BOARD BRIEFING

Crypto, Payments & AML Risk

How digital assets and modern payments create financial-crime exposure — and the controls that keep an institution out of trouble

2026 | R. McConnell Group PLLC

00

What Your Board Needs to Know

Five things to understand about crypto, payments, and money-laundering risk

01	**New Rails**	Crypto platforms and embedded digital payments move money in new, faster ways.
02	**The AML Duty**	The Bank Secrecy Act requires a written, risk-based anti-money-laundering program.
03	**Three Lines of Defense**	The business owns risk; independent compliance oversees it; audit assures it.
04	**Core Controls**	KYC, transaction monitoring, enhanced due diligence, and suspicious-activity reporting.
05	**The Stakes**	Civil and criminal penalties, asset forfeiture, and personal exposure for directors.

01

The New Payment Rails

Crypto platforms and embedded digital payments are reshaping how value moves

CRYPTO PRODUCTS

— **Exchanges and apps.** Customers buy, sell, and hold tokens; the platform performs know-your-customer onboarding.

— **Crypto-linked payments.** Branded cards and crypto pay rails let users spend digital assets at merchants.

— **Wallets and DeFi.** Self-custody wallets, swaps, and lending move assets outside traditional intermediaries.

— **Earn and credit.** Interest-style and collateralized-lending products turn holdings into financial services.

DIGITAL PAYMENT CHANNELS

— **Embedded payments.** Pay features built into apps, marketplaces, and devices across many countries.

— **Stored value and prepaid.** Gift cards and prepaid access subject to controls such as the $10,000 per-person, per-day threshold for sellers of prepaid access and the $1,000 per-day value limit under the open-loop prepaid-program exemption (closed-loop sales of $2,000 or less are exempt).

— **Marketplaces.** Third-party sellers transact on a platform the operator does not fully control.

— **Card-linked and fixed accounts.** Offers, deposits, and new channels broaden the money-movement footprint.

02

Why These Rails Raise AML Risk

The same features that make digital payments convenient also attract launderers

Speed and Reach

Funds move across borders almost instantly and pseudonymously, compressing the time available to detect and stop illicit flows.

Third-Party Exposure

Marketplaces and partner sellers introduce parties the operator does not directly control, expanding the surface for abuse.

Stored Value

Prepaid and gift-card products can be loaded, transferred, and redeemed in ways that obscure the source and destination of funds.

Innovation Outpaces Controls

New products—digital wallets, tokens, DeFi—emerge faster than monitoring rules and regulatory guidance evolve.

03

The Legal and Regulatory Framework

Money movement is governed by overlapping financial-crime and payments laws

FINANCIAL-CRIME LAWS

— **Bank Secrecy Act.** Requires a written AML program, recordkeeping, and reporting of suspicious and large-currency activity.

— **AML / CFT / sanctions.** Obligations to screen customers and payments and to block dealings with sanctioned parties.

— **Enforcement reach.** Non-compliance can expose the company, its directors, and individual officers to liability.

PAYMENTS REGULATION

— **Tier 1 — core laws.** Payments, money-transmission, e-money, AML/CFT, sanctions, and currency-control laws aimed directly at financial activity.

— **Tier 2 — tangential laws.** Consumer-protection, privacy, and competition laws that still reach payment and billing practices.

— **Licensing uncertainty.** In crypto, the regulatory status of tokens is unsettled and licenses are not assured in every jurisdiction.

04

Managing the Risk: Three Lines of Defense

Regulators expect clearly separated roles for taking, overseeing, and assuring against risk

1

FIRST LINE

The Business

The people and units doing the work own and manage risk day to day—onboarding customers, running payments, following procedures.

2

SECOND LINE

Independent Risk

An independent BSA / compliance function sets policy, runs risk assessments, monitors the program, and reports to senior management.

3

THIRD LINE

Audit

Internal and external auditors independently test the program and give the board assurance that controls actually work.

WHY IT WORKS Separating who takes risk, who oversees it, and who assures it gives the board independent visibility and prevents any one function from grading its own work.

05

The Core AML Controls

A program is built to prevent, detect, and respond—turning legal duties into testable operations

1. **KYC / CDD**
   Verify identity and screen against sanctions, PEP, and watch lists at onboarding

2. **Transaction Monitoring**
   Automated systems flag unusual or structured activity for review

3. **Enhanced Due Diligence**
   Higher-risk customers and outliers get deeper, documented investigation

4. **SAR Filing**
   Confirmed suspicious activity is reported to the financial-intelligence unit

WRAPPED BY risk-based training tailored to each role, quality assurance, and independent testing on a risk-based cycle, generally every 12 to 18 months.

06

Risk Assessment and Monitoring

Programs must continuously re-rank risk and watch for regulatory change

STEP 1

Risk Assessment

Identify the most vulnerable products, channels, and jurisdictions

STEP 2

Tier and Prioritize

Score risks and rank regulatory developments by impact

STEP 3

Monitor

Track new and pending laws on a regular, scheduled cadence

STEP 4

Action Plans

Assign owners, mitigate, and report results to leadership

WHY IT MATTERS Regulators and prosecutors ask whether a program is well designed, adequately resourced, and works in practice—a static program fails all three.

07

What Is at Stake

AML failures carry financial, criminal, and reputational consequences

BEYOND THE FINES

— **Reputational harm.** AML weaknesses make headlines and erode customer and partner trust.

— **Business limits.** Compliance gaps can block new ventures, market entry, and partnerships.

— **Asset forfeiture.** The government may seize property involved in criminal violations.

— **Individual exposure.** Directors and officers can face personal liability.

STATUTORY PENALTIES

$25,000 — civil penalty per willful BSA violation (or the amount involved, up to $100,000, if greater)

$250,000 — fine for a willful violation (up to 5 years' imprisonment)

$500,000 — fine for a willful violation tied to other unlawful activity (pattern over $100,000 in 12 months; up to 10 years)

08

Board Implications

Where oversight of crypto, payments, and AML risk meets the board's role

Empower the Program

Confirm an independent BSA / compliance function—and a chief risk officer—with authority, resources, and a direct line to the board.

Demand Monitoring

Require ongoing monitoring of crypto and payments regulatory change, with risk assessments refreshed as products evolve.

Test the Controls

Insist on independent audits and quality assurance that confirm KYC, monitoring, and reporting actually work.

Document Engagement

Record the board's questions, the information it received, and the actions it required—engagement is itself a defense.