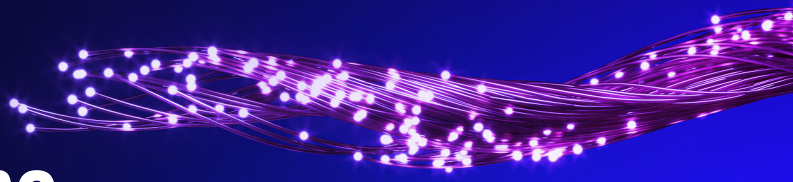
Rapidly changing regulatory landscape



The regulatory landscape for the digital asset industry is evolving rapidly, transitioning from regulatory uncertainty to enacted law and executive actions creating compliance frameworks. Actions taken by Congress and by the Trump Administration this year provide a tangible public policy direction and preview of changes to the regulatory environment for the digital asset industry.

- Congress overwhelmingly approved the **GENIUS Act**, which President Trump enacted into law on July 18, 2025[1]. The GENIUS Act establishes a regulatory framework for payment stablecoins in the United States, and specifically includes new AML requirements on stablecoin issuers where they will now be treated as financial institutions under the Bank Secrecy Act. These new requirements will include KYC standards, customer due diligence, and sanctions compliance.
- President Trump signed an Executive Order 14178,[2] **Strengthening American Leadership in Digital Financial Technology**, to "support the responsible growth and use of digital assets, blockchain technology, and related technologies across all sectors of the economy."
- The **US Securities and Exchange Commission (SEC)** established a dedicated **Crypto Task Force**[3] to "provide clarity on the application of the federal securities laws to the crypto asset market and to recommend practical policy measures that aim to foster innovation and protect investors."

The movement of legislative and regulatory clarity in 2025 suggests a potential for greater legitimacy for the crypto industry as well as a need to navigate new guardrails. KPMG LLP (KPMG) is equipped to assist our clients navigating these changes.

KPMG support for digital asset providers

KYC and AML solutions

- KYC program development: Establish tailored know your customer (KYC) programs covering customer identification, sanctions screening, ongoing due diligence, and risk rating, taking into account specific risks related to digital assets and crypto currencies.
- AML program design: Design anti-money-laundering (AML) programs specific to regulatory requirements for broad compliance as well as anticipated legislation and leading practices in the crypto industry.
- Compliance assessments: Perform AML program readiness and gap assessments to help clients meet compliance obligations and industry standards, including crypto compliance best practices.
- Blockchain integration support: Provide support for integrating blockchain analytical tools, including onboarding, customization, and optimization for smooth transition and enhanced benefits.

[1] https://www.congress.gov/bill/119th-congress/senate-bill/1582?q=%7B%22search%22%3A%22s.+1582%22%7D&s=1&r=1

[2] SEC.gov | Crypto Task Force

[3] Strengthening American Leadership in Digital Financial Technology – The White House

Ongoing monitoring and investigations

- Detect suspicious activity: Utilize blockchain monitoring systems to help identify and flag suspicious activities.
- Conduct internal reviews: Examine transaction details through thorough internal reviews to help ensure compliance and detect irregularities.
- Wallet investigation and tracing: Perform detailed tracing of digital wallets to help track the movement and flow of digital assets. Analyze the on-ramping and off-ramping processes to help identify the sources and destinations of funds.
- Improve compliance and rule sets: Provide oversight and refinement of compliance systems and rule sets, implementing and validating robust models for risk assessment, AML, KYC, and transaction monitoring, and adapting to regulatory changes and evolving risk landscapes.

Regulatory compliance and oversight solutions

- Develop STR/SAR filing process: Establish a robust process for filing Suspicious Transaction Reports (STR) and Suspicious Activity Reports (SAR) to help ensure compliance with regulatory requirements.
- Perform independent AML reviews: Conduct independent review and testing of all aspects of an AML program, providing observations and tailored recommendations aligned with regulatory standards.
- Conduct retrospective examinations: Perform retrospective examinations of digital asset transactions and develop targeted remediation strategies to help address any identified issues.
- Regulatory response implementation: Develop and execute action plans for responding to regulatory inquiries and audits, helping ensure timely and effective communication and compliance with all regulatory directives.

Training and leading practices

- Digital asset investigation training: Deliver training programs on digital asset investigations, covering essential concepts, regulatory compliance, and investigative techniques.
- Live on-chain demonstrations: Conduct live demonstrations of on-chain transactions and complex obfuscation schemes to help enhance practical understanding.
- Leading practices recommendations: Provide leading practices recommendations based on industry trends and extensive experience to help optimize investigation processes.
- Insights analysis: Offer insights analysis derived from current industry trends and expert experience to inform strategic decision-making in digital asset investigations.

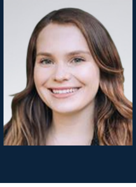
Contact us

John Caruso
Principal
Forensics – Financial Crimes
johncaruso@kpmg.com

Steven D'Antuono
Partner
Forensics – Financial Crimes
sdantuono@kpmg.com

Cory Lefkowitz
Director
Forensics – Financial Crimes
clefkowitz@kpmg.com

Mario Cosby
Manager
Forensics – Financial Crimes
mcosby@kpmg.com



Rebecca Crum
Senior Associate
Forensics – Financial Crimes
rcrum@kpmg.com

Emmett Brown
Senior Associate
Forensics – Financial Crimes
emmettbrown@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: in | **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.