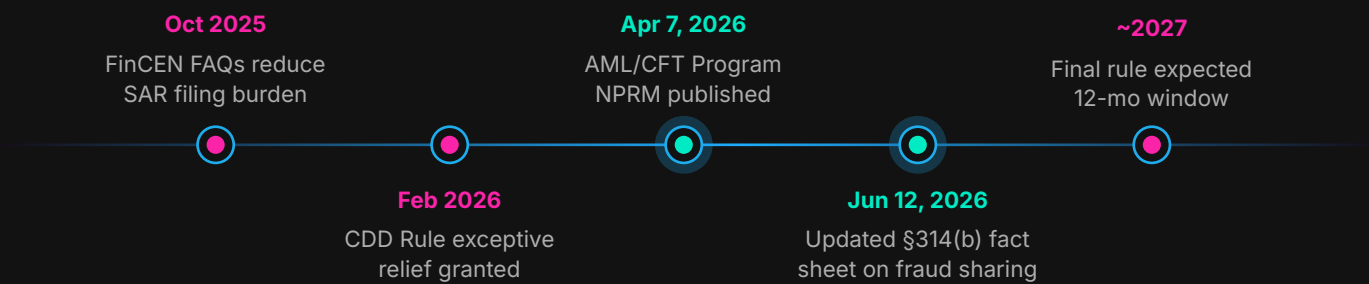
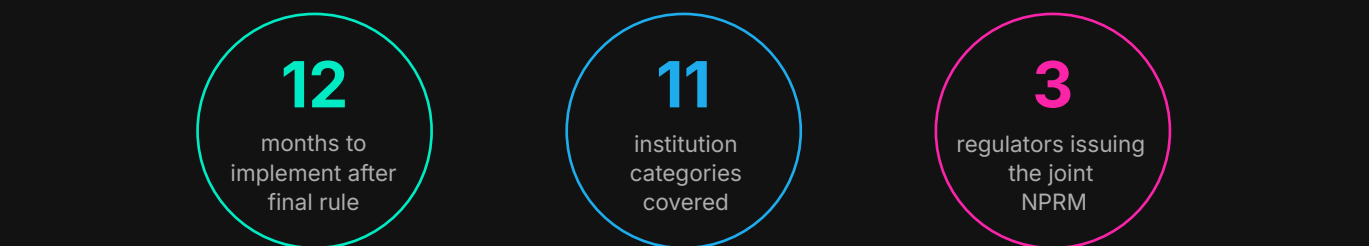


# FinCEN's Dual Mandate: Modernize AML Programs and Expand Information Sharing



## PART 1 · FINCEN NPRM — AML/CFT PROGRAM MODERNIZATION (APR 7, 2026)

**The shift in plain terms:** FinCEN is replacing a decades-old, process-driven "check-the-box" model with an outcomes-based, risk-tiered framework. Success is measured by whether a program actually detects and disrupts illicit finance — not by the volume of paperwork. The NPRM supersedes the July 2024 proposal and sets a 12-month implementation window after finalization.



### Four Core Program Pillars (codified)

**1**  
**Risk-Based Internal Controls**  

Policies must identify, assess, and document ML/TF risks, incorporate FinCEN's national priorities, and update promptly as risk profile changes.

**2**  
**Independent Testing**  

Testing must evaluate whether the program is effective, not merely whether it exists — frequency and scope tailored to actual risk.

**3**  
**U.S.-Based AML/CFT Officer**  

Must be physically located in the U.S. and accessible to regulators. Support staff may remain offshore; SAR sharing abroad stays restricted.

**4**  
**Ongoing Employee Training**  

Standardized across institution types, but frequency and content are tailored by role and risk profile — not uniform across headcount.

### The Old Model vs. The New Model

| BEFORE                                                                          | AFTER                                                                                                                                                     |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enforcement scrutinized every technical or process gap, regardless of severity. | <b>Two-tier enforcement</b> — establishment separated from implementation; action reserved for significant or systemic failures.                          |
| Program success was measured by SAR filing volume.                              | <b>Effectiveness over volume</b> — programs judged on useful outcomes for law enforcement; fewer resources justified for lower-risk segments, in writing. |

**REGTECH SIGNAL**  
The NPRM explicitly lists use of innovative tools such as AI as a factor FinCEN may weigh before taking enforcement action — elevating technology adoption from discretionary to strategically protective.

**AI and Innovation — Now a Mitigating Factor**

**Key Implications for Financial Institutions**

☒ Gap-assess risk assessment methodology and documentation now — before the final rule

☒ Confirm the AML/CFT Officer is U.S.-based and accessible to regulators

☒ Build evidential frameworks that demonstrate program effectiveness, not just existence

☒ Formalize alignment of internal controls with FinCEN's national AML/CFT priorities

☒ Review governance: board/senior management approval of the written program is required

☒ Treat AI/technology adoption as a strategic compliance asset, not a back-office cost

☒ Re-evaluate resource allocation — justify lower spend on low-risk segments in writing

## PART 2 · FINCEN §314(B) UPDATED FACT SHEET (JUN 12, 2026)

**The core clarification:** Section 314(b) was always a fraud tool — FinCEN has now made this explicit. The June 2026 update removes years of institutional hesitation about sharing fraud cases, permits real-time sharing, and replaces the December 2020 fact sheet in its entirety. It's part of the White House Task Force to Eliminate Fraud.

**Real-Time Sharing Permitted**  
No restriction on method or timing — information may be shared as activity is occurring. Sharing isn't limited to customer or transaction overlaps with the receiving institution; context-free intelligence sharing is now permissible.

**Fraud Is Explicitly In Scope**  
Covers mail, wire, bank, securities, and computer fraud, romance scams, pig butchering, and mule account activity. Institutions need only suspect fraud — not identify laundered proceeds — to invoke the safe harbor.

**What Can Be Shared**  
Transaction records, entity relationship data, monitoring alerts, adverse media, device fingerprints, IP addresses, video surveillance footage, and fraud indicators.

**Association Operators and Non-FI Entities**  
A non-financial institution may form and operate a 314(b) association, opening the door for RegTech vendors to serve as network orchestrators. Foreign sharing is limited — it doesn't benefit from the safe harbor unless the foreign entity qualifies as a FinCEN-regulated FI. Joint SARs remain available to institutions collaborating through 314(b).

**Operational Requirements**  
Register (and renew annually) through the FinCEN FI Portal — expired registration means no safe harbor. Verify the receiving institution is a registered participant before sharing, and safeguard shared data for AML/CFT, account decisions, or BSA compliance only. Eligible: banks, MSBs, broker-dealers, mutual funds, insurance and loan/finance companies, and associations.