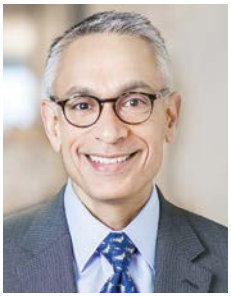
Strengthening AML and sanctions controls in the digital assets era

Received (in revised form): 13th November, 2025

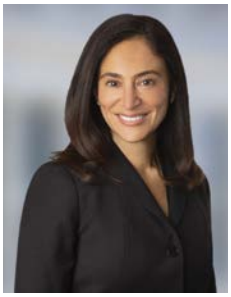
Satish M. Kini*
Partner, Debevoise & Plimpton, USA

Aseel M. Rabie**
Counsel, Debevoise & Plimpton, USA

Jonathan R. Wong†
Associate, Debevoise & Plimpton, UK



Satish M. Kini



Aseel M. Rabie

Jonathan R. Wong

Satish M. Kini *is the Co-Chair of Debevoise's National Security practice, the Chair of the Banking Group and a member of the Financial Institutions Group. He advises leading financial institutions on a broad range of US regulatory, compliance and transactional matters. Mr Kini represents banks, securities firms, insurers and asset managers in navigating complex regulatory frameworks, including those related to anti-money laundering, economic sanctions, data privacy and security, the Volcker Rule and affiliate transactions. He assists clients in developing robust compliance programmes and governance structures and regularly secures regulatory approvals for mergers, acquisitions and other transactions from US federal and state banking agencies. He also counsels clients on enforcement and examination matters before the federal banking agencies and the Office of Foreign Assets Control (OFAC) and provides guidance on cross-border regulatory issues, including sanctions and money laundering risks associated with international transactions and outsourcing arrangements. Mr Kini frequently advises financial institutions and industry trade associations on major regulatory reforms and engages with federal regulators and policymakers on behalf of clients and industry coalitions to shape and clarify key regulatory developments.*

Aseel M. Rabie *is a member of Debevoise & Plimpton LLP's National Security practice and the Banking and Financial Institutions Groups. Ranked in Chambers USA (2025) and Chambers Global (2026), Ms Rabie focuses her practice on advising financial institutions, multinational corporations and other clients on a broad range of regulatory, supervisory and enforcement matters in the sanctions and anti-money laundering space. She also works closely with clients on compliance programmes and risk mitigation strategies and provides counsel on matters involving financial crimes in the context of transactions, fundraising, lending and investigations. Ms Rabie provides guidance on navigating complex US regulatory requirements and frameworks, including those implemented by the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN). Her practice also encompasses engagement with US federal regulators, including the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), on policy, rulemaking and enforcement matters. Ms Rabie has extensive experience helping clients manage compliance and operational risks in international business contexts.*

Jonathan R. Wong *is a member of Debevoise & Plimpton LLP's National Security practice and the Banking and Financial Institutions Groups. His work focuses on regulatory, transactional and enforcement matters, with particular emphasis on anti-money laundering (AML) and sanctions matters and the Outbound Investment Security*

Journal of Financial Compliance
Vol. 9, No. 4 2026, pp. 323–339

2398-8061 (2026)

Journal of Financial Compliance is included in **The Business & Management Collection**

Program (OISP) governing US investments in certain national security technologies and products in countries of concern. Mr Wong advises US and non-US banks and other financial institutions on AML and sanctions compliance obligations, assisting clients in developing and refining policies and procedures. He also counsels clients on supervisory matters, including examinations, formal and informal enforcement actions, governance and regulatory reporting. In addition, Mr Wong supports the firm's private equity, M&A, finance and white collar & regulatory defence practices on transactional and enforcement matters involving AML, sanctions and OISP-related issues.

Abstract

This paper explores the anti-money laundering (AML) and sanctions regulatory environment for digital assets in the US, with particular emphasis on the emerging digital asset policy framework under the current presidential administration. The paper considers the principal illicit finance risks presented by digital asset activities and addresses key implications for AML and sanctions compliance controls for both digital asset firms and traditional financial institutions entering the digital asset ecosystem. Although US authorities have endorsed a more supportive approach to innovation and digital asset activities, regulators have simultaneously reaffirmed the importance of AML and sanctions compliance and risk management as key priorities. Among other topics, the paper discusses practical considerations and challenges related to leveraging blockchain analytics tools, structuring risk-based transaction monitoring procedures and addressing sanctions compliance obligations for digital asset transactions. The paper then addresses similar AML and sanctions control considerations from the perspective of traditional financial institutions that have dealings with digital asset firms or digital asset activities. For compliance teams and legal practitioners, this paper provides an actionable understanding of the AML and sanctions framework for digital assets and how to operationalise a compliance programme that appropriately addresses relevant risks and regulatory obligations. This article is also included in ***The Business & Management Collection*** *which can be accessed at https://hstalks.com/business/.*

Keywords: anti-money laundering (AML), sanctions, financial crime, digital assets, blockchain, crypto, illicit finance

DOI: 10.69554/ENVF3501

Debevoise & Plimpton LLP, 801 Pennsylvania Avenue NW, Washington, DC 20004, USA

**Tel: +1 202 383 8000; E-mail: smkini@debevoise.com*

***Tel: +1 (202) 383-8000; E-mail: arabie@debevoise.com*

†Debevoise & Plimpton LLP, The Northcliffe, 28 Tudor Street, London EC4Y 0AY, UK

Tel: +44 20 7786 3043; E-mail: jrwong@debevoise.com

INTRODUCTION

The regulation of digital assets has been one of the most contested recent US financial policy issues, demanding a balance between innovation and the various risks presented by digital asset activities. In July 2025, pursuant to President Trump's Executive Order 14178 of 23rd January, 2025, the President's Working Group on Digital Asset Markets released a report (the PWG Report) acknowledging, among other things, the importance of protecting the digital asset ecosystem by combatting the risks of illicit financial activity, while also calling for greater clarity around sanctions and anti-money laundering (AML) obligations and expectations to enable the lawful use of digital assets by individuals and firms.[1]

The current Trump administration has taken significant steps towards establishing a more friendly regulatory and supervisory environment with respect to digital asset activities. This includes the administration's emphasis on the need for risk-based supervision that allows financial institutions to adopt risk-based approaches to their AML and sanctions risk mitigation measures. At the same time, in contrast to certain other areas of regulatory enforcement or compliance, administration officials have also signalled that AML and sanctions compliance and enforcement will remain priorities.

Given the developing landscape for digital asset regulation and the continuing focus on AML and sanctions compliance, it is crucial for digital asset firms and traditional financial institutions that have relationships with digital asset firms to understand the AML and sanctions risks that may arise in the digital asset ecosystem and to adopt appropriate controls tailored to relevant risks.

This paper first summarises the changing financial crime regulatory landscape with respect to digital assets and the AML and sanctions risks associated with digital assets. The paper then outlines key AML and sanctions control considerations for both digital asset firms and traditional financial institutions engaging with digital asset activities and market participants. The paper concludes with expected developments related to emerging risks, evolving regulatory guidance and new regulatory obligations.

THE FINANCIAL CRIME LANDSCAPE FOR DIGITAL ASSETS

The AML regulatory landscape for digital asset activities in the USA has in recent years been defined largely by guidance issued in May 2019 by the US Treasury Department's Financial Crimes Enforcement Network (FinCEN), which provided comprehensive guidance on the application of AML regulations implementing the US Bank Secrecy Act (BSA) to various digital asset business models.[2] In particular, FinCEN's 2019 guidance explained that certain digital asset activities may trigger money services business (MSB) status and registration requirements along with associated AML programme and other compliance obligations. For the digital asset industry, this guidance has offered the most instructive insight into how FinCEN regards different business models for BSA/AML purposes.

In 2021, the US Treasury Department's Office of Foreign Assets Control (OFAC) issued its first consolidated guidance on sanctions compliance obligations for the virtual currency industry, emphasising that US sanctions compliance obligations apply equally to digital asset transactions and firms as they do to traditional financial transactions and institutions.[3]

In November 2023, digital asset AML and sanctions enforcement activity came into full view when the US Treasury Department (Treasury), including through FinCEN and OFAC, announced unprecedented, record-setting settlements totalling US$4.3bn against the virtual currency exchange Binance Holdings Ltd and its affiliates for US AML and sanctions violations, including wilful failure to establish, implement and maintain an effective AML programme.[4]

Key developments during the current Trump administration

Under the current Trump administration, US authorities are moving quickly to change the regulatory and supervisory posture towards digital asset activities. The July 2025 PWG Report calls for relevant agencies to re-examine AML and sanctions regulations and guidance applicable to digital assets, including providing clearer guidance to industry participants on AML risks and regulatory and supervisory expectations for digital asset activities. The report also echoes what the administration has said more broadly with respect to AML supervision, namely that firms' risk-based approaches should be respected under more effective risk-based supervisory approaches, including in the digital asset context.

The US Department of Justice (DOJ) has simultaneously adjusted its enforcement posture with respect to digital asset activities. In April 2025, Deputy Attorney General Todd Blanche released a memorandum on digital asset enforcement priorities (the Blanche Memo) stating that the DOJ will no longer 'pursue litigation or enforcement

actions that have the effect of superimposing regulatory frameworks on digital assets'.[5] Rather, the Blanche Memo emphasised that enforcement priority would be given to cases involving the victimisation of digital asset investors or the use of digital assets to further crimes such as terrorism, narcotics and human trafficking, organised crime, hacking and cartel and gang financing. The approach is in line with the administration's broader focus on combating illicit activity in the digital asset ecosystem.

The Trump administration supported the passage of the bipartisan Guiding and Establishing National Innovation for US Stablecoins Act (the GENIUS Act), which aims to create a comprehensive US regulatory framework for 'payment stablecoins' and was signed into law on 18th July, 2025.[6] The GENIUS Act, among other provisions, treats payment stablecoin issuers as financial institutions under the BSA subject to AML compliance obligations and calls for Treasury to take steps to consider innovative or novel methods, techniques or strategies that regulated financial institutions use, or have the potential to use, to detect digital asset-related illicit activity. The GENIUS Act also requires appropriate BSA and sanctions compliance standards and controls for US federally or state-licensed payment stablecoin issuers and foreign payment stablecoin issuers whose payment stablecoins are made available in the USA. This includes requiring that such issuers have the technological capability to comply with 'lawful orders' to seize, freeze, burn or prevent the transfer of their payment stablecoins.

More generally, although not pertaining specifically to digital asset AML and sanctions risks, the Trump administration has lowered barriers to financial institutions engaging in digital asset activities. In July 2025, the federal banking agencies [ie the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC)] issued a joint statement clarifying for supervised banks how existing risk management principles apply to crypto-asset safekeeping activities, albeit without announcing any new standards.[7] This statement followed the agencies' withdrawal of several 2023 joint statements that had been interpreted as discouraging banks from engaging in digital asset-related activities, and their rescission of prior approval or notice requirements for banks and bank holding companies to engage in digital asset-related activities.[8]

GENIUS Act implementation timeline

Many elements of the GENIUS Act require implementing regulations, including, as noted above, BSA and sanctions compliance standards for payment stablecoin issuers. These standards had not yet been implemented or proposed as of the date of this paper. However, the GENIUS Act establishes a phased regulatory and implementation timeline, including the following key deadlines:

- *14th January, 2026:*
    - The Secretary of the Treasury must submit to Congress a report outlining, among other things, novel and innovative methods, techniques or strategies to detect illicit activity involving digital assets and efforts to support financial institutions in implementing such measures.
- *18th July, 2026:*
    - Each primary federal payment stablecoin regulator (ie the FRB, FDIC, OCC, and the National Credit Union Administration), the Secretary of the Treasury and each state payment stablecoin regulator must promulgate regulations to carry out

the GENIUS Act through appropriate notice-and-comment rulemaking.

- *18th July, 2027:*
  - The Secretary of the Treasury should complete any reciprocal arrangements with jurisdictions that have comparable payment stablecoin regulatory regimes, including adequate AML and sanctions compliance standards.
- *18th July, 2028:*
  - FinCEN must issue guidance and rulemaking relating to methods to detect digital asset-related illicit activity, standards for payment stablecoin issuers to identify and report illicit activity involving payment stablecoins and standards for payment stablecoin issuers' monitoring of transactions on blockchains, digital asset mixing services, tumblers and similar services.
  - Digital asset service providers (DASPs) may not offer or sell a payment stablecoin to any person in the USA unless the payment stablecoin is issued by a permitted payment stablecoin issuer or a foreign stablecoin issuer that meets certain requirements.
- *General effective date:*
  - The GENIUS Act takes effect on the earlier of: (i) 18th January, 2027 (ie the date that is 18 months after the date of enactment); or (ii) the date that is 120 days after the primary federal payment stablecoin regulators issue implementing regulations.

In line with these steps, in August 2025, Treasury invited the public to provide comment on the use of innovative methods or strategies for detecting and mitigating illicit finance activity involving digital assets.[9] Treasury also issued an advance notice of proposed rulemaking seeking comment on potential regulations to implement the GENIUS Act, including in relation to AML and sanctions obligations.[10]

Non-US developments

Outside the USA, regulatory expectations for firms' digital asset financial crime controls are also in focus. For example, in July 2025, the UK sanctions authority, the Office of Financial Sanctions Implementation (OFSI), issued a crypto-asset sector threat assessment addressing threats to UK sanctions compliance involving digital asset firms to assist stakeholders with prioritisation as part of their risk-based compliance approaches.[11] In its report, OFSI set out relatively detailed regulatory expectations for due diligence and risk-based controls in the digital asset space, including in relation to common compliance issues for firms, such as setting thresholds for indirect sanctioned person exposure and minimum expectations for scanning certain numbers of 'hops' back in a chain of blockchain transactions. OFSI's publication may provide a useful benchmark for firms seeking to establish risk-based sanctions controls related to digital asset activities.

Evolving engagement with digital assets

As a result of changes in the regulatory and supervisory environment for digital assets, particularly under the current Trump administration, traditional financial institutions are looking to enter the digital asset ecosystem, including through various relationships with digital asset firms. At the same time, as the digital asset ecosystem matures, some digital asset firms are seeking to establish relationships with more traditional financial institutions.

Table 1: Representative examples of products and services that may involve digital asset firms and traditional firms

Asset management services	Execution and trading services
Digital asset exchange-traded products, investment funds or derivatives	Market making
Tokenisation of assets	Payments
Custody of native or tokenised assets	Cash management services
Custody of stablecoin reserves	Financing for mining equipment, digital asset-backed loans or other lending
Stablecoin or another digital asset administration/issuance	Plug-and-play/white labelling (eg banking-as-a-service, FinTech-as-a-service, crypto-as-a-service, wallet-as-a-service, mining-as-a-service, and staking-as-a-service)

The Wolfsberg Group, an association of 12 global banks that develops financial crime risk management frameworks and guidance, has provided various examples of products and services that may involve both digital asset and traditional firms, including those listed in Table 1, among others.[12]

Thus, there is increasing connectivity between the digital asset and traditional financial systems, making it incumbent on digital asset firms and traditional financial institutions alike to consider their AML and sanctions controls and risk-based compliance approaches in the digital asset space.

DIGITAL ASSET ILLICIT ACTIVITY RISKS

Despite technological differences in how digital asset and traditional financial transactions are conducted, the same types of illicit activity risks — eg facilitating money laundering, terrorism financing, or sanctions evasion — are presented, even if the means by which such risks may materialise or be mitigated are different. Moreover, digital asset firms that are MSBs or trust companies are subject to AML compliance obligations under the BSA that are in significant part similar to the obligations applicable to firms engaged in traditional financial services. Thus, similar core practices, including customer due diligence, transaction monitoring, suspicious activity reporting and sanctions screening, will support risk management in both the digital asset and traditional financial systems, although firms' implementation of related processes may vary due to technological differences.

A comparison of key characteristics of digital assets versus fiat currencies in Table 2 elucidates the point that the manner in which illicit finance risks may materialise, or may need to be mitigated, will vary depending on the medium of exchange involved.[13]

The nature of digital asset transactions, the types of bad actors that may be drawn to using digital assets and uneven AML and sanctions regulations and compliance in the digital asset ecosystem may heighten illicit finance risks related to digital assets. Risks related to each of these elements are described below.

Nature of digital asset transactions

The pseudonymity of digital asset transactions makes it more difficult for firms to determine which parties may be conducting or benefiting from such transactions. At the same time, the speed of digital asset transactions and the ability to transfer digital assets

Table 2: Comparison of key characteristics of digital assets and fiat currencies

Digital assets	*Fiat currencies*
Digital assets are decentralised and distributed through digital networks	Currency is centrally issued by a government
Transactions can be peer-to-peer and occur only between two parties	Transactions typically include at least one intermediary, such as a bank or payment provider
Transactions are recorded on a public ledger, but the identities behind wallets are typically not visible	Cash offers some degree of anonymity, but users transacting through financial institutions must disclose their identities
Transactions can be instantaneous, including across borders	Transactions can sometimes take multiple days to settle, particularly cross-border transactions involving multiple intermediaries
Digital assets can be highly volatile	Most currencies are generally relatively stable
Governed by majority rule and/or a network of users	Governed by a central bank

quickly across borders mean that firms may have a more limited opportunity to apply appropriate AML and sanctions diligence, monitoring or other controls and to interdict or block transactions.

Although transparent blockchains may provide a level of visibility into digital asset transactional flows and offer information that may be helpful in detecting potentially suspicious or illicit activity, widely available obfuscation methods and tools can make it more difficult in practice to obtain and analyse transactional information that would otherwise be visible. For example, as reflected in Table 3, bad actors may move digital assets through a sequence of 'hops', or transactions between blockchain addresses that increase the distance from the initial source.[14]

More sophisticated methods and tools present particular AML and sanctions concerns for digital asset transactions. These include mixers that obscure the origin and destination of digital asset transactions; anonymity-enhanced cryptocurrencies that use technology to limit the traceability of transactions; chain hopping to transfer value from one virtual currency to another on a different blockchain, often in rapid succession and peel chaining to move a large amount of digital assets from one wallet address through a series of smaller transactions to new addresses to conceal the source of the funds. Mixing to make transactions difficult to trace is depicted in Figure 1 for illustrative purposes.[15]

Treasury's 2023 Illicit Finance Risk Assessment of Decentralized Finance highlighted mixers, anonymity-enhancing services and bridges facilitating cross-chain activity as challenges to blockchain tracing and the identification of transaction participants.[16] The July 2025 PWG Report acknowledges that there may be valid

Table 3: Examples of 'hops' in a blockchain transaction

1 hop: Address A → End-User Address B
2 hops: Address A → Intermediate Address C → End-User Address B
3 hops: Address A → Intermediate Address C → Intermediate Address D → End-User Address B

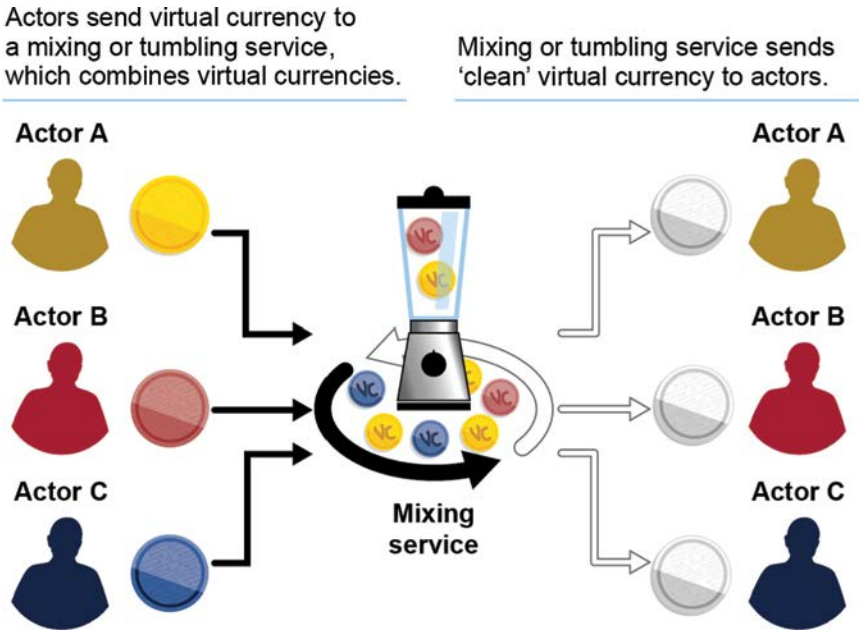


Figure 1 Mixing to make transactions difficult to trace

reasons for users to use privacy tools but also recognises that such tools can heighten illicit finance risks if they do not allow for or promote risk mitigation measures.[17] Further, activities can occur off-chain, and there are challenges associated with obtaining this data.[18] Thus, even though blockchains provide transaction information and blockchain analytics tools are available, various methods and tools present challenges to digital asset transaction monitoring approaches. For market participants, customers who use or transactions with a nexus to obfuscation or privacy-enhancing tools may warrant additional diligence and the use of these tools may be a red flag, depending on the relevant circumstances.

Variety in digital asset-related illicit activity

Although digital assets are used for lawful activities, they are known to be attractive to bad actors engaged in various forms of illicit activity, including ransomware, fraud, sanctions evasion, money laundering and drug-trafficking activity.

Well-known examples include North Korea's state-sponsored cyber-hacking Lazarus Group, which has long targeted digital asset platforms and users for digital asset heists and the obfuscation of its illicit activities, and which has been targeted under US sanctions by OFAC.[19] OFAC has also designated specific mixers, such as Blender.io, that have been identified as being involved in malicious cyber activities and the laundering of stolen digital assets, as well as other digital asset firms and related persons engaging in or supporting cybercrime, sanctions evasion, ransomware attacks and money laundering.[20] The July 2025 PWG Report recognises that ransomware groups continue to leverage digital assets as a favoured means of payment.[21]

More recently, in August 2025, FinCEN released an advisory urging financial institution to maintain vigilance regarding bad

actors using convertible virtual currency (CVC) kiosks to launder suspected drug proceeds and facilitate a variety of frauds, including elder fraud, government impersonation fraud, confidence/romance scams, emergency/person-in-need scams and lottery/sweepstakes scams.[22]

Thus, although not all digital asset transactions involve illicit activity, key characteristics of digital assets make them attractive to bad actors involved in a wide variety of frauds, scams and criminal activities. It is therefore important to consider risk factors relevant to different types of illicit transactions and to assess exposure to those risks comprehensively.

Uneven regulatory playing field

Uneven AML regulation between jurisdictions means that digital asset transactions, including on-ramps and off-ramps between the fiat and digital asset ecosystems, may pass through unregulated or less-regulated entities, which may elevate risks for transactions involving such entities. The July 2025 PWG Report also recognises that there is some lack of clarity regarding the applicability of AML compliance obligations to certain decentralised digital asset services for which, in any case, there may be no single intermediary that has control or visibility to conduct customer-level diligence, implement sanctions screening or perform other AML or sanctions controls. Consequently, illicit finance risks may be heightened for digital asset transactions that involve jurisdictions or entities that are not subject to sufficient AML obligations.

DIGITAL ASSET FIRM CONTROL CONSIDERATIONS

For digital asset firms, the threshold question in determining the controls that a firm should implement is whether the firm is a regulated financial institution subject to BSA/AML obligations (eg an MSB, a state-chartered trust company or, once the GENIUS Act becomes effective, a permitted payment stablecoin issuer).

However, even if a firm is not subject to affirmative BSA/AML obligations, there may be good reason for the firm to adopt certain risk-based controls. First, sanctions obligations apply to all digital asset firms that are US persons, regardless of their AML-regulated status. Further, even if a firm is not a regulated financial institution, if it has relationships with traditional financial institutions, it may be expected to provide information about its AML and sanctions compliance programme or may be required to represent that it maintains certain AML and sanctions controls to satisfy the other financial institutions' AML and sanctions risk management procedures.

The current administration has continued to emphasise the importance of AML and sanctions efforts to protect national and international security,[23] and institutions of varying types will be expected to take appropriate steps to mitigate risks presented by digital asset activities.

AML and sanctions risk assessments

Whether a firm is subject to regulatory AML obligations or not, the firm should conduct AML and sanctions risk assessments as the basis for developing a risk-based approach to its AML and sanctions controls.

This process would include assessing risk factors long outlined in supervisory guidance for financial institutions, such as risks presented by the geographic locations, customers, transactions and business activities specific to the firm, including risks associated with the firm's particular digital asset activities.[24] The firm's AML and sanctions policies, procedures and controls should then be tailored to reflect and address the risks identified through this process.

Customer identification and due diligence and sanctions screening

Firms should also implement appropriate controls to comply with applicable obligations to identify customers and conduct customer due diligence or otherwise to undertake appropriate risk-based know-your-customer diligence. Given that many digital asset firms onboard customers through non-face-to-face means, firms should ensure that their policies, procedures and relevant tools enable them to appropriately identify and verify the identities of their customers. These procedures should also include appropriate sanctions screening to ensure that firms do not engage in prohibited dealings with sanctioned persons.

In addition, if there is a risk that a digital asset firm's customers may access or use the firm's services from anywhere in the world, the firm may need to consider additional controls to mitigate AML and sanctions risks. For example, OFAC recommends that firms incorporate geolocation tools and Internet protocol (IP) address blocking controls to ensure that they do not provide services to parties in sanctioned jurisdictions.[25] OFAC has brought enforcement actions against digital asset firms that failed to screen IP and physical address information indicating that users were in sanctioned jurisdictions.[26] Other controls implemented by some digital asset firms to avoid dealings with sanctioned or high-risk jurisdictions include device telemetry tools to gather additional information indicating the location from which a customer may be accessing the firm's services.

Risk-based transaction monitoring

Firms may be subject to suspicious activity monitoring and reporting obligations for digital asset transactions. Given the nature of blockchain transactions, blockchain analytics tools are commonly used by firms to review and identify transactions that may involve potentially suspicious or illicit activity or that may involve sanctioned or other high-risk parties. Blockchain analytics firms provide tools to facilitate the identification, tracing and attribution of digital asset transactions on certain blockchains to real-world individuals.[27]

Blockchain analytics tools can be deployed in conjunction with transaction monitoring tools designed for fiat currency transactions to enable a firm to monitor activity that may occur across both the digital asset and traditional financial systems. Recent guidance from the New York State Department of Financial Services (DFS) provides examples of how firms may deploy blockchain analytics tools to monitor the activity of customers engaged in both digital asset and traditional fiat currency transactions, such as:

- screening wallets of customers who have disclosed or exhibited digital asset transactions to assess risk exposure;
- verifying the source of incoming funds originating from a DASP;
- monitoring the digital asset ecosystem holistically to assess customer (eg DASP) exposure to money laundering, sanctions violations or other predicate crimes;
- identifying and gauging the risk of third parties (eg DASP counterparties) with which a customer has engaged;
- evaluating expected versus actual activity (eg dollar thresholds) of customers engaging in digital asset activity;
- utilising intelligence gained from holistic monitoring to further develop the firm's risk assessments and risk appetite; and
- weighing the risks associated with a digital asset product or service to be offered.[28]

Importantly, blockchain analytics tools need to be tailored to a firm's activities and risks, and firms should develop procedures to enable the appropriate investigation and disposition of any alerts that may be generated

by such tools. In this regard, key factors to consider in relation to monitoring digital asset transactions include attribution, transaction interdiction and technical limitations for blockchain transactions, as described below.

Attribution

Because blockchain analytics tools use probabilistic methods to assess the risk that a transaction may be associated with high-risk wallets, such as wallets associated with sanctioned parties or scams, such tools' risk attribution for a particular transaction may not be accurate or may, in fact, change after the transaction as further information becomes available. Further, blockchain analytics firms may employ varying attribution methods. For example, some analytics tools may look back a certain number of hops in a transaction chain to identify potential exposure to high-risk wallets, whereas other tools may assess the portion of any given transaction that could be attributed to certain wallets, regardless of the number of intervening transactions that have occurred. As a result, different attribution methods could result in potentially inconsistent determinations. Moreover, even if a blockchain analytics tool indicates that a transaction may implicate a high-risk wallet, there may be other factors that affect the relevant risk considerations for the firm, such as the level of direct or indirect exposure to that wallet, the nature of any intervening transactions or parties and/or the timing of the alert.

Consequently, firms should consider risk-based approaches to determining the level of transaction screening conducted by any blockchain analytics tools (eg how many 'hops' back a transaction should be reviewed or what portion of a transaction implicating high-risk wallets should trigger an alert) and procedures for investigating and ultimately deciding on alerts generated by such tools. For example, a firm's risk-based approach might allow *de minimis* indirect exposure to a wallet attributed to a sanctioned person that is more than three hops removed in the chain of transactions and where the relevant digital assets have passed through an AML-regulated intermediary, absent other high-risk indicators and subject to enhanced monitoring of the relevant account, while calling for automatic freezing of transactions and accounts where exposure to sanctioned or other high-risk wallets is direct or indicative of potentially suspicious activity.

Transaction interdiction

Given the speed of digital asset transactions and the challenges involved in attribution as noted above, firms should consider their risk-based approaches to interdicting or freezing transactions. Digital asset firms may choose to temporarily hold assets when they identify suspected illicit activity. During the time those assets are held, firms can investigate and determine whether, for example the transaction involves sanctioned or stolen assets or has links to fraud or other criminal activity.

However, real-time review of transactions may be more challenging than reviews of historical activity, even when using blockchain analytics tools. Accordingly, firms should determine what level or type of exposure to sanctioned or high-risk wallets will result in automatic or manual freezes being placed on a transaction or a customer's account so that the firm may have adequate time to conduct appropriate diligence, assess the relevant risks and take appropriate steps, such as filing suspicious activity reports with the relevant authorities.

Technical limitations for blockchain transactions

Firms should consider technical limitations with respect to digital asset transactions

that may impact compliance with sanctions obligations. US sanctions require all US persons — including US-incorporated entities and their foreign branches, US citizens and permanent residents wherever located, and all individuals and entities within the USA — to block property and reject certain transactions involving sanctioned persons; failure to do so constitutes a sanctions violation. Non-US persons are likewise subject to certain sanctions prohibitions, including on processing transactions through the USA that are prohibited to US persons.

As noted earlier, the faster pace of digital asset transactions makes real-time transaction monitoring and interdiction more difficult. Further, even as blockchain analytics tools evolve and improve, the tools and techniques used by illicit actors to obscure their involvement in digital asset transactions and their identities are also rapidly shifting, which necessitates that firms regularly assess whether the tools they deploy are appropriately designed to mitigate relevant risks.

Moreover, regulators have recognised that firms may not be able to reject incoming transactions on the blockchain, even if the applicable sanctions regulations call for rejecting transactions involving certain sanctioned parties.[29] Some regulators have also taken the view that, given the immutability of blockchain transactions, the exposure to a sanctioned person in subsequent transactions does not disappear.[30] Thus, firms should determine how they wish to address scenarios involving potential exposure to sanctioned persons and implement appropriate procedures.

In making these control determinations, firms may reasonably vary in the approaches taken based on their particular risk profiles. However, a firm should ensure that its controls are grounded in its risk assessment and appropriately documented. A firm should also implement appropriate oversight and testing of its controls to ensure that they are applied consistently and updated as necessary to address any emerging risks.

CONTROL CONSIDERATIONS FOR TRADITIONAL FINANCIAL INSTITUTIONS

Under the current Trump administration, as discussed earlier, a more permissive regulatory and supervisory environment towards digital asset activities means that more traditional financial institutions may look to enter various types of relationships with digital asset firms. From an AML and sanctions perspective, for traditional financial institutions engaging in such relationships, many of the same core risk management principles will remain the same, but risk-based approaches and controls must be adapted to the digital asset context.

In this regard, one of the main challenges for traditional financial institutions may be upskilling compliance teams that only have experience in traditional financial systems and have a limited understanding of the digital asset space. Thus, as a foundational step, compliance teams should be trained and equipped to understand the digital asset ecosystem, assess risks relevant to different digital asset activities or participants with which the firm may be involved and apply AML and sanctions risk mitigation measures and controls that appropriately address those risks. Other key AML and sanctions compliance considerations for traditional financial institutions' relationships with digital asset firms are outlined below.

First, licencing and registration questions may be key diligence issues for digital asset firm counterparties or customers, including, for example, with respect to payment stablecoin issuer licencing regimes that come into effect under the GENIUS Act or other similar foreign licencing regimes. This is in line with existing supervisory due diligence expectations for financial institutions with respect to MSB customers.[31] For example,

a financial institution may consider obtaining appropriate assurances regarding, and/or conducting sufficient diligence to understand, whether a digital asset firm's business model triggers MSB registration requirements under FinCEN's 2019 guidance and whether the entity may be appropriately registered or licenced at the federal and state levels. If not, this may be a red flag for the financial institution to resolve before onboarding the digital asset firm. FinCEN's August 2025 advisory notes risks related to CVC kiosk operators that do not comply with MSB registration requirements and misrepresent their registration status to other financial institutions and indicates that financial institutions should treat as a red flag indicator the fact that a CVC kiosk business is not registered with FinCEN or does not maintain applicable state licences.

Second, financial institutions must understand the nature and purpose of their customer relationships with digital asset firm customers, including developing customer risk profiles by considering similar risk factors to those the financial institution would assess for other customers and customer relationships. Financial institutions should ensure they have a sufficient understanding of the digital asset ecosystem to assess the various risks that may be implicated by a digital asset customer and its related transactions and activities, particularly with respect to the contemplated relationship with the financial institution. For example, a bank that custodies reserve assets for a regulated stablecoin issuer subject to its own BSA/AML compliance obligations and BSA/AML supervision may assess its issuer customer as presenting different risks from another customer that operates a CVC kiosk. Alternatively, a financial institution may assess transactions involving non-US, unregulated exchanges as presenting different AML and sanctions risks from transactions through a US-based exchange conducting full customer identification and due diligence processes and implementing a US sanctions compliance programme. As part of financial institutions' due diligence frameworks for digital asset firms, institutions will need to decide whether and how enhanced due diligence should be applied to digital asset firms, including what additional diligence or risk mitigation measures may be implemented. Further, appropriate monitoring and ongoing diligence must continue after onboarding, as changes in a digital asset firm's activities may call for further diligence or risk mitigation measures.

As part of a financial institution's customer due diligence procedures, the institution should have a clear understanding of the scope of its customer relationship with a digital asset firm and how the institution will account for risks that may be related to the digital asset firm's underlying customers. For example, a bank that provides services to a digital asset firm may conclude that it does not have AML or sanctions obligations with respect to its digital asset firm customer's underlying customers, depending on the transactions and activities involved. However, in order for the bank to assess the risks of its direct customer relationship with the digital asset firm, it may still need to seek assurances from its digital asset firm customer that the firm is applying appropriate AML and sanctions controls to its underlying customers.

Accordingly, a financial institution engaging in relationships with digital asset firms should have an understanding of digital asset-related AML and sanctions controls and compliance programmes so that the institution can take an informed view as to whether a digital asset firm customer has implemented reasonably designed compliance programmes that will not expose the financial institution to undue risk. Given the Trump administration's signalling in the PWG Report that new or clarifying supervisory and regulatory guidance and expectations may be issued related to

digital asset activities and that GENIUS Act implementation steps are still forthcoming, financial institutions should stay abreast of developing regulatory and supervisory requirements and expectations for digital asset firms, as well as evolving market practices for AML and sanctions controls and risk management approaches adopted by digital asset firms.

Finally, financial institutions should consider whether their suspicious activity monitoring and reporting procedures and controls are appropriately tailored to address risks related to their activities in the digital asset ecosystem. This assessment will depend on a customer's exposure to digital assets, the types of transactions a financial institution will conduct with respect to a digital asset customer or counterparty, whether the financial institution will itself engage in any digital asset transactions and the particular nature of the products and services (including digital asset products and services) involved. Many of the same control considerations outlined earlier for digital asset firms will apply, and the financial institution will need to consider how to coordinate and implement risk-based compliance procedures and controls across its digital asset and traditional financial activities, as appropriate, to address holistically risks associated with transactions involving both digital and fiat currencies. Given the pace of technological change, evolving threats and regulatory developments, it will be important for financial institutions to re-evaluate and update their risk management frameworks periodically, as needed.

Financial institutions may also seek to partner with digital asset firms to enable their customers to engage in digital asset transactions. In such relationships, many of the same considerations already addressed will apply, including the need for a financial institution to understand its digital asset firm service provider's AML and sanctions compliance programme and controls. Additional considerations may include clearly allocating responsibilities between the financial institution and its digital asset firm service provider for AML and sanctions controls applicable to the digital asset transactions of the financial institution's customers, including ongoing suspicious activity monitoring and reporting responsibilities and arranging appropriate information sharing between the parties. The financial institution should also maintain appropriate oversight and testing processes for AML and sanctions functions implemented by the digital asset firm.

CONCLUSION

The digital asset regulatory and supervisory framework is undergoing significant change, and further developments related to the AML and sanctions risks and compliance obligations for digital asset firms and traditional financial institutions engaged in digital asset activities are on the horizon. Looking ahead, expected developments should fall broadly into three categories: emerging risks, evolving regulatory guidance and new regulatory obligations.

Regulators have warned that changes to digital asset uses, technologies and markets could increase AML and sanctions risks. To date, the use of digital assets has remained far below that of traditional fiat currency transactions; however, greater uptake of digital assets may lead to a higher incidence and scale of illicit finance activity using digital assets. There is also an ongoing race between the evolution of digital asset technologies and techniques used to facilitate illicit financial activity and the tools being developed to prevent such activity. Firms that engage in digital asset activity should stay up to date with the rapidly changing risk landscape and relevant guidance from law enforcement and regulatory authorities regarding new risks.

As regulators gain a greater understanding of the digital asset ecosystem and the various

technologies and parties involved, more developed guidance should be issued regarding regulatory expectations and standards for firms' AML and sanctions risk management. Such guidance may help firms operationalise core requirements or functions, such as customer due diligence obligations, suspicious activity detection and reporting, sanctions screening, third party oversight and governance and testing, and may assist firms in assessing whether their controls are appropriately calibrated to their specific customers and activities. That said, to the extent regulators do not fully understand or appreciate the technical and operational complexities of digital asset transactions or the connectivity between digital assets and the traditional financial system, such guidance could present challenges for firms' compliance efforts.

Finally, as evidenced by the GENIUS Act, new regulatory obligations may be imposed on digital asset firms or activities. As a result, both digital asset firms and traditional financial institutions engaged in digital asset activities should stay abreast of the developing regulatory environment and ensure that their compliance programmes account for applicable regulatory requirements.

AML and sanctions risks related to digital asset activities remain a priority focus area for US authorities and must be managed appropriately. For both digital asset firms and traditional financial institutions engaged in digital asset activities, compliance teams must ensure they understand and appropriately assess their digital asset-related AML and sanctions risks and apply AML and sanctions risk management principles appropriately in the digital asset context.

References

(1) President's Working Group on Financial Markets (30th July, 2025) 'Strengthening American Leadership in Digital Financial Technology', available at https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf (accessed 5th March, 2026).

(2) FinCEN, FIN-2019-G001 (9th May, 2019) 'Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies', available at https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf (accessed 5th March, 2026).

(3) OFAC (October, 2021) 'Sanctions Compliance Guidance for the Virtual Currency Industry', available at https://ofac.treasury.gov/media/913571/download?inline (accessed 5th March, 2026).

(4) U.S. Department of the Treasury (21st November, 2023) 'U.S. Treasury Announces Largest Settlements in History With World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws', available at https://home.treasury.gov/news/press-releases/jy1925 (accessed 5th March, 2026).

(5) U.S. Department of Justice (7th April, 2025) 'Office of the Deputy Attorney General, Ending Regulation by Prosecution', available at https://www.justice.gov/dag/media/1395781/dl?inline (accessed 5th March, 2026).

(6) Guiding and Establishing National Innovation for U.S. Stablecoins Act, Pub. L. No. 119-27, 139 Stat. 419 (2025), codified at 12 U.S.C. §§ 5901-5916.

(7) FDIC *et al.* (14th July, 2025) 'Crypto-Asset Safekeeping by Banking Organizations', available at https://www.fdic.gov/interagency-statement-crypto-asset-safekeeping.pdf (accessed 5th March, 2026).

(8) *See*, *e.g.*, FDIC (24th April, 2025) 'Agencies Withdraw Joint Statements on Crypto-Assets', available at https://www.fdic.gov/news/press-releases/2025/agencies-withdraw-joint-statements-crypto-assets (accessed 5th March, 2026); FDIC, FIL-7-2025 (28th March, 2025) 'FDIC Clarifies Process for Banks to Engage in Crypto-Related Activities', available at https://www.fdic.gov/news/financial-institution-letters/2025/fdic-clarifies-process-banks-engage-crypto-related (accessed 5th March, 2026); FRB (24th April, 2025) 'Federal Reserve Board Announces the Withdrawal of Guidance for Banks Related to Their Crypto-Asset and Dollar Token Activities and Related Changes to its Expectations for These Activities', available at https://www.federalreserve.gov/newsevents/pressreleases/bcreg20250424a.htm (accessed 5th March, 2026); OCC (7th March, 2025) 'OCC Clarifies Bank Authority to Engage in Certain Cryptocurrency Activities', available at https://www.occ.treas.gov/news-issuances/news-releases/2025/nr-occ-2025-16.html (accessed 5th March, 2026).

(9) U.S. Department of the Treasury (18th August, 2025) Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets, 90 Fed. Reg. 40148. In March 2026, Treasury issued a report to the US Congress on innovative technologies to counter illicit finance involving digital assets, as required under the GENIUS Act. U.S. Department of the Treasury (March 2026)

'Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets', available at https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf (accessed 26th March, 2026).

(10) U.S. Department of the Treasury (19th September, 2025) GENIUS Act Implementation, 90 Fed. Reg. 45159. Some federal payment stablecoin regulators have proposed regulations to implement the GENIUS Act, and AML and sanctions standards under the GENIUS Act are expected to be proposed in April 2026.

(11) OFSI (21st July, 2025) 'Cryptoassets Threat Assessment', available at https://assets.publishing.service.gov.uk/media/687e6362791bb4d8c309a06e/OFSI_Cryptoassets_Threat_Assessment.pdf (accessed 5th March, 2026).

(12) The Wolfsberg Group (2024) 'The Wolfsberg Group Frequently Asked Questions (FAQs) on Defining Digital Assets', p. 14, available at https://db.wolfsberg-group.org/assets/344e51dd-243c-4fe8-adfa-0e1d6567c4ed/Digital%20Assets%20FAQs%20-%20For%20publication.pdf (accessed 5th March, 2026).

(13) *See*, *e.g.*, Elliptic (28th September, 2023) 'What Is Blockchain Analytics?', available at https://www.elliptic.co/blockchain-basics/what-is-blockchain-analytics (accessed 5th March, 2026).

(14) OFSI, Cryptoassets Threat Assessment, *supra* note 11 at 12.

(15) U.S. Government Accountability Office, GAO-24-106178 (December, 2023) 'Economic Sanctions: Agency Efforts Help Mitigate Some of the Risks Posed by Digital Assets', p. 17, available at https://www.gao.gov/assets/d24106178.pdf (accessed 5th March, 2026).

(16) U.S. Department of the Treasury (April, 2023) 'Illicit Finance Risk Assessment of Decentralized Finance', p. 33, available at https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf (accessed 5th March, 2026).

(17) *Supra* note 1 at 103.

(18) *Supra* note 16.

(19) *See*, *e.g.*, U.S. Department of the Treasury (13th September, 2019) 'Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups', available at https://home.treasury.gov/news/press-releases/sm774 (accessed 5th March, 2026).

(20) *See*, *e.g.,* U.S. Department of the Treasury (6th May, 2022) 'U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats', available at https://home.treasury.gov/news/press-releases/jy0768 (accessed 5th March, 2026); U.S. Department of the Treasury (14th August, 2025) 'Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals', available at https://home.treasury.gov/news/press-releases/sb0225 (accessed 5th March, 2026).

(21) *Supra* note 1 at 102.

(22) FinCEN, FIN-2025-NTC1 (4th August, 2025) 'FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity', available at https://www.fincen.gov/system/files/shared/FinCEN-Notice-CVCKIOSK.pdf (accessed 5th March, 2026).

(23) *See*, *e.g.*, U.S. Department of the Treasury (4th November, 2025) 'Treasury Sanctions DPRK Bankers and Institutions Involved in Laundering Cybercrime Proceeds and IT Worker Funds', available at https://home.treasury.gov/news/press-releases/sb0302 (accessed 5th March, 2026) (explaining sanctions were imposed "to reaffirm our commitment" to targeting support for malicious North Korean activities that "pose a threat to our citizens, international security and the global digital economy"); U.S. Department of the Treasury (17th September, 2025) 'Remarks by Under Secretary for Terrorism and Financial Intelligence John K. Hurley at the Association of Certified Anti-Money Laundering Specialists Assembly Conference', available at https://home.treasury.gov/news/press-releases/sb0251 (accessed 5th March, 2026) (stating the "North Star" of BSA/AML modernization "will be to remain laser focused" on "law enforcement and the national security establishment").

(24) Federal Financial Institutions Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual, BSA/AML Risk Assessment, available at https://bsaaml.ffiec.gov/manual/BSAAMLRiskAssessment/01 (accessed 5th March, 2026).

(25) OFAC, Sanctions Compliance Guidance for the Virtual Currency Industry, *supra* note 3 at 14.

(26) *See*, *e.g.*, OFAC Settles with Bittrex, Inc. for $24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs (11th October, 2022), available at https://ofac.treasury.gov/media/928746/download?inline (accessed 5th March, 2026).

(27) These same tools also are used by government authorities to identify actors using digital assets for illicit finance activities and to undertake investigation and enforcement activities. U.S. Government Accountability Office, Economic Sanctions: Agency Efforts Help Mitigate Some of the Risks Posed by Digital Assets, *supra* note 15 at 32–33.

(28) DFS (17th September, 2025) 'Industry Letter Regarding Notice on Use of Blockchain Analytics for New York Banking Organizations', available at https://www.dfs.ny.gov/industry-guidance/industry-letters/il20250917-blockchain (accessed 5th March, 2026). Although this guidance is directed to banking institutions, the examples DFS provides have relevance also to digital asset firms.

(29) *See* FinCEN, Frequently Asked Questions, Subject: Section 9714 Order Prohibits Certain Transmittals of Funds Involving Bitzlato, p. 3 (18th January, 2023), available at https://www.fincen.gov/system/files/shared/FAQs_Bitzlato%20FINAL%20508.pdf (accessed 5th March, 2026) ("FinCEN recognizes that, under certain circumstances, covered financial institutions may be subject to technological constraints that limit their ability to decline or reject incoming CVC transfers from addresses outside of their control."). With respect to payment stablecoins however, and as discussed above in Section I.A., the GENIUS Act will require U.S. federally or state-licensed payment stablecoin issuers and foreign payment stablecoin issuers whose payment stablecoins are made available in the United States to have the technological capability to comply with "lawful orders" to seize, freeze, burn or prevent the transfer of their payment stablecoins. Such orders are expected to include U.S. sanctions prohibitions. *See* U.S. Department of the Treasury, GENIUS Act Implementation, *supra* note 10 at 45162 ("In the economic sanctions context, lawful orders will include sanctions designations.").

(30) OFSI, Cryptoassets Threat Assessment, *supra* note 11 at 13.

(31) Federal Financial Institutions Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual (n.d.) 'Nonbank Financial Institutions—Overview', available at https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaundering AndTerroristFinancing/22 (accessed 5th March, 2026).