

INNOVATION WITHOUT CONTROLS

How Risks Materialize and Why Banks and Fintechs Are Facing Enforcement Actions

Sarah Beth Felix M.F.S.

President, Palmera Consulting

Co-Founder & Chief AML Officer, Acceleron Bank

PANAMÁ 2026 · ENFORCEMENT REVIEW, SEPT 2025 – AUG 2026

The total is falling. The target moved.

Global penalties declined for a second year - while the share aimed at crypto, payments and fintech climbed.

In 2025, crypto exchanges and money transmitters accounted for more than 90% of every AML dollar penalized in the United States. Securities firms and casinos were a rounding error.

\$15B

global AML, KYC and
sanctions penalties, 2023–
2025

\$927.5M

of US AML penalties in 2025
fell on crypto exchanges

\$228.8M

sanctions penalties in H1 2025
- up from \$3.7M a year earlier

\$275M

one OFAC penalty, against
a non-US company

Twenty-one US enforcement actions in twelve months. Six agencies. Half the targets were not US financial institutions - and some were not US companies at all.

PART ONE · SANCTIONS

When the sanctions control stops working

None of these firms lacked a program. Each had one that no longer matched the business it was protecting.

1 An upgrade switched three controls off at once

Three separate geo-blocking layers, undone by an IT release. No dual control on the change, and nobody noticed the OFAC alerts had stopped arriving — which OFAC said should itself have been the warning.

TradeStation - \$1.11M

2 Screening looked at names and nothing else

Iranian mailing addresses sitting in the core, country-level email domains, phone country codes, a VPN behind an unchanged device ID. Country-level programs are 75 years old; the name list was never the whole test.

Exodus - \$3.1M

3 Staff had the knowledge; nobody had the training

Emails referencing Iran, arriving from Iranian domains. A global manufacturer with no screening of employee correspondence — and prompt self-reporting and remediation visibly reduced the penalty.

Rice Lake Weighing - \$60,764

SANCTIONS LESSONS

- 1 **Knowledge is burden.**
Once it is known - an email, a test result - it is yours.
- 2 **Screen far beyond names.**
Countries, addresses, domains, phone codes, IPs, device IDs.
- 3 **Every change is a control event.**
Dual control on releases. Confirm alerts still arrive.
- 4 **Use the 2019 Framework.**
The roadmap and the mitigating factor. Start there.
- 5 **Disclose and cooperate.**
It halved one penalty this year - but is never promised.

PART ONE · SANCTIONS

Why this reaches you here

A US office is not the trigger. US dollars, US persons, US-origin goods and US counterparties are.

\$275M

An Indian company, penalized for Iran violations

More than every OFAC penalty issued in 2025 combined, and over five times all of 2024. Egregious, not self-disclosed. The finding was that red flags were ignored - no name match was ever required.

\$1.6M

One shipment, two sanctions programs at once

A single Venezuela contract pulled in a wholly-owned subsidiary of the state airline, plus an Iranian aircraft with Iranian crew. WMD proliferation and global terrorism programs, from one hurried job.

\$3.78M

A US person who had not lived in the US for years

Naturalized in the 1990s, resident abroad throughout the conduct, penalized for services alone - marketing, signing financial statements, approving staff. Check your board and executive rosters.

\$1.05M

A consultancy and its law firm both missed it

Invoicing routed through outside counsel for a sanctioned Russian bank. OFAC's principle is unambiguous: it is prohibited to do indirectly what one cannot do directly. Outside advice is not a defence.

PART TWO · AML

The fintech and crypto orders

Four AML actions where the partner, the processor or the platform was the risk the program never covered.

1 A crypto marketplace with no program at all

Four years operating before any AML program, three years without an AML officer, one independent audit in eight. Over 1,500 accounts opened from Iranian, Syrian, Cuban, Crimean and Sudanese IP addresses. **Paxful - \$3.5M · FinCEN**

2 A partner bank pointed the wrong monitoring at processors

Monitoring built for fintech activity one layer removed, aimed at unregulated payment-processor flows with entirely different typologies. The service agreement compelled little; the auditor found nothing. **CFSB - consent order · OCC**

3 Third-party banking that ran ahead of its controls

The order demands the AML officer hold full autonomy, independence and direct Board access. Third-party and correspondent business must be preceded by staffing, data and technology - not followed by it. **United Texas Bank - consent order · OCC**

4 A community bank exposed through its business customers

Unregulated processors, hard-money lenders and payroll fintechs reaching the bank through commercial accounts. Remediation spans every pillar, plus quality control over SAR and CTR output. **Covington County Bank - consent order · FDIC**

AML LESSONS

- Threats before risks.**
Threats + vulnerabilities = risk. Generic risk assessments miss.
- A clean audit is not a good audit.**
Check the auditor is actually qualified for your model.
- Your service agreement is a control.**
Vague MSAs leave the regulated partner holding the exposure.
- The AML officer is an executive.**
Stature, staffing, budget, direct Board access - not a title.
- CDD is not a silo.**
It must feed monitoring and alert dispositioning to work.

PART TWO · AML

The finding behind the finding

Strip out the typologies and the same four governance failures are left standing in almost every order.

1 An AML officer with a title and no power

Orders now spell out the standard: full autonomy, independence and responsibility. Meaningful decision-making authority. Adequate staffing and resources. Stature and direct reporting access to the Board. One order goes further and reads the role as an executive position.

United Texas Bank · First National Bank of Pasco

2 A board that cannot check the work

One order sets twenty-one minimum steps for board oversight and requires the Board to verify the effectiveness of each remediated area. Verify it how, when no director has AML experience? Someone has to define what effectiveness looks like and then teach it upward.

First National Bank of Pasco

3 Culture, written into the order

The regulator recorded limitations associated with the sponsorship of the project within the wider organization. That is a polite way of saying the real decision-makers did not care. However, your institution phrases its excuses internally, examiners read between the lines.

UBS

4 One officer, and staff nobody trained

A single AML officer offloading to an untrained compliance officer and analysts wearing several hats. Employees who did not know what to do with the monitoring reports they received. Two of them falsified reviews - one falsified four hundred documents.

Canaccord Genuity

Effectiveness is not a fluff word. Define your indicators, measure them, report them to the Board - and put the result in the minutes.

PART TWO · AML

When monitoring only looks like monitoring

Every one of these institutions had a system, a vendor and a validation. None of them had a program that found things.

1 A threshold that became alert suppression

The firm tested its cutoff score, found reportable activity sitting below it, and left the score where it was. A prior penalty in 2023 involved a cutoff of \$25,000. A risk-based threshold is not a get-out-of-jail score — it needs threat analysis behind it, not a validation.

Merrill Lynch — \$7.5M · SEC

2 Data that could not carry the program

Foreign wire data copied and massaged by hand, incomplete, and only fully accurate when paired with a second feed. The question almost nobody asks: does your system tell you when data is missing, or only when it is wrong?

UBS · Canaccord Genuity

3 Dispositioning by copy and paste

Alerts closed with pasted rationale. Cancelled trades left outside the monitoring scope. No written investigatory or dispositioning standards — and putting the words “not suspicious” in a procedure does not make them a standard.

FINRA AWCs · First National Bank of Pasco

4 Risk ratings frozen where they were set

High and higher-risk customers given eyes once every twelve months. Phone country codes, email domains and IP addresses treated as an alert but never allowed to move the customer's risk rating. Static ratings describe the customer you onboarded, not the one you have.

UBS

Model validation asks whether the system runs as designed. An effectiveness review asks whether it finds the dirty money. Choose the second.

PART TWO · AML

And it is not only the Americans

Banco Central do Brasil, May 2026. Same failures, different flag — and a regulator in this region saying it will do it again.

WHAT THE COMMITTEE FOUND

- US\$1.7bn** in virtual-asset FX operations, Oct 2020 – Sep 2021
- 15** corporate clients accounted for all of it
- 63% / 47%** of outbound FX transfers / of primary-market operations
- R\$16.2m** fine, for client qualification, records and AML control failures
- 2 years** barred from crypto FX in the over-the-counter market
- 3** administrators fined personally; one barred from the sector for five years

LESSONS LEARNED

- 1 Concentration is a threat, not a product line.**
When one activity is 63% of your cross-border flow, it is no longer a product - it is your risk profile, and it needs its own assessment.
- 2 Qualify the beneficiary, not only the client.**
The finding was inadequate qualification of the third parties benefiting from the operations. Your customer's customer is your exposure.
- 3 “The rules were not written yet” is not a defense.**
Brazil's virtual-asset framework arrived in November 2025. The conduct was punished under the AML law that already existed.
- 4 The real penalty was the license.**
Two years out of a market costs far more than the fine - and the supervisor said it can be imposed pre-emptively.
- 5 Atypical is not the same as proven.**
Operations were never reported to the FIU. You do not need certainty to file; you need the activity to be atypical.

Conduct in 2021. Decision in 2026. Whatever your institution is doing this quarter will be judged by a supervisor who has not read the memo you wrote to justify it.

TAKEAWAYS

If you remember five things

Not one of these needs a budget approval, a vendor, or permission from anybody outside your own building.

1

If you have knowledge, you have burden.

An employee email. A test result. A prior exam finding. Once it is known, it is yours.

2

Threats before risks.

Threats plus vulnerabilities equals risk. Monitoring built on a generic risk assessment misses.

3

Screen far beyond names.

Countries, addresses, email domains, phone codes, IPs, device IDs. Country programs are 75 years old.

4

A clean audit is not a good audit.

Tailor the testing to your threats — and check that the auditor is qualified for your model.

5

The AML officer is an executive.

Stature, staffing, budget and a direct line to the Board. Not a title, and not buried beneath the CCO.

Thank you!
Questions? SB@PalmeraConsulting.com or on LinkedIn #ifollowdirtymoney