

May, 2026

SYNTEGRAL LEGAL PRACTICE

CRYPTO FRAUD, SCAMS AND PONZI SCHEMES: LEGAL REMEDIES FOR VICTIMS.

Authors



Oladiran Falore
Senior Partner



I.M Igwebuike
Associate Counsel

www.syntegrallp.com
info@syntegrallp.com
@syntegral_lp

INTRODUCTION

Digital asset fraud has moved from the margins of Nigerian financial life to its centre. The Securities and Exchange Commission ("the SEC") published, in March 2025, a list of fifty-eight Ponzi schemes operating in the country; the National Deposit Insurance Corporation has estimated that Nigerians lost approximately ₦911 billion to Ponzi-related schemes between 2000 and 2023. In April 2025, the Crypto Bridge Exchange (CBEX) collapse alone generated reported losses ranging, depending on the methodology, from $12 million to over $800 million, and an estimated 250,000 to 300,000 retail victims.

Nigeria's regulatory approach to cryptocurrency has evolved significantly over the past decade. The Central Bank of Nigeria ("the CBN") initially adopted a cautious stance in 2017 by warning financial institutions about the risks associated with virtual currencies. This position became stricter in February 2021 when the CBN directed banks and other financial institutions to cease facilitating cryptocurrency transactions and to close accounts connected with such activities. However, the restriction proved difficult to enforce effectively, as cryptocurrency transactions merely shifted to peer-to-peer channels outside formal banking oversight.

Recognising this reality, the CBN reversed its position in December 2023 through the issuance of the Guidelines on Operations of Bank Accounts for Virtual Assets Service Providers, which permitted banks to maintain accounts for SEC-licensed Virtual Assets Service Providers ("VASPs") subject to regulatory conditions. At the same time, the SEC expanded its regulatory role by introducing rules in 2022 governing digital assets, including crypto assets, utility tokens, security tokens, and crypto-related investment products, each with varying compliance and disclosure obligations.

The enactment of the Investments and Securities Act 2025 ("ISA 2025") represents the most significant milestone in Nigeria's digital asset regulatory framework. The ISA 2025 formally recognises virtual and digital assets as securities and grants the SEC clear authority to regulate digital asset exchanges and related market participants. This effectively resolves the previous uncertainty surrounding the legal status of cryptocurrencies in Nigeria. The Act also introduces stricter enforcement mechanisms by expressly criminalising Ponzi schemes and unregistered digital asset operations, with penalties including imprisonment for up to ten years and fines of up to ₦40 million.

Beyond the ISA 2025, there are other municipal laws that shape Nigeria's cryptocurrency regulatory framework;

1. The Money Laundering (Prevention and Prohibition) Act 2022 imposes customer due diligence and suspicious transaction reporting obligations on Virtual Assets Service Providers,

2. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended in 2024) addresses offences such as computer-related fraud, identity theft, and unauthorised access commonly associated with crypto scams.

3. Similarly, the Nigeria Data Protection Act 2023 regulates the processing and disclosure of customer data obtained through KYC procedures by exchanges and financial platforms.

4. Nigerian courts and practitioners also increasingly rely on persuasive English authorities in resolving cryptocurrency disputes. For instance, in AA v Persons Unknown, the English Commercial Court recognised bitcoin as property capable of being traced and protected through proprietary injunctions. Subsequent cases such as Fetch.ai v Persons Unknown further strengthened this principle by permitting freezing orders and disclosure applications against crypto exchanges.

Types of Crypto Fraud, scams and Ponzi Scheme

Cryptocurrency fraud schemes continue to evolve in sophistication, exploiting investor greed, technological ignorance, emotional vulnerability, and weak due diligence practices. One of the most prevalent categories remains Ponzi and high-yield investment schemes, which typically promise unrealistic returns within short periods while relying on continuous inflows from new investors to sustain payouts.

A notable Nigerian example is the collapse of CBEX, a platform that presented itself as an artificial intelligence-powered crypto trading exchange allegedly affiliated with the Beijing Equity Exchange. The platform promised investors returns of up to 100 percent within thirty days, accepted deposits in USDT, and heavily relied on referral-based recruitment structures characteristic of pyramid schemes.

By April 2025, withdrawal requests became delayed, users were compelled to pay so-called “verification fees” to unlock accounts, and the SEC subsequently issued a public warning against the platform before its eventual collapse. The Economic and Financial Crimes Commission (“EFCC”) later identified CBEX as a Ponzi scheme and commenced investigations, arrests, and international recovery efforts through Interpol. Similar schemes previously witnessed in Nigeria include MMM Nigeria, MBA Forex, Famzhi Interbiz, and Racksterli, while internationally notorious examples include BitConnect and OneCoin. These schemes commonly display warning signs such as guaranteed profits, opaque trading models, aggressive referral incentives, and false claims of regulatory approval or international licensing.

Another major category of cryptocurrency-related fraud involves exchange and platform failures, where users lose access to their funds due to security breaches, mismanagement, insolvency, or deliberate misconduct by operators. One significant Nigerian example is Patricia, a Lagos-based crypto and gift-card exchange that disclosed in 2023 that it had suffered a major security breach affecting customer bitcoin and naira balances. Following the incident, withdrawals were suspended, allegations of misappropriation emerged, and the platform controversially converted users’ outstanding balances into a proprietary token known as Patricia Token (PTK), prompting widespread accusations of an exit scam disguised as compensation. Similar international cases include the collapse of FTX in 2022 and QuadrigaCX in 2019, both of which resulted in substantial investor losses.

These incidents highlight the significant custodial risks associated with leaving large amounts of cryptocurrency on exchanges. Investors are therefore increasingly advised to assess whether platforms are properly licensed under the ISA 2025, review terms of service carefully, and where possible, move substantial holdings into private self-custody wallets rather than relying entirely on third-party custodial services.

Cryptocurrency scams also increasingly rely on social engineering and technical compromise. Romance scams and “pig-butchering” schemes have emerged as highly organised forms of fraud in which victims are manipulated through emotional relationships developed on dating applications, social media platforms, or messaging services. Fraudsters gradually build trust before directing victims to fake trading platforms displaying fabricated investment gains. These schemes are often linked to organised criminal networks operating across multiple jurisdictions.

Similarly, phishing attacks, SIM-swap fraud, and wallet compromise remain major threats within the cryptocurrency ecosystem. Fraudsters commonly impersonate exchanges,

wallet providers, or technical support teams through fake websites, malicious links, cloned applications, and phishing emails designed to steal login credentials, private keys, or seed phrases. In Nigeria, SIM-swap vulnerabilities have become particularly concerning because many users still rely on SMS-based two-factor authentication. Rug pulls and fraudulent token launches also remain widespread within decentralised finance ecosystems, where developers deploy tokens with hidden smart-contract vulnerabilities or withdraw liquidity after attracting investor deposits, leaving investors with worthless assets. These trends reinforce the importance of due diligence, cybersecurity awareness, hardware wallet usage, independent verification of projects, and careful scrutiny of token audits, liquidity structures, and founding teams before committing funds to any cryptocurrency project or platform.

Legal And Regulatory Framework Guiding the Crypto Market:

A. Criminal Law Instruments

Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended by the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, remains the principal legislation governing criminal complaints relating to cyber-enabled offences in Nigeria. Section 14 criminalises computer-related fraud, while Section 13 addresses identity theft and related offences. Significantly, the 2024 amendments further strengthen the legal framework for the prosecution of electronic fraud, unlawful interception of data, and unauthorised interference with computer systems, whilst also expanding the scope of offences relating to unauthorised access carried out for fraudulent purposes.

The Advance Fee Fraud and Other Fraud Related Offences Act 2006 also remains applicable in circumstances involving false representations intended to induce payments, particularly during the solicitation and investment stages commonly associated with Ponzi arrangements. In addition, the Money Laundering (Prevention and Prohibition) Act 2022 provides the basis for prosecuting persons involved in handling the proceeds of crypto-related fraud, including VASPs that fail to comply with applicable anti-money laundering obligations.

Furthermore, the Economic and Financial Crimes Commission (Establishment) Act 2004 and the Independent Corrupt Practices and Other Related Offences Commission Act 2000 establish and empower the principal enforcement and prosecutorial agencies in this area. The Criminal Code applicable in Southern Nigeria and the Penal Code applicable in Northern Nigeria also continue to provide for general offences such as obtaining property by false pretences, cheating, and stealing, which are frequently relied upon as alternative or ancillary charges in fraud-related prosecutions

B. Regulatory Instruments

The ISA 2025 vests the “SEC” with extensive regulatory and enforcement powers, including the authority to investigate, register, sanction, suspend, and, where necessary, prosecute operators of unregistered investment platforms and Ponzi schemes. In parallel, the anti-money laundering and counter-terrorism financing (“AML/CFT”) framework administered by the Central Bank of Nigeria (“CBN”) applies to financial institutions facilitating fiat currency on-ramp and off-ramp transactions, thereby creating a

thereby creating a regulatory mechanism for identifying, monitoring, and freezing suspicious proceeds before such funds exit the formal banking system. The Nigerian Financial Intelligence Unit ("NFIU") further performs a critical role in financial intelligence gathering, transaction tracing, and inter-agency coordination in relation to suspicious financial flows and illicit digital asset transactions.

C. Civil Foundations

From a civil law perspective, the tort of conversion may arise where the digital asset in question is treated as property capable of being wrongfully interfered with or appropriated. The viability of such a claim will largely depend on whether the court recognises the proprietary character of the asset. In circumstances where the disputed asset has already been converted into fiat currency, actions for money had and received, as well as broader restitutionary remedies based on unjust enrichment, may provide a more practical basis for recovery.

Equitable remedies such as tracing and constructive trust principles also remain relevant, particularly where misappropriated digital assets can be followed through identifiable wallets, exchanges, or intermediary accounts. These doctrines may enable a claimant to assert proprietary rights over traceable assets or their substitutes. In addition, contractual claims may arise against custodians, exchanges, or service providers where obligations contained in their terms of service have been breached. Claims in negligence may likewise arise where custodial entities fail to implement reasonable security standards or safeguards expected within the digital asset industry.

D. Constitutional and Procedural Backing

Section 44 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) guarantees and protects the right to property, thereby providing a constitutional foundation for proprietary claims and protection against unlawful deprivation of recovered assets. Furthermore, Section 321 of the Administration of Criminal Justice Act 2015 empowers courts, upon conviction of an offender, to make restitution orders in favour of identifiable victims, thereby reinforcing the compensatory and restorative dimensions of criminal proceedings involving financial and digital asset-related fraud.

Legal Remedy for Victims:

For victims of cryptocurrency fraud and Ponzi schemes, the path to justice is no longer an insurmountable "black hole" of anonymity. Nigeria has established a robust legislative architecture led by the ISA 2025 and the Proceeds of Crime (Recovery and Management) Act 2022 that recognizes digital assets as securities and prioritizes the recovery of stolen funds. While the technical nature of the blockchain means there is no "magic button" for an instant return, these evolving mechanisms provide a systematic framework for tracing, freezing, and eventually returning stolen capital through both civil litigation and criminal prosecution.

If you have fallen victim to a crypto scam, there are four primary legal pathways available for seeking justice and recovering your funds:

A. Regulatory Oversight: The SEC and Securities Laws -The ISA 2025 expanded the regulatory jurisdiction of the SEC over virtual assets, crypto-related investment arrangements, and VASPs. This development effectively subjects crypto-based investment schemes and digital asset platforms to securities regulation and regulatory supervision.

By bringing these activities within the scope of securities law, the SEC now possesses broader powers to investigate, regulate, suspend, sanction, and where necessary shut down unregistered or fraudulent investment platforms, including crypto-based Ponzi schemes. The SEC is also empowered to impose administrative penalties, freeze assets connected with unlawful investment activities, and enforce compliance obligations against operators who fail to adequately protect investors or comply with applicable regulatory standards

B. Criminal Law: Prosecution for Fraud and Cybercrime –Crypto-related fraud and digital asset scams are no longer viewed as legally obscure or untraceable activities. Existing criminal law frameworks relating to fraud, cybercrime, money laundering, and financial misconduct now apply with equal force to digital assets and blockchain-based transactions. The Cybercrimes (Prohibition, Prevention, etc.) Act, as amended in 2024, remains one of the principal statutory mechanisms for the investigation and prosecution of cyber-enabled financial crimes, including hacking, identity theft, unlawful access to systems, electronic fraud, and related offences. Depending on the nature and severity of the offence, the legislation prescribes significant penalties, including substantial fines and terms of imprisonment.

In practice, enforcement agencies such as the Economic and Financial Crimes Commission ("EFCC") have increasingly developed specialised investigative and digital forensic capabilities aimed at tracing suspicious blockchain transactions, identifying illicit financial flows, and tracking the movement of compromised or "tainted" digital assets across wallets and exchanges. These developments demonstrate a growing institutional capacity to investigate and prosecute crypto-related fraud within Nigeria's evolving digital financial ecosystem.

C. Civil Remedies: Restitution through the Courts - Victims of crypto-related fraud may also institute private civil proceedings before the Federal High Court to recover misappropriated funds and protect their proprietary interests. Even in circumstances where no criminal prosecution has commenced, an aggrieved party may apply for interim preservatory reliefs, including a Mareva Injunction, to freeze the suspected fraudster's bank accounts, digital wallets, or other identifiable assets pending the determination of the substantive suit. The legitimacy and applicability of Mareva reliefs within Nigerian jurisprudence was affirmed by the Supreme Court in *Sotuminu v. Ocean Steamship (Nig.) Ltd*, where the Court recognised the power of Nigerian courts to restrain a defendant from dissipating assets in a manner capable of frustrating the enforcement of a future judgment.

In the context of crypto fraud, such orders may be particularly significant in preventing the rapid transfer or dissipation of digital assets through exchanges or intermediary wallets. Although asset recovery remains challenging due to the pseudonymous nature of blockchain transactions and the cross-border structure of many fraudulent schemes, Nigerian courts may also grant Norwich Pharmacal orders compelling banks, exchanges, custodians, or other intermediaries to disclose identifying information relating to anonymous account holders or wallet operators connected to suspicious transactions. These disclosure mechanisms play a crucial role in tracing assets, identifying perpetrators, and facilitating both civil recovery and regulatory enforcement efforts

D. Asset Recovery Laws: The POCA 2022 Framework - In the past, seized money often sat in government accounts indefinitely. However, Part IX of the Proceeds of Crime (Recovery and Management) Act (POCA) 2022 established the Confiscated and Forfeited Properties Account at the Central Bank of Nigeria. The POCA provides a modern framework for seizing stolen property. One of its most important features is "Non-Conviction Based Forfeiture," which allows the court to seize money or crypto that is reasonably suspected to be the proceeds of fraud, even if the scammer hasn't been caught yet. The law specifically states that money recovered from crimes should be used for "reparations to victims". This law also ensures that once assets are recovered and forfeited to the government, they are kept in a special account designed to provide reparations to victims.

Immediate Steps: What to Do If You Are Scammed

A. Stop the Loss: Immediately change your passwords and enable two-factor authentication. If you use an app like Luno or Monica Cash, use their emergency "lock" features to prevent any more money from leaving.

B. Save the Trail: Identify the Transaction ID (TxID) for every fraudulent transfer. This is the unique fingerprint on the blockchain that allows the police to trace the funds.

C. Notify the Exchange: Tell the receiving exchange immediately. While they cannot "undo" a transaction, they can freeze the receiver's account to prevent them from cashing out.

D. Official Report: File a report on the NPF-NCCC portal or submit a formal signed petition to the EFCC with all your evidence.

Conclusion

Although blockchain technology was originally designed to promote decentralisation, speed, and transactional finality, the legal and regulatory landscape has steadily evolved to ensure that digital assets do not become safe havens for fraud, financial abuse, or criminal activity. Nigeria's transition from the restrictive banking measures introduced in 2021 to the more structured and comprehensive regulatory regime under the Investments and Securities Act 2025 represents a significant shift towards legal recognition, oversight, and investor protection within the digital asset ecosystem.

Today, victims of crypto-related fraud have access to a growing range of civil, criminal, regulatory, and equitable remedies capable of supporting asset tracing, preservation, and recovery. Through the combined use of interim court orders, disclosure mechanisms, regulatory intervention, and increasingly sophisticated blockchain investigative techniques, the prospects of identifying perpetrators and recovering misappropriated assets are considerably stronger than they once were.

While the pseudonymous and cross-border nature of blockchain transactions continues to present practical enforcement challenges, the Nigerian legal system is progressively demonstrating its willingness to adapt traditional legal principles to emerging digital realities. Ultimately, although vigilance and due diligence remain the first line of protection against digital asset fraud, the law is no longer passive in the face of technological abuse and increasingly serves as a meaningful avenue for accountability, enforcement, and redress in the digital age.

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.

www.syntegrallp.com
info@syntegrallp.com
syntegral_lp

© Copyright 2026 - Syntegral Legal Practicie