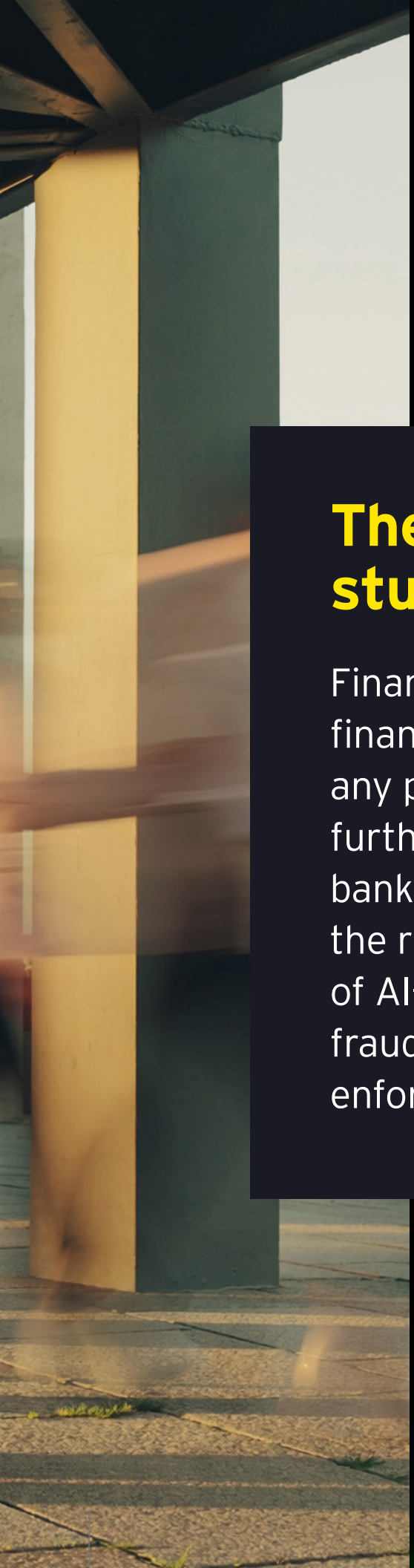
When criminals move at machine speed, FinCrime operating models must adapt

The case for managed services

The better the question. The better the answer.
The better the world works.

Shape the future with confidence



The cost of staying stuck in the past

Financial institutions are investing more in financial crime (FinCrime) compliance than at any point in history, yet they continue to fall further behind. Criminals innovate faster than banks can respond; real-time payment rails, the rise of digital assets and the emergence of AI-driven threats have amplified both fraud and money laundering risks. Global enforcement actions remain unrelenting.

More effort ≠ better outcomes

$10b AML penalties globally 2025

In 2025 alone, anti-money laundering (AML) penalties exceeded $10 billion, with US regulators driving much of the enforcement.[1] At the same time, traditional alert-centric operating models are failing, delivering up to 95% false-positive rates,[2] overwhelming investigative teams and diverting the expertise required to identify true risk.

1 "Global AML Enforcement Surge: Record Fines Hit HSBC, Binance, Revolut in 2025," *AML Network website*, https://amlnetwork.org/aml-news/global-aml-enforcement-surge-record-fines-hit-hsbc-binance-revolut-in-2025/, accessed March 27, 2026.

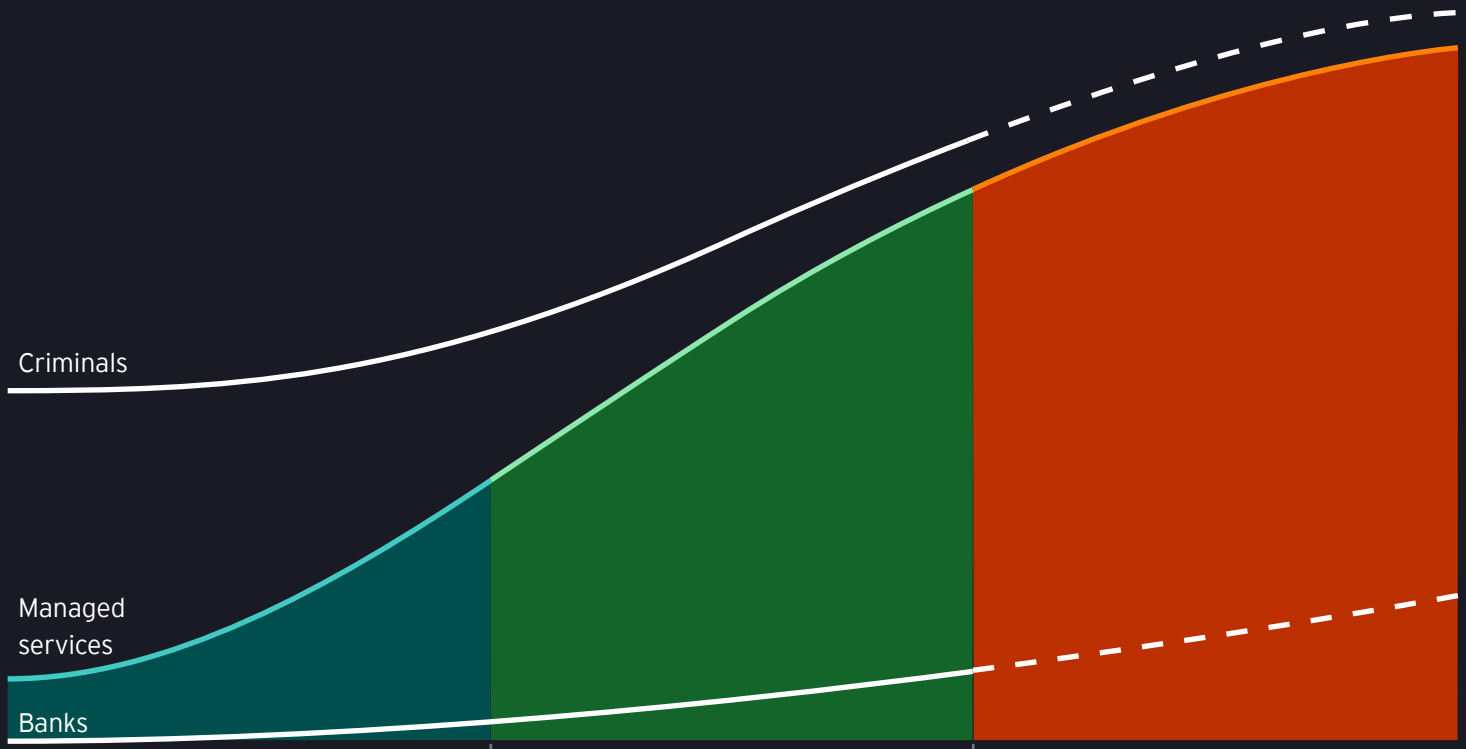
2 "Silencing the Noise: Effective Strategies for Reducing False Positives in Transaction Monitoring," NICE Actimize, https://resources.niceactimize.com/wp-content/uploads/2024/11/aml-reducing-false-positives-in-transaction-monitoring-brochure.pdf, November 2024.

The shift to real-time payments has raised the stakes further

Volumes and values on networks such as RTP and FedNow have surged,[3] while authorized push payment fraud, mule activity and synthetic identity schemes scale at machine speed. Legacy batch-processed FinCrime programs simply cannot match this velocity. Meanwhile, the human capital model underpinning most in-house programs is showing signs of stress: Repetitive, high-volume, Level 1 (L1) work drives chronic turnover, leaving persistent capacity gaps and degraded control quality.[4]

The conclusion is unavoidable: Running FinCrime operations entirely in-house has become a strategic liability. It yields rising costs, inconsistent outcomes and operational fragility at the exact moment when criminals scale and real-time payments eliminate any margin for delay or error.

For financial services leaders, the choice is no longer between outsourcing and building in-house; it is between a model that can scale with modern FinCrime and one that cannot. The institutions that move first to a managed services model will reclaim investigative capacity, reduce risk, meet rising regulatory expectations and build resilience for the next wave of real-time payment expansion and geopolitical volatility. Those that wait will face rising costs, widening gaps and increasing enforcement exposure.



Today

Pilot AI-led alert triage, vendor-managed investigations, data quality uplift, governance and regulator engagement

Near future

Scaled managed services that embed cognitive investigators and automate quality assurance and reporting through agentic processes

Beyond

Autonomous compliance ecosystems that are orchestrated using AI marketplaces, predictive risk sensing, geopolitical scenarios and continuous regulatory assurance

[3] "RTP's Instant Payment Volume Nearly Doubled in 2024," *PaymentsJournal website*, www.paymentsjournal.com/rtps-instant-payment-volume-nearly-doubled-in-2024/, January 13, 2025.

[4] "How to increase financial crime analyst capacity without increasing headcount or burnout," *WorkFusion website,* www.workfusion.com/blog/how-to-increase-financial-crime-analyst-capacity-without-increasing-headcount-or-burnout/, August 24, 2023.

The harsh reality: in-house models are no longer sustainable

While institutions continue to expand their FinCrime budgets, the operational foundations of in-house programs are weakening in ways that incremental investment cannot fix. The core issue is not simply rising volume or regulatory pressure: The traditional, internally staffed model is structurally mismatched to the speed, scale and complexity of today's FinCrime landscape.

Despite sizable compliance spend, even global banks with significant resources continue to fall short of regulatory expectations. Record high settlements in recent years underscores that conventional internal programs, even when mature and well resourced, are struggling to demonstrate sustained effectiveness under modern supervisory scrutiny. This reflects a broader trend: Investments increasingly flow into labor-intensive processes rather than driving meaningful improvements in detection or control strength, creating a trajectory where programs grow costlier without becoming more capable. With a shortage of qualified talent increasing the cost of labor, fully staffing an operation is turning into a challenge that can't be conquered by any but the largest institutions.

A major driver of this inefficiency is the fragility of the human capital model underpinning most in-house operations. Analysts shoulder repetitive, high-volume investigative work, driven largely by noise rather than risk. As a result, predictable L1 attrition near the 12-month mark creates chronic gaps and forces institutions into continuous cycles of hiring and retraining.[5] This instability is compounded by industry-wide monthly separation rates

Why in-house models break under pressure

Volume and speed

- Rising transaction volume
- Real-time payments
- Faster criminal adaptation

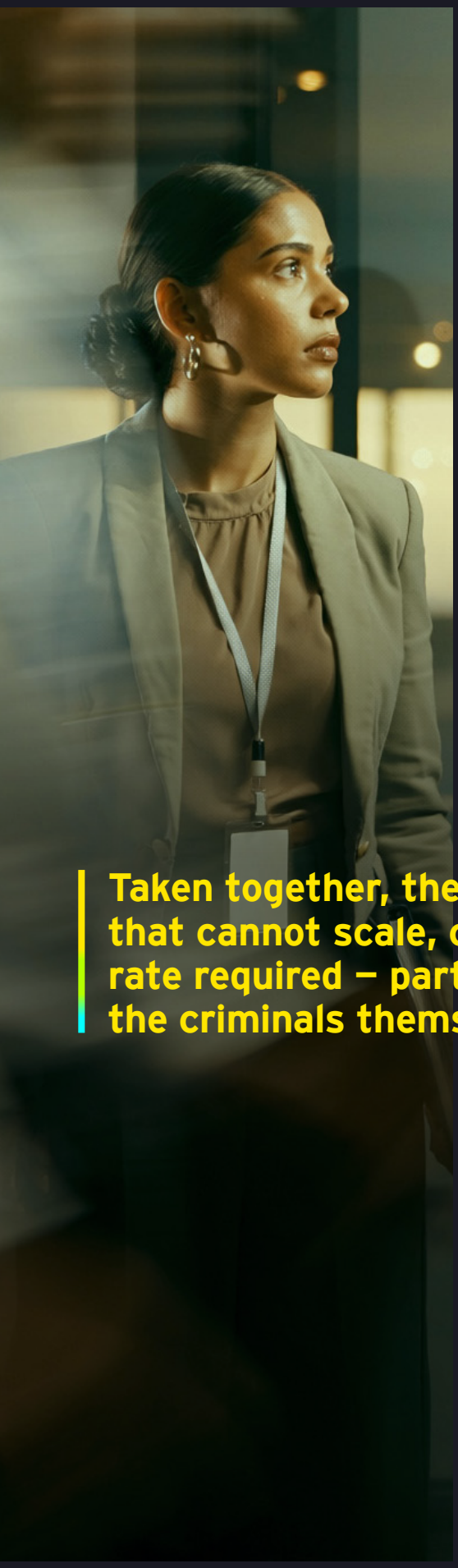
Operating model limits

- Fixed headcount
- Manual workflows
- Alert overload/ false positives

Outcomes

- Burnout and attrition
- Slower response times
- Inconsistent quality
- Regulatory gap

[5] Ibid.



of 2% to 3%, which disproportionately affect specialized functions that depend on retained expertise and continuity. The end state is a fixed-capacity operation that cannot flex when payment volumes surge, typologies evolve or regulatory expectations tighten.

Complicating this further is the fact that traditional alert-centric monitoring systems are fundamentally misaligned with today's threat velocity. Many banks still operate with as much as 95% false-positive rates.[6] These legacy rules engines generate overwhelming queues that divert investigator attention toward low-value activity and bury genuinely suspicious behavior. In a real-time payments world where criminals exploit machine speed movement, manual, human-dependent workflows cannot be optimized fast enough to keep pace.

At the same time, regulatory expectations are expanding faster than internal teams can adapt. Supervisors and regulators globally are formalizing what robust, risk-based AML and countering the financing of terrorism (CFT) programs must demonstrate: stronger governance, rigorous documentation and more dynamic responsiveness to emerging risks.[7,8] Even where outsourcing is allowed, frameworks from bodies such as the European Banking Authority (EBA) and Financial Conduct Authority (FCA) impose strict expectations around oversight and auditability, effectively raising the baseline for what constitutes an "effective program" beyond what most individual institutions can internally sustain.[9]

Taken together, these forces reveal an in-house paradigm that cannot scale, cannot stabilize and cannot evolve at the rate required — particularly to match the speed with which the criminals themselves are scaling.

6 "Silencing the Noise: Effective Strategies for Reducing False Positives in Transaction Monitoring," NICE Actimize, https://resources.niceactimize.com/wp-content/uploads/2024/11/aml-reducing-false-positives-in-transaction-monitoring-brochure.pdf, November 2024.

7 "Anti-Money Laundering and Countering the Financing of Terrorism Programs," Federal Register, https://www.federalregister.gov/documents/2024/07/03/2024-14414/anti-money-laundering-and-countering-the-financing-of-terrorism-programs, July 3, 2024.

8 "FinCEN Issues Proposed Rule Requiring Financial Institutions to Maintain 'Effective, Risk-Based' AML Programs: Six Things to Know," *Covington & Burling LLP website*, https://www.cov.com/news-and-insights/insights/2024/07/fincen-issues-proposed-rule-requiring-financial-institutions-to-maintain-effective-risk-based-aml-programs-six-things-to-know, July 3, 2024.

9 "Guidelines on outsourcing arrangements," European Banking Authority, https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-outsourcing-arrangements, revised 2019 (current).

Criminals scaled faster than banks could respond

FinCrime as a service

FinCrime threat actors have rapidly industrialized their operations, adopting automation, AI and cross-border networks at a pace that has far outstripped banks' ability to adapt. Synthetic identity fraud and deepfake-enabled onboarding have surged, with synthetic ID cases rising 60% year over year in 2024,[10] prompting the Financial Crimes Enforcement Network (FinCEN) to issue a formal alert on deepfake misuse.[11] Analysts now expect mule networks and synthetic IDs to remain among the most persistent and scalable threats through 2026.[12]

At the same time, the post-2022 sanctions wave created historically large designation volumes, heightening complexity for screening and counterparty risk management across global networks. The Office of Foreign Assets Control (OFAC) continues to expand determinations, such as those updated on June 12, 2024, requiring banks to adjust controls in near-real time to remain compliant.

These pressures collide with the rise of real-time payments. RTP transaction value nearly doubled to $246 billion in 2024, exceeding one million payments per day, while FedNow participation and volume grew sharply into 2025.[13] Regulators are now scrutinizing instant payment fraud and considering confirmation of payee controls as criminals increasingly exploit the speed and irreversibility of these rails.

What this means for FinCrime operations is that criminal networks are now operating at machine speed, across borders and with AI-enabled sophistication. Batch-based in-house FinCrime programs simply cannot match this challenge.

> **Criminal networks are now operating at machine speed, across borders and with AI-enabled sophistication.**

[10] "'Synthetic fraud' reaches record levels," *Experian website*, https://www.experianplc.com/newsroom/press-releases/2025/-synthetic-fraud--reaches-record-levels, March 18, 2024.

[11] "FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions," FinCEN Alert, https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf, November 13, 2024.

[12] "Synthetics, Mule Accounts Will Still Pose Threats in 2024," *BankInfoSecurity website*, www.bankinfosecurity.com/synthetics-mule-accounts-to-continue-to-pose-threat-in-2024-a-23913, December 18, 2023.

[13] "RTP's Instant Payment Volume Nearly Doubled in 2024," *PaymentsJournal website*, www.paymentsjournal.com/rtps-instant-payment-volume-nearly-doubled-in-2024/, January 13, 2025.

Why a managed services model is the only one built for what's next

The challenge facing financial institutions is no longer one of effort or intent; it's one of operating model fit. FinCrime has become a high-velocity, data-intensive, always-on risk. Yet most banks still attempt to manage it with static teams, siloed tools and institution-specific processes. Managed services succeed where in-house models struggle because they are structurally designed for scale, adaptability and sustained effectiveness.

The value of a managed services model

In-house	Managed services
Fixed capacity	Elastic capacity
Siloed intelligence	Pooled intelligence
Manual tuning	Embedded technology
Fragmented processes	Standardized workflows
Static teams	Redeployed teams

Built for scale, not headcount: Managed services replace fixed, labor-heavy cost structures with elastic capacity. Instead of hiring ahead of demand or falling behind during volume spikes, institutions gain access to pooled investigative resources that scale up or down with alerts, onboarding volumes, sanctions waves or geopolitical shocks. This shift from fixed to variable cost is not just cheaper, it's also operationally safer in an environment where volatility is the norm.

Pooled intelligence beats isolated learning: No single institution sees enough activity to fully map today's typologies. Managed services providers operate across clients, products and geographies, enabling earlier pattern recognition and faster control refinement. That pooled exposure translates into sharper detection logic, better investigator judgment and more defensible outcomes, exactly what regulators now emphasize under "effectiveness" standards.

Modernization without multiyear transformation risk: Technology refresh has become table stakes, but full platform replacements are slow, expensive and disruptive. Managed services embed modern tooling, automation, machine-assisted triage, dynamic segmentation and continuous tuning into day-to-day operations without forcing banks to run parallel transformation programs. For example, a regional bank facing rising AML alert volumes adopts a managed service that layers automation, AI-assisted triage and continuous tuning on top of its existing platform, cutting false positives and improving investigator throughput in weeks, without a costly core replacement.

The result is faster impact on false positives, throughput and quality, without accumulating new tech debt.

Managed services models institutionalize what many banks struggle to sustain: They standardize workflows, implement instrumented quality assurance, facilitate documented decisioning and provide audit-ready evidence. These controls are not after-the-fact overlays; they are embedded into production. That consistency improves outcomes, reduces rework and strengthens defensibility under regulatory scrutiny, particularly in outsourced permitted frameworks that demand transparency and oversight.

Focus internal talent where it matters most: Perhaps most importantly, managed services allow banks to redeploy scarce internal expertise. Risk ownership, program governance, model risk management, policy setting and regulator engagement remain firmly in-house, where judgment and accountability belong. Execution-heavy, repeatable work moves to a model optimized to deliver it at scale and with discipline.

The myth of control: Managed services are suited for mission critical operations. In practice, effective managed services follow a hybrid target operating model that balances scale with control. This structure strengthens control by embedding standardized processes, consistent quality and regulator-ready transparency into day-to-day operations.

Managed services are not only a tactical cost play but also a strategic response to an environment where criminals scale continuously, regulators demand measurable effectiveness, and standing still is the most expensive option of all.

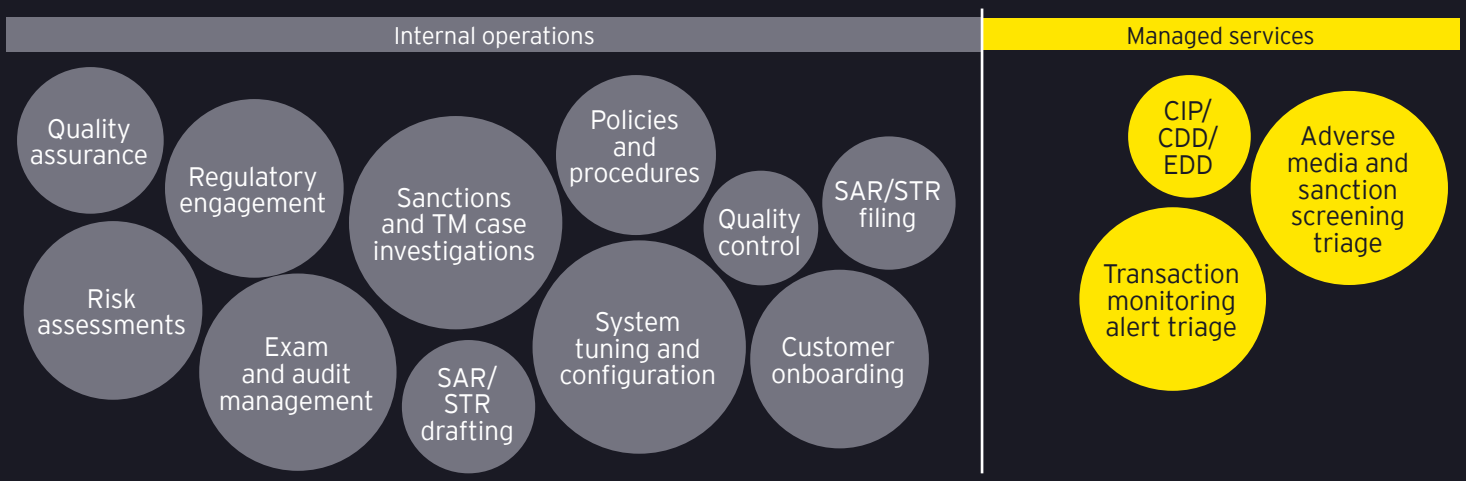
The economics complete the case

While the business case for managed services is compelling to counter the industrialization of FinCrime, the economics can't be dismissed. Traditional in-house FinCrime operations lock institutions into high fixed costs, including permanent headcount, overtime, attrition churn and parallel remediation spend. Managed services reset that equation by aligning cost, capacity and performance to actual risk and demand.

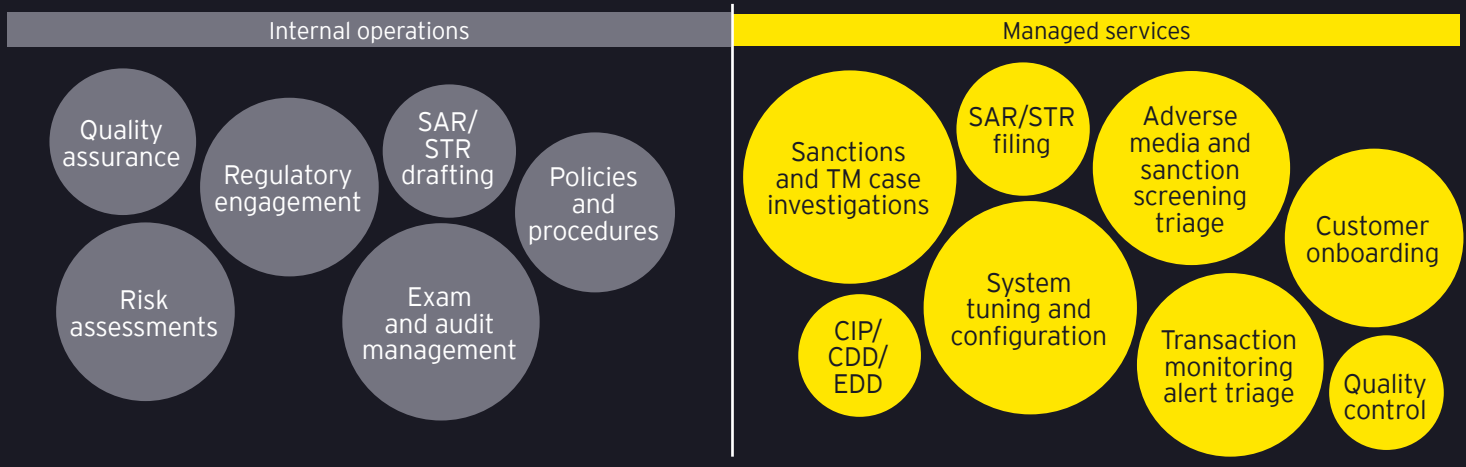
At scale, managed services models shift FinCrime from a fixed overhead to a variable operating expense. Standardized processes, global delivery and automation enable materially lower run rate costs than fully internal teams, while absorbing volatility that would otherwise require overstaffing or emergency hiring. Importantly, savings are not achieved by reducing controls but by eliminating wasted efforts, most notably the labor consumed by excessive false positives and rework through process re-engineering and the implementation of AI and other innovative technologies.

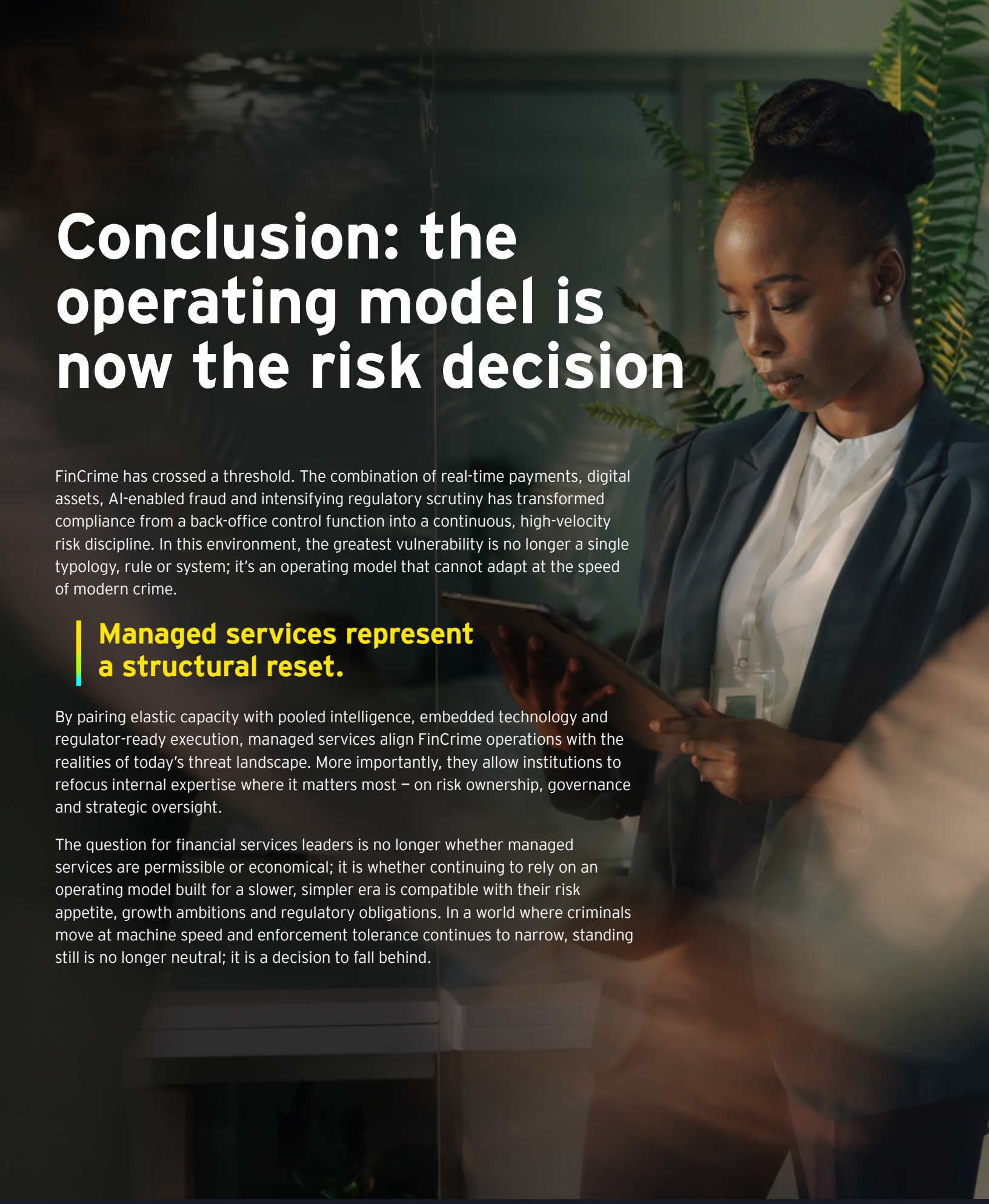
The economic upside extends beyond direct cost reduction. Improved detection precision, embedded quality assurance and consistent documentation reduce the likelihood and severity of exam findings, remediation programs and enforcement actions, often the largest unbudgeted costs in compliance. At the same time, elastic capacity enables faster product launches, smoother onboarding and rapid response to sanctions or fraud surges without destabilizing the core program. In aggregate, managed services deliver a compounding return: lower unit costs, higher control effectiveness, reduced regulatory downside and greater strategic flexibility.

In-house control



Balanced control





Conclusion: the operating model is now the risk decision

FinCrime has crossed a threshold. The combination of real-time payments, digital assets, AI-enabled fraud and intensifying regulatory scrutiny has transformed compliance from a back-office control function into a continuous, high-velocity risk discipline. In this environment, the greatest vulnerability is no longer a single typology, rule or system; it's an operating model that cannot adapt at the speed of modern crime.

Managed services represent a structural reset.

By pairing elastic capacity with pooled intelligence, embedded technology and regulator-ready execution, managed services align FinCrime operations with the realities of today's threat landscape. More importantly, they allow institutions to refocus internal expertise where it matters most — on risk ownership, governance and strategic oversight.

The question for financial services leaders is no longer whether managed services are permissible or economical; it is whether continuing to rely on an operating model built for a slower, simpler era is compatible with their risk appetite, growth ambitions and regulatory obligations. In a world where criminals move at machine speed and enforcement tolerance continues to narrow, standing still is no longer neutral; it is a decision to fall behind.

Authors

Tom Scazzafavo
EY Global Financial Crimes
Managed Services Leader

Carl Case
EY US Financial Crimes
Compliance Technology
Consulting Leader

Laurie Hollingworth
EY Americas Managed
Services Leader

Doug Stevenson
Director
Ernst & Young LLP

Allie Thacker
Senior Manager
Ernst & Young LLP

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

US SCORE no. 30753-261US
2512-10881-CS
ED None

ey.com