulation has undergone a significant transformation. The enactment of the ISA 2025 marks a decisive shift from regulatory uncertainty to a more structured framework that recognises and regulates digital and virtual assets. While this development provides greater legal certainty, strengthens regulatory oversight and enhances investor protection, it does not eliminate the risks associated with cryptocurrency transactions.

Fraudsters continue to exploit the speed, anonymity and cross-border nature of digital assets, making vigilance an essential part of every investment decision. Nevertheless, victims of cryptocurrency fraud are no longer without legal recourse. Through a combination of regulatory intervention, criminal investigation, civil remedies and asset recovery mechanisms, Nigerian law now provides a more comprehensive framework for pursuing wrongdoers and, where possible, recovering misappropriated assets.

Ultimately, regulation alone cannot eradicate cryptocurrency fraud. Effective investor education, robust compliance by VASPs, stronger regulatory cooperation and timely enforcement will remain critical to fostering a safe and resilient digital asset ecosystem. As Nigeria's cryptocurrency market continues to mature, striking the right balance between innovation, investor protection and regulatory oversight will be essential to sustaining confidence in the digital economy.

Disclaimer:

The information provided in this publication does not, and is not intended to constitute legal advice. It is intended for general informational purposes only. Please contact us for further information.

© Copyright 2025 - Syntegral Legal Practicie