Articles + Publications | March 2, 2026

Despite Changing Priorities, DOJ's Money Laundering, Narcotics, and Forfeiture Section Enforces AML Requirements Against Cryptocurrency Marketplace

WRITTEN BY

Ryan DiSantis | Lawrence J. Cameron | Michael S. Lowe | Edward M. Nogay | Ryan Last

Guilty pleas by a now defunct crypto exchange and its co-founder and former chief technology officer (CTO), along with the recent arrest of its other co-founder and former chief executive officer (CEO) in the Eastern District of California, send a strong reminder to the digital assets industry that it cannot grow lax in establishing, implementing, and maintaining robust anti-money laundering (AML) compliance programs. This case also illustrates that, consistent with the Criminal Division's May 2025 White-Collar Enforcement Plan, the Department of Justice (DOJ) continues to prioritize holding individual wrongdoers accountable.

The Company

On December 9, 2025, Paxful Holdings, Inc. (Paxful), an online cryptocurrency marketplace, pleaded guilty to three counts of conspiracy related to: (1) operating an unlicensed money transmitting business (MTB), (2) failing to comply with its AML obligations under the Bank Secrecy Act (BSA), and (3) violating the Travel Act. Under a plea agreement executed in 2024 and accepted by the court in December 2025, Paxful agreed to pay a $4 million criminal penalty, reflecting its limited ability to pay as it winds down operations. Paxful also agreed to a separate $3.5 million penalty imposed by the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), substantially reduced from a potential $112.5 million penalty in light of the company's financial condition.

According to the plea agreement, Paxful operated a cryptocurrency marketplace but willfully failed to establish, develop, implement, and maintain an effective AML compliance program, resulting in the platform being used to transfer the proceeds of, among other things, fraud schemes, illegal prostitution, and hacks by malign state actors.

Established in 2015, Paxful, among other things:

- Failed to designate an AML compliance officer until 2018;
- Failed to train employees on AML and know-your-customer (KYC) requirements until 2019;
- Did not verify the true identities of customers as required under applicable laws, regulations, and rules;
- Marketed itself to customers as a platform where users could buy and sell cryptocurrency without providing government-issued identification or other standard KYC documentation;
- Facilitated transactions associated with illegal activity but failed to file suspicious activity reports (SARs); and
- Falsely represented the strength and scope of its AML compliance program to other financial institutions.

The Paxful resolution demonstrates that, even where a company is insolvent or winding down, DOJ and FinCEN will pursue criminal and civil enforcement for willful AML failures, but may calibrate monetary penalties based on an ability-to-pay analysis.

The Executives

Artur Schaback (Co-founder and former CTO)

In addition to the company, in July 2024, Paxful's co-founder and former CTO, Artur Schaback, pleaded guilty to a conspiracy charge arising from Paxful's failure to maintain an effective AML compliance program. Schaback is cooperating with the government and faces a statutory maximum sentence of up to five years in prison, but has not yet been sentenced, as the sentencing has been repeatedly delayed and has not yet occurred.

Ray Youssef (Co-founder and former CEO)

Most recently, federal prosecutors have charged Paxful's other co-founder and former CEO, Ray Youssef, with charges similar to Schaback, including conspiring to evade AML requirements, operating an unlicensed MTB, and facilitating illegal prostitution-related activities through the crypto exchange's operations. The indictment alleges Youssef helped design a business model that targeted illicit "vice industries," including enabling crypto payments for prostitution advertising websites such as the defunct Backpage.com. Youssef, arrested earlier in February, has publicly claimed he is being targeted for his crypto advocacy and has vowed not to plead guilty and to fight the charges.

Takeaways

This criminal action confirms that DOJ continues to prioritize promises made in its May 2025 memorandum setting out the Criminal Division's White-Collar Enforcement Plan for the new administration. Specifically, the memorandum stated: "[I]n the digital assets context, prosecutors should 'focus on prosecuting individuals who victimize digital asset investors, or those who use digital assets in furtherance of criminal offenses.'" As shown here, the Division is actively working to identify, investigate, and prosecute both corporate and individual criminal wrongdoing and prioritizing schemes involving senior-level personnel or other culpable individual actors. The Criminal Division developed these policies "because justice demands the equal and fair application of criminal laws to individuals and corporations who commit crimes," noting that "[t]he Department's first priority is to prosecute individual criminals."

The case also illustrates that, despite the current administration's stated efforts to move away from "regulation by prosecution" in the digital assets industry, as stated in the deputy attorney general's digital assets memorandum, DOJ's Criminal Division's Money Laundering, Narcotics, and Forfeiture Section (formerly known as MLARS) in coordination with FinCEN, continues to bring BSA-based charges where it can establish knowing and willful violations tied to significant underlying criminal activity. As described in the digital assets memorandum, federal prosecutors are directed not to charge regulatory violations in digital asset cases under the BSA or for operating an unlicensed MTB *absent* evidence of knowing and willful misconduct. This approach is consistent with the Criminal Division's May 2025 white-collar enforcement priorities to pursue digital asset cases where *willful* violations facilitate substantial criminal conduct such as fraud, exploitation, or other criminal offenses.

Paxful's resolution with the DOJ also highlights the distinction between voluntary self-disclosure and receiving cooperation credit. The plea agreement noted that Paxful did not receive credit for voluntarily self-disclosing its misconduct under the Criminal Division's Corporate Enforcement and Voluntary Self-Disclosure Policy (CEP), but because the company did not self-report its misconduct before it was already on the government's radar. It did, however, receive meaningful credit under the policy for cooperating with the DOJ's investigation by, among other things: (1) promptly collecting, analyzing, and organizing voluminous information; (2) providing timely updates on facts learned during its internal investigation; and (3) making detailed factual presentations to the government. In addition, Paxful received cooperation credit for taking extensive and timely remedial measures, including engaging an external auditor to enhance its compliance program, using automated tools to assist with the implementation of its KYC and AML compliance policies, and working with federal law enforcement to respond to law enforcement requests despite having moved its operation outside the United States.

For companies in the digital asset space, the distinction matters: early voluntary self-disclosure can materially improve the outcome, but robust cooperation and remediation can still meaningfully influence charging decisions and penalty outcomes where self-disclosure is no longer available.

Cryptocurrency companies should also consider using automated tools to enhance the effectiveness of their AML controls. Banks and other financial institutions doing business with cryptocurrency companies should closely review those companies' compliance programs for these components. Financial institutions in the digital assets industry must continue to maintain and regularly review their AML compliance programs to avoid willful violations.

In particular, companies operating in the cryptocurrency industry should ensure they:

1. Promptly designate and empower a qualified AML compliance officer with sufficient authority and resources;
2. Implement robust KYC identification and verification procedures, including for higher-risk customers and counterparties;
3. Provide timely and ongoing AML/KYC training to relevant personnel tailored to the company's business model and risk profile;
4. Monitor for and timely report suspicious activity, including filing SARs where appropriate, supported by effective transaction monitoring;
5. Accurately describe the strength and scope of their AML compliance programs to banks and other counterparties; and
6. Conduct periodic risk assessments and independent testing of their AML compliance programs, and remediate identified gaps.

Troutman Pepper Locke is closely monitoring this development in digital asset enforcement and the current administration's evolving priorities. If you have questions on how these priorities impact your business or wish to begin evaluating your existing compliance programs, please do not hesitate to contact a member of our White Collar Litigation and Investigations team.

RELATED INDUSTRIES + PRACTICES

- White Collar Litigation + Investigations