Fighting market abuse in the age of AI: Five strategic shifts every financial services executive must address

Received (in revised form): 3rd February, 2026

Chris DeNigris
Director of Product Marketing, NICE Actimize, USA

Chris DeNigris

NICE Actimize,
Saint Johns, FL,
USA

E-mail: chris.denigris@nice.com

Journal of Financial Compliance
Vol. 9, No. 4 2026, pp. 380–391
© Henry Stewart Publications
2398-8061 (2026)

Journal of Financial Compliance is included in **The Business & Management Collection**

Chris DeNigris *is the Director of Product Marketing for the Compliance line of business at NICE Actimize. He is responsible for building marketing programmes that drive pipeline, accelerate revenue and enable sales teams within the financial services vertical. He leverages over 20 years of experience in financial technology to translate complex products into clear market messaging. Prior to joining NICE Actimize, he was a Global Director of Product Marketing at FIS Global.*

Abstract

Market abuse has entered a new era. What was once episodic, localised and largely detectable is now growing in frequency and magnitude, cross-border and increasingly difficult to detect. Insider trading, spoofing and manipulation no longer necessarily occur within a single asset class, venue or communication channel. They can unfold across markets, platforms and jurisdictions. Technology has accelerated this shift. Algorithmic trading compresses reaction times to milliseconds. Digital assets trade 24/7 across fragmented venues. Social media and encrypted messaging enable rapid coordination outside traditional surveillance perimeters. Meanwhile, regulators are raising expectations, not lowering them, using advanced analytics of their own and imposing record-breaking penalties for failures in supervision, recordkeeping and detection. For senior executives, the implication is clear: market abuse has evolved beyond a traditional compliance issue. It is a strategic risk that tests the resilience of a firm's governance, data architecture, operating model and culture. As markets accelerate, AI is no longer optional. It has become the foundation of effective surveillance, while simultaneously introducing new governance, explainability and accountability expectations from regulators. This paper explores five structural trends redefining market abuse risk and outlines the decisions leaders must make to adopt AI-driven surveillance in a way that is defensible, scalable and aligned with regulatory expectations. This article is also included in ***The Business & Management Collection*** *which can be accessed at https://hstalks.com/business/.*

Keywords: Market abuse, artificial intelligence (AI), market surveillance, financial compliance, regulatory enforcement, cross-market manipulation, off-channel communications, crypto assets, natural language processing (NLP), anomaly detection

DOI: 10.69554/TKFJ7658

TREND #1: REGULATORY ENFORCEMENT IS BECOMING SYSTEMIC — AND LESS FORGIVING

Global enforcement activity has reached historic levels (see Figure 1), but the more important shift is not the size of the fines, it is *how* regulators are enforcing.

In North America, enforcement penalties surged to US$25.3bn in 2024,[1] nearly triple the prior year.[2] The US Securities and Exchange Commission (SEC) brought more than 500 enforcement cases[3] related to insider trading and market manipulation, underscoring that selective deregulation in areas such as crypto or Environmental, Social and Governance (ESG) does not

Recent Enforcement Cases Across Regions

Region	Firm	Infraction	Fine
	Global Bank	Treasury securities and futures manipulation	US$35M
	Oil & Gas Comp.	Gasoline price manipulation (derivatives)	US$48M
	Major Supplier	Coordinated trades across physical & derivative markets	US$55M
	Bank	Electricity futures manipulation	A$ 4.995M

Figure 1 Examples of regulatory actions
Sources:[4,5,6] (see footnotes)

Figure 2 How regulators evaluate market abuse programmes today

translate into reduced scrutiny of core market integrity obligations.

During the same period, the UK's Financial Conduct Authority *tripled fines year-over-year to £176m,*[7] supported by expanded use of data analytics and a renewed focus on senior manager accountability. Across the European Union (EU), MAR 2.0 and updated European Securities and Markets Authority (ESMA) guidance on digital communications are closing surveillance gaps by requiring firms to monitor previously untracked channels (such as chat apps, social media and collaboration platforms) and detect more subtle or complex forms of market abuse.

Across Asia–Pacific, regulators are moving beyond reactive, outcome-based reviews and into programmatic inspections, scrutinising the inner workings of surveillance programmes, from governance and design to testing and implementation. This trend is mirrored globally both in Europe and in the US, where the SEC and Financial Industry Regulatory Authority (FINRA) are increasingly focusing on programme design and control effectiveness rather than just flagged trades. In Canada and parts of the Middle East, regulators are similarly examining the robustness of monitoring frameworks, signalling a worldwide shift towards proactive, structurally focused oversight.

Executive Takeaway

Regulatory enforcement has evolved from identifying isolated control failures to assessing whether firms have built structurally sound, AI-enabled surveillance programmes capable of detecting modern market abuse by design (see Figure 2). Regulators are increasingly focused on surveillance architecture, model governance, cross-market visibility and management accountability, not just isolated outcomes.

At the same time, scrutiny is intensifying rather than plateauing. Firms that fail to integrate technology, analytics and organisational culture into a unified surveillance strategy face escalating financial, operational and reputational risk. In this environment, complacency is no longer a passive exposure but an active liability. Sustainable compliance now requires integrated, real-time monitoring embedded across products, channels and regions.

TREND #2: OFF-CHANNEL COMMUNICATIONS ARE NO LONGER TACTICAL, THEY ARE STRATEGIC

Off-channel communications (WhatsApp, Signal, WeChat, personal email, collaboration tools and social platforms) now sit at the centre of coordination, intent and execution in financial markets. US regulators alone have imposed *more than US$3.5bn in penalties*[8] for recordkeeping and supervision failures tied to unapproved communications.

Similarly, in its latest report on off-channel communications, the Financial Conduct Authority (FCA) found breaches in 8 of 11 firms examined,[9] concentrated among larger institutions with complex operating models.

Around the globe, watchdogs are making it crystal clear: if it is business-related, it must be recorded, regardless of the platform. The takeaway? Geography changes the fine print, but the message is universal: unmonitored off-channel business communications are a compliance landmine (see Figure 3).

Executive takeaway

The core surveillance challenge facing financial institutions is not off-channel communications themselves but architectural fragmentation. Without a unified, end-to-end view of communications across voice, messaging, email, collaboration tools and emerging platforms, firms cannot reliably detect intent, collusion or evolving forms of market abuse. Fragmented systems create blind spots that no policy prohibition can fully address.

Senior leaders therefore face a strategic choice: prohibit off-channel communications

Regulators worldwide are tightening controls on unmonitored business communications across all channels.

Region	Key regulatory requirements	Enforcement actions/activities
US SEC, CFTC, FINRA	• Preserve all business communications • Capture off-channel messages • Non-rewritable, non-erasable storage	US$3.5B+ in fines US$393M to 26 firms for WhatsApp lapses US$6.5M fine for unapproved messaging
UK FCA	• Retain all business communications • Ban unmonitored channels • Prohibit misleading info/insider dealing	650 illegal promotions removed Influencers arrested Criminal offences under FSMA
EU ESMA, BaFin, AMF	• MAR: Ban insider trading and market manipulation • Record off-channel communications • Monitor social media	Strict compliance warnings Updated guidance on social media monitoring
Singapore MAS	• Monitor social media and chat apps • Control communication tools	Close regulatory scrutiny
Australia ASIC	• Record client trader communications • Strengthen retention across all channels	Criminal prosecutions
Hong Kong SFC	• Capture client orders and calls • Capture off-channel messages	Ongoing fines and investigations

Figure 3 Global crackdown on off-channel communications
Sources:[10,11,12,13,14] (see footnotes below)

Figure 4 Why off-channel bans fail

and accept growing enforcement risk as usage persists beyond visibility; tolerate off-channel use and accept material surveillance gaps; or enable compliant communications through systematic capture, archiving and monitoring.

Only the controlled enablement approach is sustainable. High-net-worth clients, younger traders and globally distributed teams increasingly rely on informal, mobile or encrypted channels, making outright prohibition operationally unrealistic and regulatorily insufficient (see Figure 4).

Sustainable compliance now requires an integrated, AI-driven surveillance strategy that enables communication while ensuring full regulatory coverage. This includes omni-channel capture across voice, messaging, email and collaboration platforms; consolidation of all records into a single regulatory archive; and correlation of communications with trading activity to identify intent and suspicious behaviour.

Advanced AI and natural language processing (NLP) analytics are essential to process unstructured data at scale, reduce false positives and surface true risk. Firms must also establish mandatory training, clear escalation paths and leadership accountability for misuse, while ensuring encrypted or ephemeral communications are captured and analysed in line with regulatory expectations. For global operations, surveillance must extend across languages, platforms and regions, linking communications directly to trading behaviour.

Holistic, AI-enabled surveillance architectures ensure no channel is left unmonitored. This empowers employees to communicate effectively while closing structural compliance gaps and positioning firms ahead of intensifying regulatory scrutiny.

TREND #3: CRYPTO IS DRIVING A RETHINK OF SURVEILLANCE ACROSS ALL ASSETS

With a global market capitalisation approaching US$4tn[15] and accelerating institutional adoption, crypto is no longer peripheral. Exchange-traded funds (ETFs) and decentralised finance (DeFi) platforms are integrating digital assets into mainstream portfolios, while regulatory frameworks such as Markets in Crypto-Assets Regulation (MiCA) in the EU and Market Abuse Rules for Crypto (MARC) in the UK formalise oversight.

Across regions, the trend is clear: regulators are closing gaps, leveraging advanced technology and demanding comprehensive oversight to protect investors and maintain market integrity. Crypto markets now face the same expectations and scrutiny as traditional financial markets (see Figure 5).

Yet crypto markets remain uniquely vulnerable: pseudonymity, fragmented liquidity, 24/7 trading and cross-exchange and cross-border activity create ideal conditions for manipulation. Pump-and-dump schemes, wash trading, spoofing and insider trading mirror traditional market abuse, but at greater speed and scale (see Figure 6).

Additionally, even in a digital-first market like crypto, human conversations matter. Negotiations and collusion can happen via phone, encrypted apps or niche chat platforms.

Executive takeaway

Crypto is not a stand-alone compliance challenge; it is a stress test for the entire

Region	Crypto adoption trends	Enforcement actions/activities
US SEC, CFTC, FINRA; FinCEN (MSB regulations)	• 83% of institutional investors plan to increase allocations in 2025 • Crypto ETFs and DeFi platforms growing • Potential 401(k) inclusion • Federal roadmap for leadership in digital assets	Intensified enforcement for fraud/manipulation Billion-dollar settlements DOJ criminal actions SEC fines for communication lapses Project Crypto launched July 2025
UK FCA under FSMA; MARC (Market Abuse Rules for Crypto)	• Institutional adoption growing • Regulatory clarity through FSMA and MARC • Surveillance and prudential rules for crypto assets in development	Enforcement for pump-and-dump/manipulation Illegal promotions removed MARC regime targeted for end of 2026 Compliance with Money Laundering Regulations
EU ESMA; MiCA (Markets in Crypto Assets Regulation); AMLD5 & 6	• Institutional adoption supported by MiCA • Enhanced investor confidence through regulatory clarity	MiCA mandates anti-manipulation systems Enforcement expected to intensify ESMA guidelines for monitoring communications and trade intent Cross-border coordination suspicious activity
APAC MAS (Singapore), ASIC (Australia), SFC (Hong Kong)	• Adoption trends rising • Jurisdictions implementing licensing and surveillance frameworks • Investor protection laws strengthening • Alignment with global standards	MAS mandates real-time surveillance ASIC expands licensing/targets misleading promos SFC enforces VATP licensing/stablecoins ordinance Fines and license revocations for violations

Figure 5 Global institutional crypto adoption and regulatory trends
Sources:[16,17,18,19,20,21,22] (see footnotes below)

Figure 6 The big challenges in crypto surveillance

market surveillance ecosystem. Its 24/7 trading cycles, pseudonymous participants, fragmented and cross-border venues and rapid, multichannel information flow expose the limitations of legacy surveillance models built on static rules, siloed systems and delayed monitoring.

Firms that cannot reliably detect manipulation in crypto (whether through on-chain activity, cross-exchange trading behaviour, derivative exposure or social media-driven hype) are unlikely to identify increasingly sophisticated abuse in traditional markets. In both environments, effective oversight now depends on real-time, cross-venue and multichannel surveillance capable of operating without gaps.

While crypto assets are digital, the stakes are tangible and growing. Market integrity, regulatory compliance and reputational protection demand integrated surveillance, advanced analytics and a strong culture of accountability.

As crypto continues its rapid move into the financial mainstream, regulators increasingly expect firms to demonstrate continuous oversight that spans trades, blockchain activity and communications. Organisations that combine real-time trade monitoring, blockchain analytics and multichannel communications oversight are better positioned to manage risk while supporting innovation.

Meeting this challenge requires an integrated, AI-driven surveillance framework that unifies crypto and traditional asset monitoring across exchanges, venues and communication channels. Continuous, 24/7 monitoring and alerting must be paired with real-time escalation protocols to address emerging risks as they develop.

Advanced AI and anomaly-detection models should be continuously updated to identify new manipulation tactics in high-velocity markets, including DeFi and tokenised assets, while correlating data across domains (eg on-chain transactions, communications, derivatives and spot trading) to uncover coordinated or cross-market abuse.

Governance and oversight are equally essential. Boards and risk committees must be educated on crypto-specific risks to enable informed decision making and reinforce accountability at the highest levels. Surveillance programmes must also extend to social media and informal communications channels, where hype, misinformation and collusion can directly influence market behaviour. Crypto's constant trading, pseudonymity and global reach make these capabilities essential, not optional.

Ultimately, firms that can meet the surveillance demands of crypto are better equipped to detect manipulation across all asset classes. By modernising surveillance architecture to operate in real time, across borders and channels, institutions can satisfy intensifying global regulatory expectations, strengthen investor confidence and future-proof compliance across both digital and traditional markets.

TREND #4: CROSS-PRODUCT MANIPULATION HAS TURNED SILOED SURVEILLANCE INTO A GOVERNANCE RISK

Market abuse has evolved. It is no longer confined to a single stock or bond at a time. Cross-product manipulation (where traders exploit multiple instruments to move markets) has become a real and costly threat.

The rise of multi-asset products and high-frequency trading has heightened these risks, allowing manipulators to affect one instrument's price through trades on another. The growth of crypto and DeFi has further exacerbated this issue, as traders may be able to exploit unregulated exchanges so as to influence prices on regulated platforms.

Recent enforcement actions underscore this shift. Penalties now regularly exceed tens of millions per case, signalling that regulators expect multi-asset visibility (see Figure 7).

Most legacy surveillance systems remain asset-specific, creating blind spots that sophisticated actors exploit. This is no longer a tooling gap; it is an operating model failure.

Entity	Market	Fine	Manipulation type
Global bank (US)	Treasury securities and futures	US$35M	Cross-product manipulation
Oil & gas company (US)	Gasoline vs futures	US$48M	Physical-derivative price manipulation
Major supplier	Physical & derivative energy markets	US$55M	Coordinated trades
Australian bank	Electricity futures	A$4.995M	Failure to prevent manipulation

Figure 7 Notable enforcement examples
Sources:[23,24,25,26] (see footnotes below)

Executive Takeaway

Traditional surveillance systems increasingly struggle to detect sophisticated market manipulation because they are designed to monitor individual assets in isolation and operate within disconnected organisational and technology silos.

Fragmented teams, inconsistent data and manual processes create structural blind spots that make it difficult to link trades, positions and communications across products, markets and channels. As a result, coordinated and cross-asset abuse, often subtle by design, can persist undetected when oversight is confined to single-asset or venue-specific monitoring (see Figure 8).

The rise of cross-product market abuse delivers a clear lesson: fragmented, single-asset surveillance is no longer sufficient (see Figure 9). Effective detection now requires a unified, real-time approach that integrates data across multiple asset classes, combines on-chain and off-chain information and applies advanced AI and analytics to identify coordinated, anomalous or intent-driven activity.

By breaking down silos and correlating information across trades, positions and communications, firms can surface manipulative behaviours (such as cross-market spoofing, mini-manipulation or coordinated positioning) that would otherwise remain hidden. Achieving this level of oversight demands an integrated, AI-enhanced surveillance architecture built on unified data and cross-asset analytics.

Firms must also establish a centralised data foundation, including a standardised ‘golden record’ through master data management, to align reference data across accounts, instruments and asset classes. Cross-asset correlation models should link activity across equities, options and derivatives, while integrated communications surveillance connects trading behaviour with intent expressed across channels.

AI-driven anomaly detection and sophisticated model tuning are essential to distinguish legitimate hedging or complex strategies from manipulative behaviour, adapt to evolving market conditions and reduce false positives.

Finally, multi-asset alerting frameworks must correlate trades, positions and communications in real time to generate actionable insights, support timely escalation and maintain regulatory compliance.

TREND #5: AI IS NO LONGER OPTIONAL

AI is rapidly reshaping financial services, improving market abuse detection, compliance and operational efficiency. Adoption is growing among firms and regulators alike, making detection faster, more accurate and harder to evade (see Figure 10).

Executive takeaway

AI directly addresses three structural limitations that prevent legacy surveillance systems from detecting sophisticated market abuse: scale and velocity, precision and adaptability.

Modern financial markets generate enormous volumes of trading, communications and behavioural data across multiple venues, asset classes and time zones. Legacy surveillance, built on siloed architectures and post-event analysis, struggles to process these

Figure 8 Why legacy surveillance systems miss the mark

continuous, high-velocity data streams. The rapid proliferation of messaging applications, collaboration tools and social platforms further compounds the challenge by introducing vast amounts of unstructured data that traditional, rules-based systems cannot

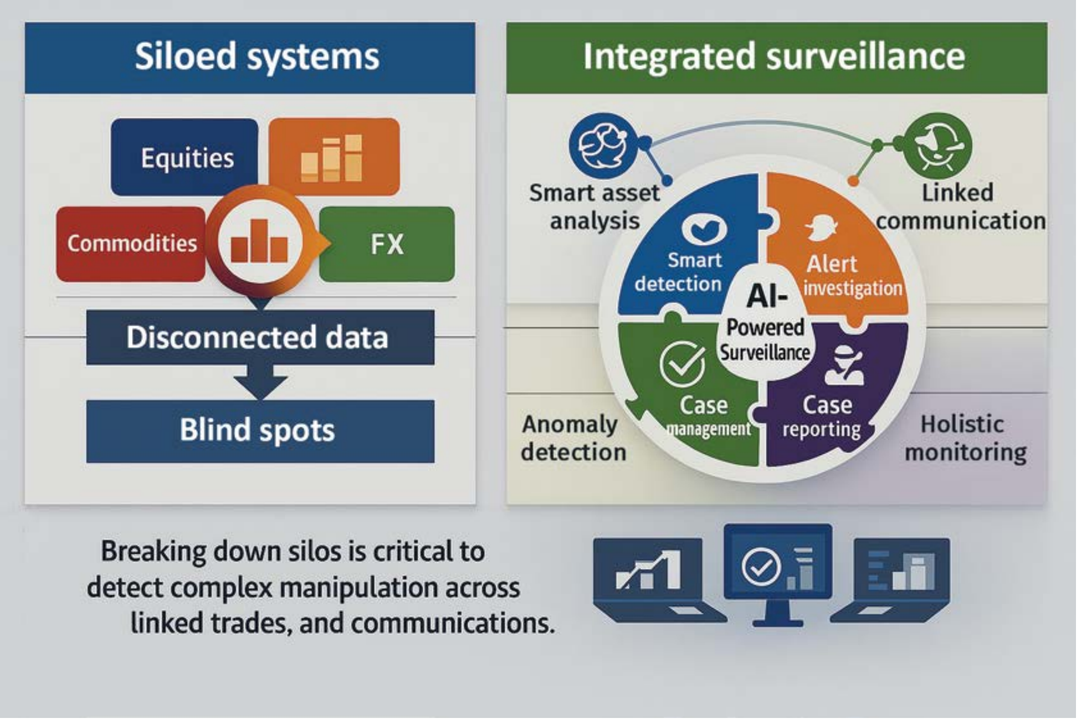

Figure 9 Siloed versus integrated approach

effectively interpret, creating gaps where manipulative behaviour can persist undetected until harm has already occurred.

Precision represents a second key weakness. Static, rule-based alerts frequently generate overwhelming volumes of false positives, flagging legitimate large trades, routine communications or normal market movements while obscuring genuine risk. At the same time, legacy tools lack the contextual awareness required to interpret coded language, sentiment, behavioural nuance and cross-channel interactions. Without this context, compliance teams are forced to sift through noise rather than focus on coordinated or intent-driven abuse.

Adaptability is the third (and most consequential) limitation. Market abuse tactics continuously evolve to exploit the blind spots of predefined detection rules. Sophisticated behaviours such as cross-asset spoofing, layering, collusion through chat

Figure 10 AI transforms financial services. Sources:[27,28,29,30] (see footnotes below)

or collaboration platforms and social media-driven hype demand detection of dynamic, previously unseen patterns. Traditional tools cannot learn or adapt quickly, leaving firms reactive. AI-driven surveillance, by contrast, continuously learns from historical and real-time data, correlates signals across trades,

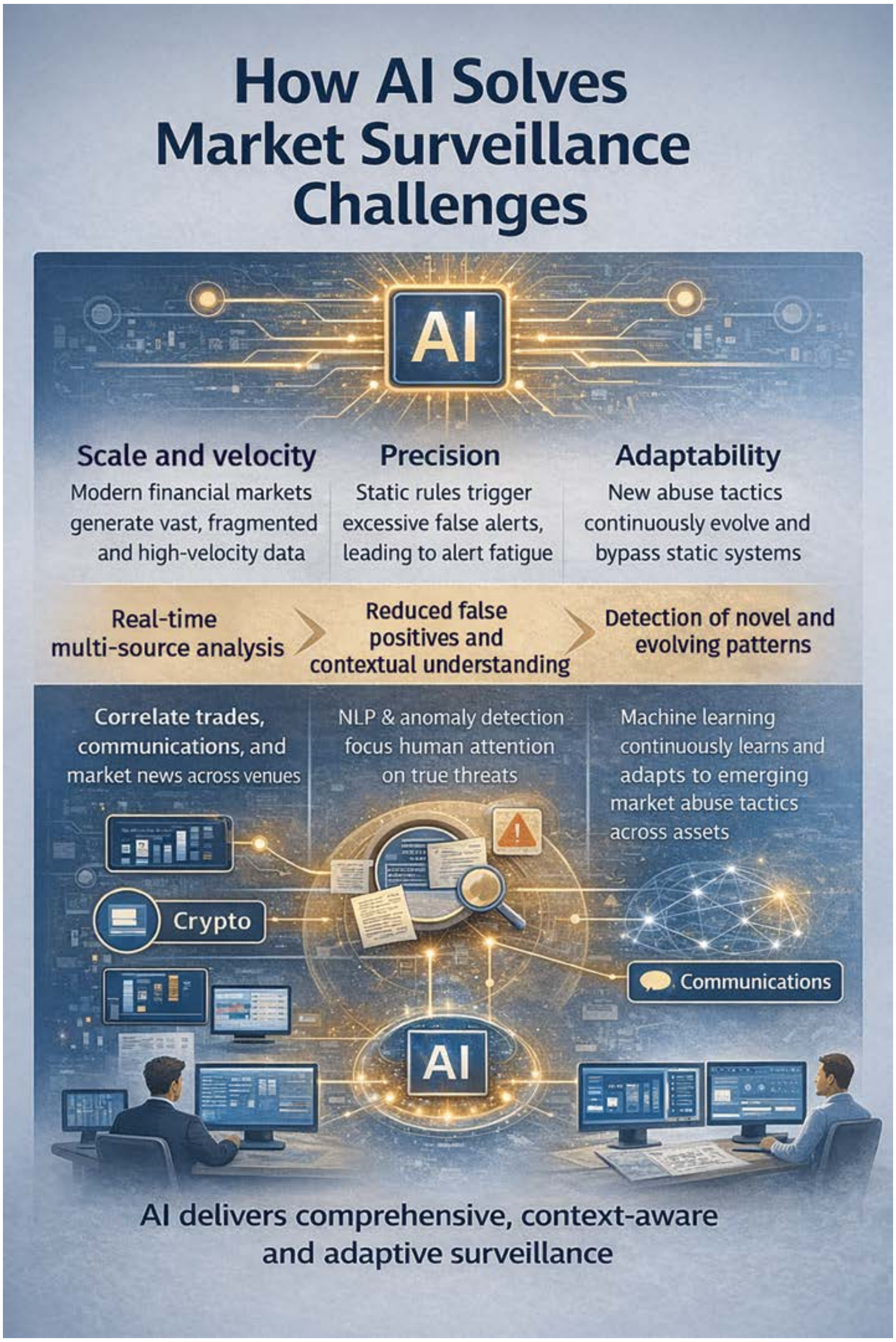

Figure 11 How AI solves market surveillance challenges

communications, market data and sentiment and surfaces emerging abuse patterns before they escalate.

To operationalise these capabilities, firms should implement AI-enabled surveillance that delivers real-time, precise and adaptive oversight by linking trades, positions, communications and market data across all assets and venues (see Figure 11).

This includes: (1) deploying real-time, multi-source analysis to correlate trading activity, communications and market sentiment as events unfold; (2) enhancing precision through NLP and anomaly-detection models that reduce false positives and surface coded or subtle manipulative behaviour; and (3) continuously adapting machine-learning models to evolving abuse tactics across equities, derivatives, crypto and social trading platforms.

AI systems must integrate across markets and data types to provide a holistic view of potential abuse, prioritise actionable insights through risk scoring, automated summaries and intelligent alerting and accelerate investigations by focusing compliance resources on the highest-risk cases.

Generative AI can further support compliance teams by assisting with evidence collation, alert prioritisation and report drafting, freeing human analysts to focus on judgement-intensive investigations.

The takeaway for executive decision-makers is clear: AI is no longer optional. Firms that harness AI-powered surveillance gain real-time, precise and adaptive oversight capable of detecting sophisticated market abuse invisible to legacy systems, while improving operational efficiency, strengthening regulatory compliance and keeping pace with the complexity of modern financial markets.

CONCLUSION: AI-DRIVEN SURVEILLANCE IS A STRATEGIC IMPERATIVE FOR MARKET INTEGRITY

The era of market abuse has evolved and so too must the way firms detect, prevent and respond to it.

Legacy systems and siloed approaches are no longer enough. Market manipulation is faster, more complex and increasingly cross-asset, cross-channel and cross-border. AI-driven surveillance is the game changer, providing real-time visibility, reducing false positives and adapting to emerging abuse tactics.

Firms that embrace integrated, multichannel, AI-enhanced oversight do not just stay compliant; they gain a strategic advantage, protecting market integrity, investor confidence and their own reputation. In today's high-speed markets, proactive, intelligent surveillance is not optional; it is the very foundation of resilience and trust.

References

(1) Starling Trust Insights (n.d.) 'US and UK Enforcement Actions Surged in 2024', available at https://insights.starlingtrust.com/content/observations/us-and-uk-enforcement-actions-surged-in-2024 (accessed 28th February, 2026).

(2) Corporate Compliance Insights (n.d.) 'SEC, CFTC Combine for $9B+ in Penalties in 2023', available at https://www.corporatecomplianceinsights.com/steeleye-fine-tracker-report-2023/ (accessed 28th February, 2026).

(3) SEC (n.d.) 'SEC Announces 2024 Enforcement Results', available at https://www.sec.gov/newsroom/press-releases/2024-186 (accessed 28th February, 2026).

(4) Reuters (n.d.) 'Trafigura Agrees to Pay $55 Million to Settle CFTC Charges', available at https://www.reuters.com/markets/commodities/cftc-orders-trafigura-pay-55-million-over-fraud-2024-06-17/ (accessed 28th February, 2026).

(5) CFTC (n.d.) 'Press Release 8953-24', available at https://www.cftc.gov/PressRoom/PressReleases/8953-24 (accessed 28th February, 2026).

(6) The Australian (n.d.) 'Macquarie Group Slapped With $49M in Fines', available at https://www.theaustralian.com.au/business/financial-services/macquarie-group-slapped-with-49m-in-fines-over-failures-to-prevent-energy-market-manipulation/news-story/88988e9f05d572d3ff264a04493e17fe (accessed 28th February, 2026).

(7) FCA (n.d.) '2023 Fines', available at https://www.fca.org.uk/news/news-stories/2023-fines (accessed 28th February, 2026).

(8) Compliance Week (n.d.) 'SEC & CFTC Off-Channel Communications Penalties', available at https://www.complianceweek.com/regulatory-enforcement/table-sec-cftc-off-channel-communications-penalties/33851.article (accessed 28th February, 2026).

(9) FCA (n.d.) 'Multi-Firm Review: Off-Channel Communications', available at https://www.fca.org.uk/publications/multi-firm-reviews/multi-firm-review-off-channel-communications (accessed 28th February, 2026).
(10) FiscalNote (n.d.) 'ESMA Guidelines & MiCA Crypto Regulation', available at https://fiscalnote.com/blog/esma-guidelines-mica-crypto-regulation (accessed 28th February, 2026).
(11) Compliance Week, ref. 8 above.
(12) SEC (n.d.) 'Press Release 2024-44', available at https://www.sec.gov/newsroom/press-releases/2024-44 (accessed 28th February, 2026).
(13) Corporate Compliance Insights (n.d.) 'SEC Crackdown Fines 26 Firms', available at https://www.corporatecomplianceinsights.com/sec-crackdown-fines-26-firms/ (accessed 28th February, 2026).
(14) IFAMagazine (n.d.) 'FCA Leads International Crackdown on Illegal Finfluencers', available at https://ifamagazine.com/fca-leads-international-crackdown-on-illegal-finfluencers/ (accessed 28th February, 2026).
(15) Bloomberg (n.d.) 'Crypto Market Cap Tops $4 Trillion', available at https://www.bloomberg.com/news/articles/2025-07-18/crypto-market-cap-tops-4-trillion-as-us-stablecoin-bill-passes (accessed 28th February, 2026).
(16) EY (n.d.) 'Growing Enthusiasm and Adoption of Digital Assets', available at https://www.ey.com/en_us/insights/financial-services/growing-enthusiasm-and-adoption-of-digital-assets (accessed 28th February, 2026).
(17) Investopedia (n.d.) 'Alternative Assets in Retirement Funds', available at https://www.investopedia.com/alternative-assets-in-retirement-funds-11794419 (accessed 28th February, 2026).
(18) Fintech Law Blog (n.d.) 'White House Working Group on Digital Asset Markets', available at https://www.fintechlawblog.com/2025/08/19/the-white-house-working-group-on-digital-asset-markets-report-what-it-means-for-stablecoins-and-payments/ (accessed 28th February, 2026).
(19) Financial Planning (n.d.) 'FINRA Finds Crypto Relationships Widespread Across Brokerages', available at https://www.financial-planning.com/news/finra-finds-crypto-relationships-widespread-across-brokerages (accessed 28th February, 2026).
(20) A&O Shearman (n.d.) 'SEC Chairman Atkins Announces Project Crypto', available at https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/sec-chairman-atkins-announces-project-crypto (accessed 28th February, 2026).
(21) U.S. DOJ (n.d.) 'Former Coinbase Insider Sentenced', available at https://www.justice.gov/usao-sdny/pr/former-coinbase-insider-sentenced-first-ever-cryptocurrency-insider-trading-case (accessed 28th February, 2026).
(22) DL News (n.d.) 'Terraform Labs Agrees to Pay SEC to End Lawsuit', available at https://www.dlnews.com/articles/regulation/terraform-labs-agrees-to-pay-sec-to-end-lawsuit/ (accessed 28th February, 2026).
(23) FX News Group (n.d.) 'NatWest Markets to Pay $35M in Penalties for Fraud in US Treasury Markets', available at https://fxnewsgroup.com/forex-news/regulatory/natwest-markets-to-pay-35m-in-penalties-for-fraud-in-us-treasury-markets/ (accessed 28th February, 2026).
(24) WSJ (n.d.) 'TotalEnergies Unit to Pay $48 Million Over Gasoline Futures Manipulation', available at https://www.wsj.com/articles/totalenergies-unit-to-pay-48-million-over-alleged-gasoline-futures-manipulation-9119c9e1 (accessed 28th February, 2026).
(25) Reuters (n.d.) 'CFTC Orders Trafigura to Pay $55 Million Over Fraud', available at https://www.reuters.com/markets/commodities/cftc-orders-trafigura-pay-55-million-over-fraud-2024-06-17/ (accessed 28th February, 2026).
(26) The Australian, ref. 6 above.
(27) Global Relay (n.d.) 'FCA Report Shows 75% of Firms Are Now Using AI', available at https://www.globalrelay.com/resources/thought-leadership/fca-report-shows-75-of-firms-are-now-using-ai-but-only-34-know-how-it-works/ (accessed 28th February, 2026).
(28) Confluence (n.d.) '68% of Financial Firms Say AI in Risk and Compliance Is a Top Priority', available at https://www.confluence.com/68-of-financial-firms-say-ai-in-risk-and-compliance-is-a-top-priority-here-are-some-best-practices-for-thoughtful-ai-adoption/ (accessed 28th February, 2026).
(29) InvestmentNews (n.d.) 'Almost One-Third of Financial Firms Embrace AI for Communications Compliance', available at https://www.investmentnews.com/ria-news/almost-one-third-of-financial-firms-embrace-ai-for-communications-compliance/259825 (accessed 28th February, 2026).
(30) Reuters (n.d.) 'German Financial Watchdog: AI Is Helping Catch Market Abuse', available at https://www.reuters.com/sustainability/boards-policy-regulation/german-financial-watchdog-ai-is-helping-catch-market-abuse-2025-06-02/ (accessed 28th February, 2026).