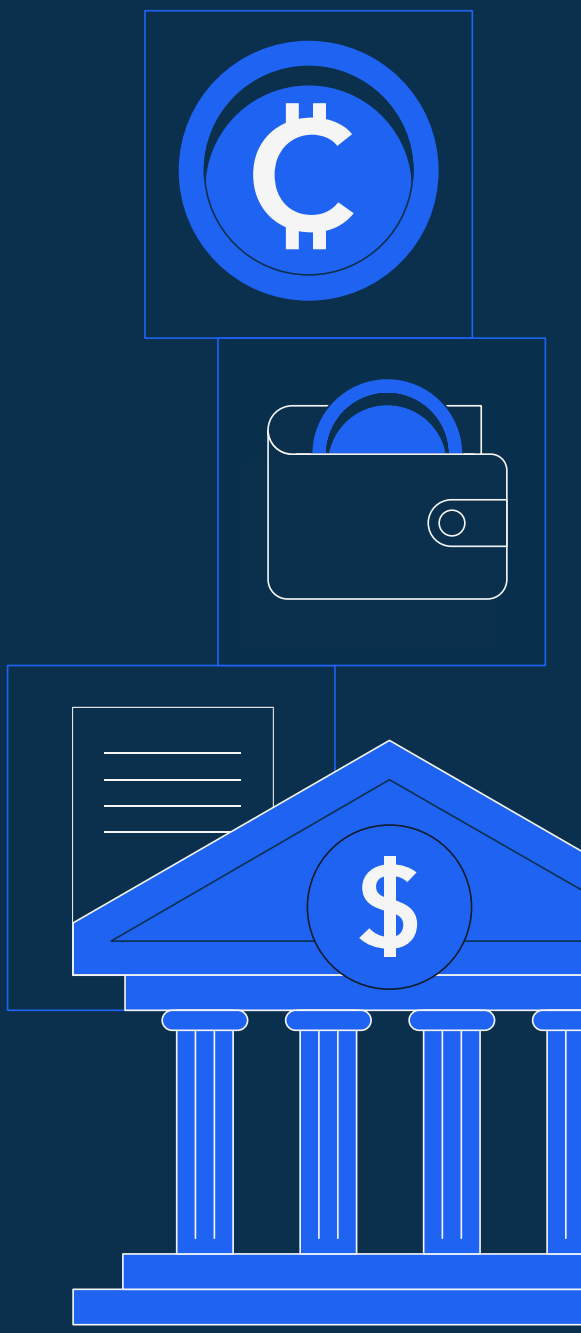
TRM GUIDE

## Part V

# Best Practices for Navigating the Regulators



CRYPTO COMPLIANCE PROGRAM GUIDE
FOR FINANCIAL INSTITUTIONS

TRMLABS.COM

Banks' journey into cryptocurrency began in earnest in the late 2010s, when a handful of institutions started exploring services like custody of digital assets and providing accounts for crypto exchanges. These early ventures were quickly met with a wary regulatory posture.

Bank supervisors, concerned about untested risks, often responded with more friction than facilitation. In some cases, this took the form of direct intervention. The Federal Deposit Insurance Corporation (FDIC), for example, quietly instructed two dozen banks to "pause" their crypto-related activities pending further review. These so-called "pause letters," later brought to light through FDIC records, signaled the extent of regulators' early skepticism.

Public supervisory statements from that period echoed a similar caution. In January 2023, the Federal Reserve, FDIC, and Office of the Comptroller of the Currency (OCC) issued a rare joint warning about crypto asset risks in banking. They pointedly cautioned that certain crypto activities were "highly likely to be inconsistent with safe and sound banking practices." The agencies catalogued a litany of concerns — from fraud and legal uncertainties to the volatility of crypto markets — and indicated a "careful and cautious approach" to any bank involvement in the sector.

Notably, regulators also stressed that banks were "neither prohibited nor discouraged" from serving lawful crypto clients. In practice, however, the tone of supervision was unmistakably guarded. The early history of banks in crypto was defined by this push-and-pull: banks eager to innovate on one side, regulators pressing the brakes on the other.

## The Trump-era pivot

As 2025 began, global regulatory momentum around crypto was accelerating — particularly in EMEA. The European Union's Markets in Crypto Assets Regulation (MiCA) had entered into force, offering a comprehensive and harmonized framework for crypto oversight across the bloc. In the UK, the Financial Conduct Authority (FCA) expanded its registration regime and introduced stricter advertising standards for crypto firms. Meanwhile, the UAE and Switzerland continued to attract digital asset firms with clear licensing structures and pro-innovation regulatory sandboxes.

Against this backdrop of increasing international clarity, the United States stood at a crossroads — prompting the Trump administration to reevaluate its own posture toward banks and crypto.

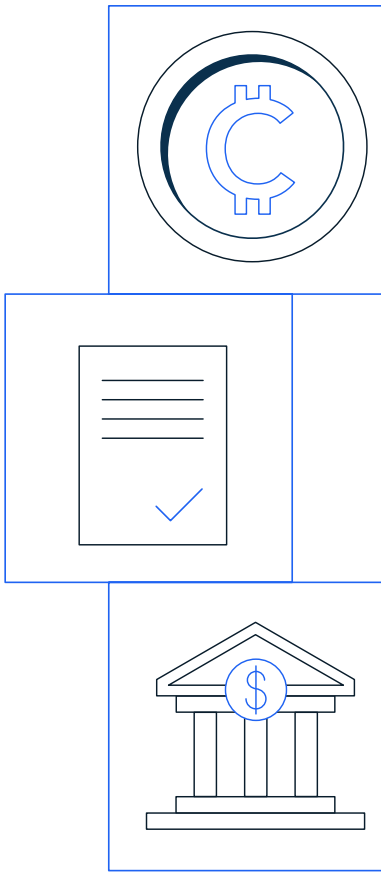
### From quarantine to competition

In the first few months of Donald Trump's second term, the administration launched a notable pivot in its regulatory posture toward crypto – one that departed from the more cautious tone of the preceding years. Rather than treating crypto as a source of systemic risk to be quarantined, the new stance emphasized strategic engagement, competitiveness, and modernization of financial infrastructure.

Key agency appointments further catalyzed this shift. The Trump administration reinstated several officials with fintech and crypto expertise into prominent roles – most notably at the OCC, which issued updated guidance supporting the permissibility of crypto custody, tokenized deposits, and even certain staking services by federally chartered banks. This was a clear signal: the administration was not just allowing crypto activity – it was looking to build a stable regulatory home for it.

For banks, the Trump administration's 2025 pivot offered an invitation – though not a free pass – to engage in crypto, provided they did so transparently, compliantly, and in dialogue with their regulators. After years of mixed signals, banks now have a path to step into the arena – with clearer guardrails and a potential partner at the supervisory table.

That said, frontline examiners may still maintain some level of cautious skepticism about risks that the crypto ecosystem presents. **Bank compliance teams will have to effectively articulate and counter this skepticism by clearly explaining that they understand the business and services offered, the risks inherent in those activities, and that they've built out a robust environment to control for those risks.**



## Working with regulators

Given this history of initial friction and ongoing skepticism from supervisors, what can banks do to collaborate more effectively with regulators as they expand into cryptocurrency initiatives? Let's explore five actionable best practices compliance professionals should consider, drawn from regulatory guidance and real-world examples.

### 1. Engage early and proactively

Don't wait for regulators to discover your crypto activities. Rather, **inform them at the outset.** Banking agencies have made clear they expect early notification and dialogue around any crypto-related plans. In fact, each federal regulator has established processes for banks to engage in "robust supervisory discussions" about proposed crypto ventures.

By consulting regulators in the planning phase, banks can address concerns up front and avoid unpleasant surprises late in the building phase. Early, proactive engagement also builds trust and gives regulators confidence that a bank is approaching crypto in a controlled, transparent way.

**2. Conduct thorough risk assessments**

Before launching any crypto product or partnership, banks should rigorously assess the risks, be prepared to show regulators they have documented these assessments, and demonstrate that these risks are controlled for. This may include areas such as the bank's existing exposure to crypto entities, or, depending on the products and services, areas like fraud or volatility risk. Regulators will expect to see that proper **controls**, **gates**, and **guardrails** are in place for any crypto activity.

Additionally, robust risk management starts with board and senior management oversight. Ensure your board is informed and approving of the crypto strategy, and that detailed policies and procedures have been developed alongside the risk assessment. Document the results of your risk assessments and the mitigants put in place (e.g. capital buffers for crypto exposures, enhanced monitoring of transactions, triggers for escalation, etc.). By presenting regulators with a thoughtful risk analysis, banks signal that they are not venturing into crypto recklessly – but rather in a manner consistent with safety and soundness expectations.

**3. Augmenting existing controls**

When launching crypto-related services, banks may feel tempted to build entirely new anti-money laundering (AML) frameworks from scratch. But creating standalone crypto compliance controls risks duplicating efforts, introducing inconsistencies with your existing program, and weakens the overall structure of your AML program.

For example, in one FDIC letter from mid-2023, a bank proposing to offer crypto custody services was explicitly cautioned that its plan to establish "a parallel transaction monitoring process" for crypto activities – separate from its core AML systems – could result in inconsistent oversight and gaps in suspicious activity reporting. The FDIC noted that "risk mitigation efforts must be coordinated within the bank's existing BSA/AML infrastructure" and warned against siloed compliance approaches that might undermine overall program effectiveness.

Instead, banks should **focus on extending and adapting their existing AML infrastructure.** There's no doubt that the crypto ecosystem introduces novel risks that may need to be controlled by novel tactics. However, institutions should endeavor to weave those novel tactics into their existing policies and procedures so as not to create fragmented programs.

This could mean integrating blockchain intelligence tools and checks into existing customer due diligence and enhanced due diligence procedures to fully assess the risks of crypto entities. Or, on a more granular level, this could mean ensuring that

specific transaction monitoring processes (e.g. escalation guidelines, timelines for closing alerts, quality assurance rates, etc.) also apply to blockchain intelligence tools used to perform ongoing monitoring of activity for on-chain transactions and alerts.

This approach ensures consistency, avoids internal silos, and allows compliance teams to operate within familiar frameworks — while still addressing new threats like blockchain obfuscation or peer-to-peer transfer risks. Regulators have made clear that AML compliance remains non-negotiable in crypto services, but they are more likely to support programs that demonstrate continuity with existing bank-wide controls.

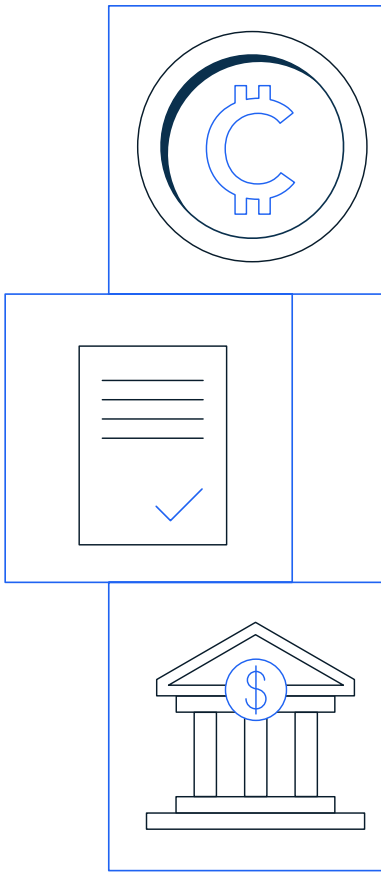
**4. Maintain open communication and documentation**

Fostering an ongoing dialogue with regulators is key to a smooth relationship. Crypto markets evolve rapidly; as your bank's strategy or partnerships change, **keep your regulators in the loop.** Regular check-ins or status updates can preempt regulatory concerns before they fester.

It is equally as important to document all communications and understandings with regulators. If a regulator requests additional safeguards or a pause on a certain activity, follow up in writing to confirm the bank's commitments or the conditions to be met for approval. This creates an audit trail and helps avoid misinterpretation.

It's also critical to seek clarity rather than operate in ambiguity. For example, some banks that received the FDIC's crypto-related letters in 2023 were left in limbo: told to pause activities, but never explicitly given the green light to resume. To avoid such dead ends, banks should politely press for clear guidance on what would satisfy regulators' concerns. For example, by asking: "What specific controls or data would give you comfort for us to proceed?"

Open, two-way communication, backed by thorough documentation, turns regulatory supervision into a collaborative process rather than an adversarial one.



**5. Embrace self-identification**

As banks build out crypto-related programs, the instinct may be to perfect every detail before bringing regulators into the conversation. But waiting too long to disclose internal challenges can erode trust and lead to regulatory skepticism. Agencies like the FDIC, OCC, and OFAC have repeatedly emphasized the value of self-identification — where institutions **proactively flag gaps, delays, or missteps in their own crypto-related activities before issues are discovered during examinations.**

For example, if your team discovers that a planned blockchain analytics integration is delayed or a key crypto custody control isn't functioning as expected, this finding should trigger immediate internal escalation and timely communication with your supervisory contact. Regulators are often more focused on how a bank responds

to problems than whether problems exist in the first place. Self-identified issues — particularly when accompanied by a clear remediation plan — demonstrate a mature risk culture and a willingness to take ownership. This builds credibility and can soften the tone of regulatory response.

## Conclusion: Collaboration is key

By adopting these best practices, banks can turn what has sometimes been a standoffish dynamic into a more constructive partnership. The goal is to show regulators that a bank is approaching crypto in a responsible, informed manner — and to give regulators comfort that the bank won't become the next headline for a crypto-related mishap.

Smoother collaboration is a win-win: banks gain clearer pathways to innovate, and regulators gain confidence that risks are being managed within the safety of the regulated system.

## About TRM Labs

TRM Labs provides blockchain analytics solutions to help law enforcement and national security agencies, financial institutions, and cryptocurrency businesses detect, investigate, and disrupt crypto-related fraud and financial crime. TRM's blockchain intelligence platform includes solutions to trace the source and destination of funds, identify illicit activity, build cases, and construct an operating picture of threats. TRM is trusted by leading agencies and businesses worldwide who rely on TRM to enable a safer, more secure crypto ecosystem. TRM is based in San Francisco, CA, and is hiring across engineering, product, sales, and data science.

To learn more, visit www.trmlabs.com