Financial Services Regulatory Outlook 2025-2027:

Implications for Surveillance Executives

This authorized reprint has been prepared for Arctera.
For more information, please reach out at info@opimas.com.

OPIMAS | arctera™

Table of Contents

Authors

Anna Griem: ag@opimas.com

Suzannah Baluffi-Fry: sb@opimas.com

Contact

Opimas LLC

75 State Street, Suite 100

Boston, MA 02109 USA

info@opimas.com

Executive Summary

Unrelenting enforcement, cooperation rewarded

Regulatory authorities remain highly focused on breaches of communications and archiving requirements but are placing greater emphasis on cooperation and self-disclosure, rewarding institutions that report violations proactively with significantly reduced penalties. Enforcement sweeps targeting off-channel communications such as WhatsApp, Signal, and mobile capture continue. Crypto and digital asset platforms have become a lucrative, nascent focal point for US regulators, generating some of the largest fines in recent years.

While the overall dollar value of penalties for communications and archiving lapses has moderated since the peak in 2021–22, the pace of this enforcement remains steady.

End of harmonization across jurisdictions?

Globally, fragmentation may be accelerating. Regulators are moving away from harmonized standards toward localized rules that reflect national priorities.

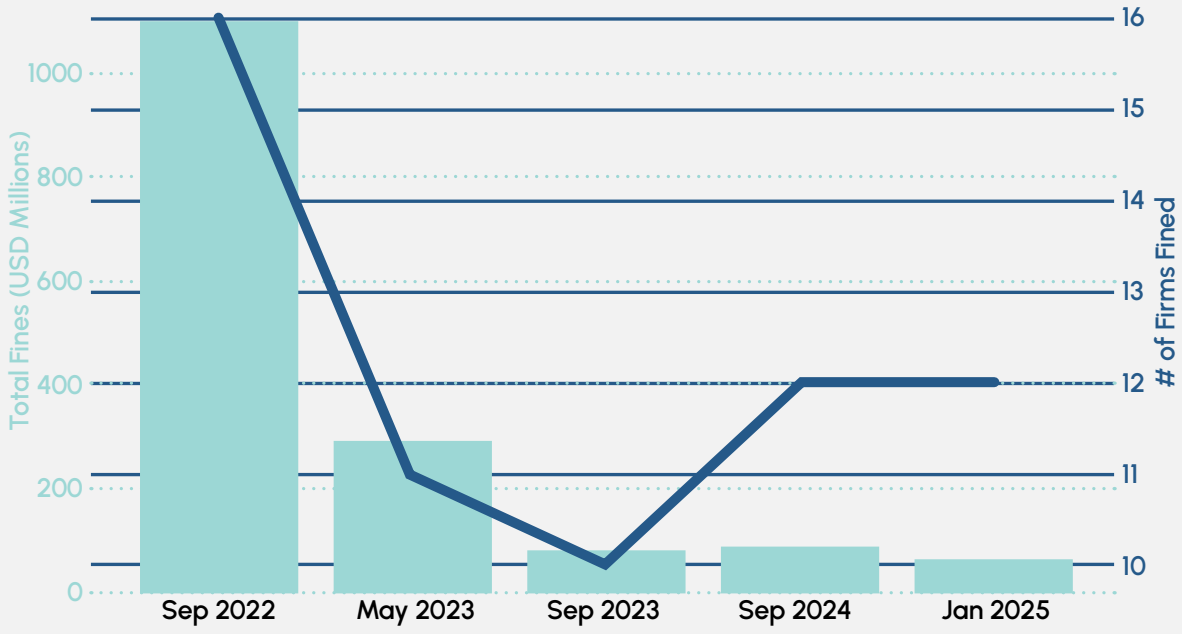
Data protection remains a priority. The EU continues to enforce the General Data Protection Regulation (GDPR), India has introduced the Digital Personal Data Protection Act (DPDP), Japan in 2022 amended its Act on the Protection of Personal Information (APPI) which clarifies obligations for cross border data transfers, and the Gulf states are tightening sovereign hosting requirements as well. In China, data localization and government access rules further restrict cross-border flows.

Outside the US, enforcement often emphasizes remediation rather than punitive fines, but the divergence forces international institutions to operate multiple compliance frameworks in parallel. If one-size-fits-all global compliance strategy is the dream, it may be going up in smoke. Still, some firms are working hard to attempt to centralize global compliance efforts.

This fragmentation in regulatory objectives by region directly shapes how firms must think about technology and vendor choices.

Figure 1: Waves of fines for off-channel communications and recordkeeping violations by the SEC

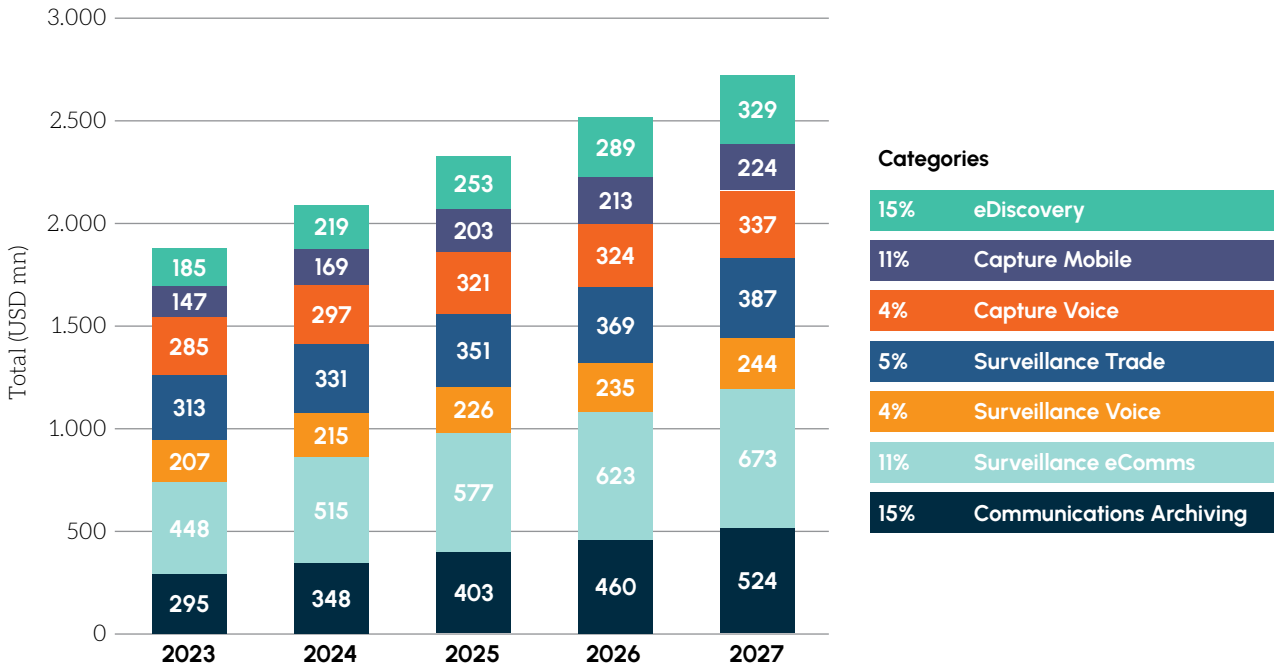
U.S. SEC Fines for Off-Channel Comms Recordkeeping Violations (2022-2025)



Source: Opimas, SEC

Figure 2: Total spending on capture, archiving, surveillance, and eDiscovery in capital markets through 2027

Spending on Capture, Archiving, Surveillance and eDiscovery in Capital Markets.



Source : Good Jobs First, Opimas analysis

AI gains ground, cloud under pressure

Data sovereignty concerns are highlighting the limits of cloud-only surveillance solutions. While cloud platforms offer scale and efficiency, they are not always fit for purpose when regulators or clients require data to remain within borders. Hybrid and on-premise models are regaining importance. Sensible vendor due diligence therefore must extend beyond functionality to cover data extraction terms, exit options, financial resilience, and deployment architecture.

Artificial intelligence has become the most visible technological development in surveillance. Regulators, once skeptical of "black box" models, now appear encouraging of responsible use of AI. In communications monitoring, natural language processing (NLP) and large language models have sharply reduced false positives and improved the capture of intent and context. In trade surveillance, impact is more limited, with AI mainly used to enrich alerts and support analysts rather than to identify cases for investigation. Across both domains, explainability and governance remain the non-negotiables. Models must be transparent and defensible if challenged by regulators.

From volume to value

Surveillance functions are being asked to deliver more with less. Compliance budgets remain constrained, with senior management expecting prior technology investments to generate lasting efficiencies rather than justify additional headcount. Even so, Opimas projects total spending on capture, archiving, surveillance, and eDiscovery solutions in capital markets to exceed US$2.7 billion by 2027.

Large offshore review teams are giving way to smaller teams of experienced analysts, with AI handling much of the first-line triage. This new model of surveillance teams emphasizes precision over volume: fewer people with deeper expertise, amplified by technology.

In addition to working with external compliance solutions, Tier 1 banks appear to be increasingly considering building bespoke systems in-house. Mid-tier firms continue to rely on vendors, but push for tighter integration into their existing and often unique infrastructure. Smaller institutions are leaning more heavily on outsourced managed services and turnkey solutions as cost-effective ways to meet complex obligations.

Implications for 2026–2027

In the coming years Opimas expects that enforcement won't ease, budgets won't balloon wildly but will steadily increase, and technology will only become more important. Institutions will be advised to use AI with discipline, maintain flexible architecture, and attempt to align operations to the shifting and increasingly regional regulations.

Regulatory Overview

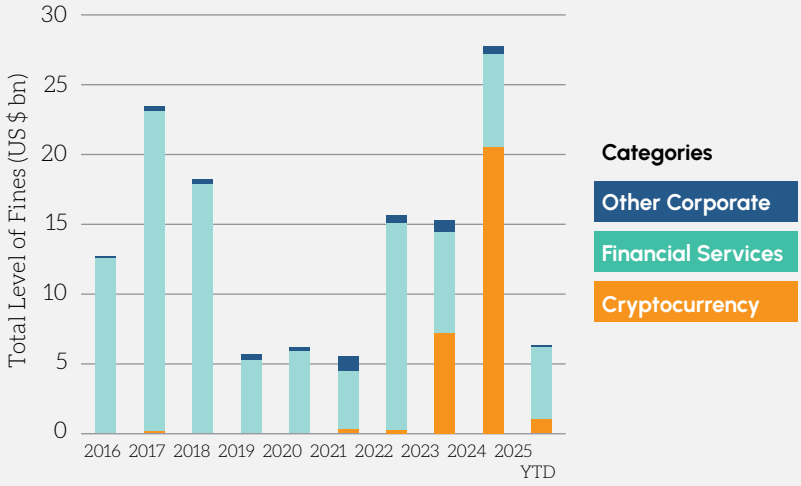
Annual global financial penalties on financial institutions exceeded US$25 billion in 2024. While fines in 2025 have been far lower thus far, this does not signify a trend. The overall level of penalties has always shown considerable volatility from year to year and there is no reason to believe that fines will remain at this low level permanently.

International regulatory requirements

Globally, regulation is increasing in complexity. A decade ago, there was a sense of convergence toward international standards; today the same cannot be so confidently said. Jurisdictions are moving away from harmonization toward localized frameworks that reflect national priorities—particularly in data privacy, sovereignty, and supervisory philosophy.

Figure 3: Total financial services penalties globally, by year

Fines have come in waves over the years, with 2022-2024 particularly bad for financial institutions and other firms subject to financial crime oversight, such as cryptocurrency companies.



Source: Good Jobs First, Opimas analysis

Data privacy rules abound

Privacy regulation in Europe remains defined by the General Data Protection Regulation (GDPR), which continues to impose strict limits on how personal data can be collected, stored, and transferred.

In the Gulf Cooperation Council (GCC), regulators in countries such as Saudi Arabia and the UAE are tightening sovereign hosting mandates, pushing for sensitive financial and personal data to remain on servers physically within national borders.

Across Asia there is a patchwork of national data and privacy legislation. In 2023, India enacted the Digital Personal Data Protection Act (DPDP), restricting the cross-border transfer of data about Indian citizens and requiring firms to consider local hosting. Japan in 2022, amended its Act on the Protection of Personal Information (APPI) to further outline obligations for cross border data transfers and privacy protections. Additional amendments are expected in the coming months. The Personal Data Protection Act (PDPA) in Singapore, last updated in 2020, also exists to promote responsible data management practices.

South Korea´s Personal Information Protection Act (PIPA) and Hong Kong´s Personal Data Privacy Ordinance (PDPO) are considered to be some of the strictest data protection laws in Asia. China's approach is more stringent still, combining data localization with government accessibility requirements that add unique risks for global firms.

Australia, Thailand and Indonesia are all expected to release further guidance on data protection in the coming year or so.

Global institutions may feel less comfortable centralizing compliance infrastructure in a few regional data centers. Instead, they may need to maintain multiple, parallel environments: European data in Europe, Indian data in India, GCC data in-country, and so forth. Surveillance vendors are adapting by offering regional cloud instances or on-premise deployments to meet client needs. For compliance leaders, this creates both financial and operational burdens: higher costs, greater complexity, and a stronger need for coordination with IT and legal functions.

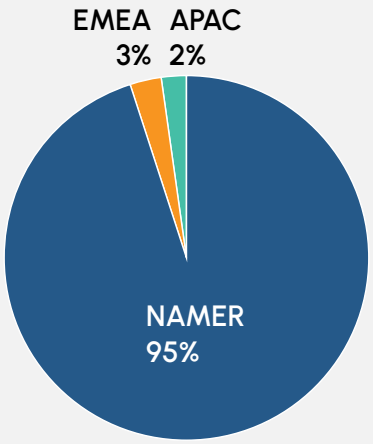
Prospective buyers also increasingly reject surveillance solutions that route data through countries perceived as insecure or adversarial. For example, institutions have raised concerns about communications captured on platforms like WeChat, given the risk that traffic may be accessible to foreign governments. Surveillance executives must therefore evaluate not only whether a solution captures the right

data, but also where that data flows, how it is stored, and who might have access. This has fueled rising demand for vendors that offer flexible hosting, including private cloud and on-premise options.

Maintaining compliance across such a fragmented landscape has become a balancing act. Institutions must uphold global standards for ethical conduct and recordkeeping while tailoring processes to local legal requirements. A retention period that is mandatory under SEC Rule 17a-4 in the US for broker-dealers, for example, may be prohibited under a privacy rule elsewhere.

Figure 4 Total financial services penalties by region

North American regulators (particularly the US) account for 95% of all financial penalties levied on banks since 2010...



Total fines since 2010: US$262 billion

Source: Good Jobs First, Opimas analysis

Tolerance for penalties differ by region

Fragmentation is also visible in how regulators enforce compliance. The US remains uniquely punitive, accounting for more than 95% of global financial penalties in financial services since 2010. By contrast, regulators in Europe and Asia often emphasize remediation and supervisory guidance over large fines.

The UK's Financial Conduct Authority (FCA) illustrates the difference. While it enforces market abuse and conduct rules, it has shown reluctance to impose the massive penalties common in the US. In early 2024, the FCA even backtracked on a proposal to publicly "name and shame" firms under investigation, citing concerns about competitiveness and the risk of driving businesses away. This reversal highlighted the FCA's preference for remediation over sanction and reinforced its role as a supervisory partner rather than a punitive enforcer.

The disparity is one of philosophy as much as magnitude. While financial institutions certainly view large penalties as a deterrent, they also view these fines as a cost of doing business in the US. Elsewhere, regulators feel more compelled to balance oversight with the need to maintain healthy domestic financial sectors. A misconduct issue that results in a stern letter in London or Hong Kong could generate a serious fine in New York. For global banks, this unevenness complicates the task of setting groupwide standards.

Emerging products and channels

Fragmentation also extends to the treatment of new asset classes and communication channels. Crypto regulation provides a clear case. The US has taken an aggressive stance, levying multibillion-dollar penalties against crypto exchanges such as FTX and Binance, as well as crypto infrastructure like Terraform Labs. By contrast, other jurisdictions have been more permissive or are still developing frameworks. This divergence creates tension for institutions that operate globally. A conservative, US-driven approach that treats crypto communications and trading as high-risk and heavily surveilled may appear excessive in more permissive jurisdictions, but failing to apply it uniformly exposes firms to US enforcement.

The same is true for communication channels. In the US, regulators explicitly prohibit the use of unmonitored platforms for business purposes, prompting firms to consider global bans. In Asia, however, platforms like WeChat are widely considered essential for client engagement. Here, the conflict is between global compliance obligations and local business practices. Firms may be forced to apply the strictest standard across all markets, even at the cost of commercial friction.

Implications for compliance leaders

For compliance executives, fragmentation means agility is no longer optional. International institutions must design modular compliance frameworks that can be customized region by region without losing sight of global standards. This requires close coordination between compliance, IT, and legal functions, as well as continuous horizon scanning to identify new regulatory developments.

The trend toward fragmentation shows no sign of slowing. If anything, data protection rules are tightening, enforcement philosophies are diverging further, and emerging technologies are raising new jurisdictional questions.

US regulatory outlook

Total fines remain high with crypto in focus

As shown in Figure 3, a defining feature of the current US regulatory landscape is the rise of crypto and digital asset enforcement. The collapse of high-profile exchanges and custodians has generated penalties in the billions. Regulators have made clear that digital assets fall squarely within their supervisory remit, and firms involved in this space are expected to maintain the same surveillance and recordkeeping standards as in traditional markets. Enforcement has already expanded to cover communications and trading activity linked to crypto assets, and this focus is likely to intensify as the sector matures. For compliance teams, this means extending surveillance to new asset classes and ensuring that crypto-related interactions are captured alongside more conventional activity.

At the same time, the current administration has adopted a somewhat warmer stance toward digital assets. While this may pave the way for clearer regulatory frameworks, it does not diminish the expectation that firms maintain rigorous surveillance and controls.

Steady enforcement but softer fines

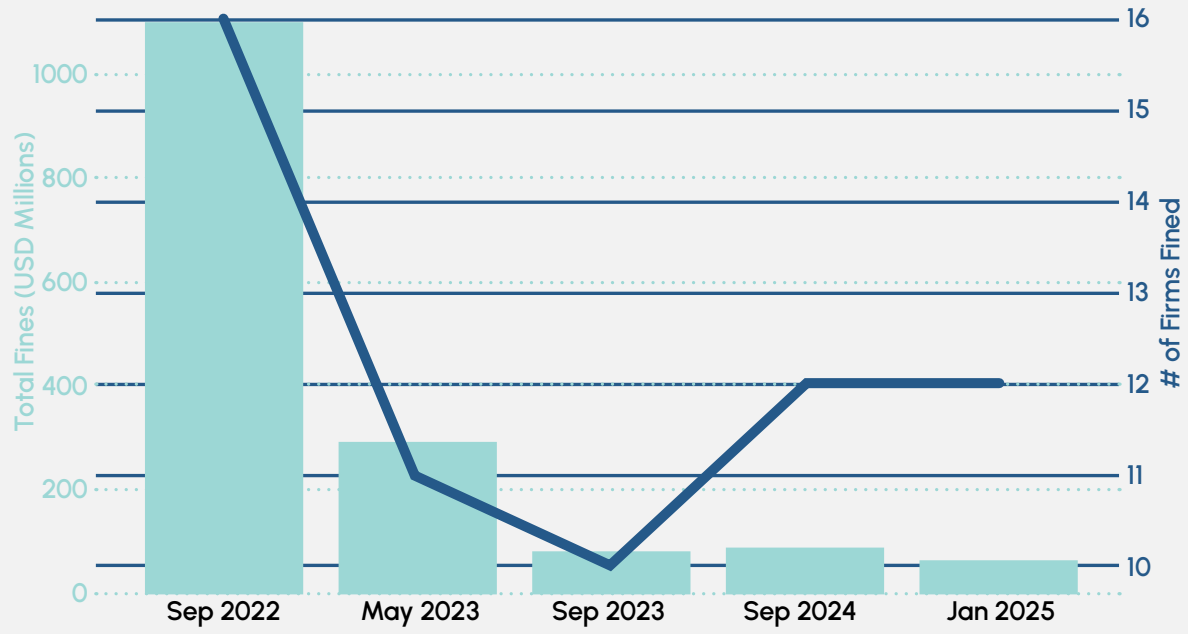
The Securities and Exchange Commission (SEC) continues to conduct sweeps for recordkeeping failures, typically charging between 10 and 16 firms at a time. While the total dollar value of penalties has moderated since the extraordinary peaks of 2021 and 2022, the frequency of actions remains steady.

Firms that self-report violations and cooperate fully with investigations are now receiving significantly reduced penalties compared with peers who wait for enforcement to find them. This has made self-disclosure one of the most important differentiators in regulatory outcomes. A January 2025 settlement underscored the point: one institution that came forward voluntarily paid US$600,000, while peers in the same sweep paid between US$4 million and US$12 million each. The message from regulators is clear: proactive cooperation can save firms tens of millions.

Communications surveillance remains important to regulators, who expect all business-related conversations—whether on email, text, WhatsApp, Signal, or other channels—to be preserved and supervised. The SEC and the Department of Justice (DOJ) remain focused on preventing the use of "off-channel" communications for business activity, a priority that emerged after the multibillion-dollar "WhatsApp fines" of 2022. Institutions cannot assume that enforcement will fade now that the headlines are less distressing. The expectation is that firms maintain compliant systems, conduct regular audits, and remediate problems before they escalate.

While new cases may benefit from reduced penalties through self-disclosure, regulators have not extended this leniency retroactively. Institutions that paid massive settlements in 2021 and 2022 for messaging violations remain bound by those agreements, with no renegotiation offered.

Figure 5 Waves of fines for off-channel communications and recordkeeping violations by the SEC



Source: Opimas, SEC

FCPA and anti-bribery oversight

On the anti-bribery front, President Trump has signaled interest in weakening the Foreign Corrupt Practices Act (FCPA) framework and reducing the use of corporate monitorships in bribery cases. If enacted, such changes could limit the number of high-profile FCPA prosecutions. However, other enforcement areas like insider trading, market manipulation, and consumer protection, might simply move higher on the agenda.

Continuity is the safest assumption

The US will remain the toughest jurisdiction. Regardless of administration, core expectations will not ease. Firms should continue to strengthen internal systems, ensure rigorous archiving across all communication channels, and conduct audits to identify violations before regulators do. Embedding a culture that encourages early escalation and remediation not only reduces risk but also positions firms to benefit from greater leniency from their regulators.

Technology Trends

Cloud-only deployment can be a dealbreaker

The array of surveillance offerings in capital markets is vast, but functionality alone does not determine the selection of a vendor. Deployment flexibility—cloud, hybrid, or on-premise—has become a decisive factor, with providers that limit options increasingly being removed from shortlists.

Cloud under pressure

The rising emphasis on data sovereignty is also reshaping technology decisions. Over the past decade, many institutions moved compliance systems to the cloud, attracted by scalability, easier updates, and lower cost. But regulatory and geopolitical shifts are prompting reassessment. The core concern is control: regulators and clients now expect sensitive communications data to remain in the correct jurisdiction, protected from potential external interference.

A purely cloud-based approach, where archives are stored in a few large data centers, can conflict with these expectations. Even in markets without such rules, regulatory guidance is trending toward caution. If a vendor hosts data in a jurisdiction that later becomes subject to sanctions or disruption, the worry is that access to archives could be cut off overnight.

US agencies have already advised against reliance on China-based infrastructure for sensitive data. For global firms, this geopolitical exposure is an active priority and concern.

The return of hybrid models

Operational resilience is equally at stake. Outages or government injunctions in a centralized cloud could disable compliance capabilities across regions. Surveillance leaders increasingly ask: Do we have alternate access if our primary cloud is constrained? Can archives be moved quickly if regulators require local hosting? These questions have pushed hybrid models back into focus. By keeping highly sensitive or regulated data on-premise or in-country, and using cloud only for permitted functions, firms can mitigate both legal and operational risks.

Vendor realignment

Vendor strategies reflect this pressure. Some leading providers that discontinued on-premise support have allegedly lost business as clients demanded flexibility. NICE Actimize's decision to move its SurveilX trade surveillance platform to cloud-only reportedly drove some banks toward Nasdaq's SMARTS, now the dominant solution with on-premise capabilities. Similarly, Smarsh reportedly faced client frustration after halting on-premise deployments of its Digital Reasoning acquisition, and encountered challenges with cloud rollouts. Conversely, younger vendors that initially launched as "cloud only", have actually begun adding on-premise or private cloud options to meet client demand. The message is clear: procurement often favors vendors able to support multiple deployment models.

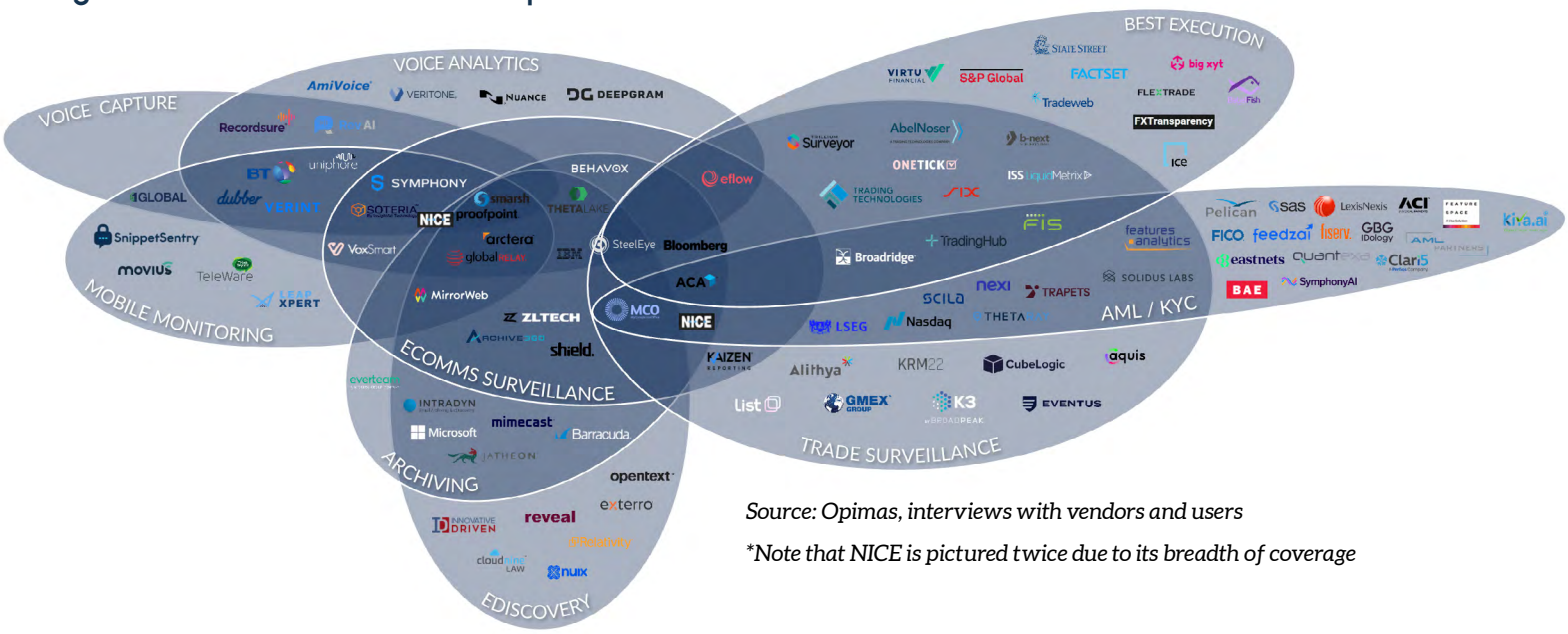
Wake-up call due to the Smarsh breach

In May 2025, TeleMessage—a secure mobile messaging archiving service acquired by Smarsh in February 2024—was compromised, exposing more than 400 GB of metadata and administrator credentials from financial and government clients. Although message contents remained encrypted, the incident demonstrated how metadata alone can pose significant regulatory and security risks. US agencies quickly warned against continued use, and many institutions were forced to reassess their vendor dependencies.

The breach reinforced a broader lesson: firms must demand stronger governance and greater portability from their vendors. Key questions now include how quickly archives can be migrated if regulators require in-country storage, and what it would cost to extract data from a provider's data center.

In practice, this means negotiating contracts that guarantee access and portability, deploying containerized software that can move across environments, and subjecting vendors to independent security assessments. Compliance leaders are also working more closely with IT risk teams, ensuring surveillance platforms undergo the same rigorous testing as core banking systems. By building optionality into deployment choices and treating vendor oversight as a central compliance task, institutions can meet sovereignty demands while reducing operational and regulatory risk.

Figure 6 Surveillance vendor landscape 2025



Source: Opimas, interviews with vendors and users

**Note that NICE is pictured twice due to its breadth of coverage*

AI moves from option to expectation

Regulators now expect AI to be part of compliance programs. Where they once asked "why are you using AI?" the question has become "why aren't you?" The most tangible gains are in communications monitoring. Legacy lexicon-based systems, built on static keyword lists, reportedly generated more than 99% irrelevant alerts. By contrast, Natural Language Processing (NLP) and large language models (LLMs) interpret context, tone, and intent, dramatically reducing noise while surfacing nuanced behaviors such as collusion or harassment. The enormous surveillance fines of 2022 accelerated adoption, forcing banks to confront the volume and complexity of chat data. Many Tier-1 institutions are now building or deploying AI models at scale, while regulators themselves have started using advanced analytics, further legitimizing industry adoption.

From lexicons to LLMs

Before 2022, keyword lexicons dominated surveillance, with innocuous phrases like "let's lunch" triggering alerts because they were thought to resemble trading slang. After contending with multibillion-dollar penalties for off-channel messaging, financial services firms accelerated investment in NLP and LLM-based tools. These models better distinguish harmless banter from suspicious activity, cutting false positives while capturing risks missed by legacy systems.

In trade surveillance, adoption of AI is slower. Alert generation remains rule-based, reflecting regulators' demand for deterministic, auditable methods. AI is used after alerts are generated to enrich explanations, prioritize risks, and streamline investigations. Some platforms now offer chatbot-style interfaces, allowing analysts to query systems conversationally to retrieve trades, related alerts, or compliance policies. These tools speed resolution and improve the analysts´ experience, but they stop short of replacing scenario-based surveillance logic.

Hallucinations and the inexcusable error rate

Despite its benefits, AI introduces new risks. Models must be auditable, with outcomes documented and defensible. Someone within the institution must be able to explain how a model functions and why it flagged a case. Regulators are clear: AI cannot operate as a "black box."

Institutions must also guard against AI "hallucinations". With concerning frequency, AI tools create outputs that are plausible but wrong. This reinforces a central principle: AI should complement, not replace, human oversight. The most effective deployments use AI as a first-line filter, with escalation and judgment reserved for compliance officers.

Data quality is another constraint. Surveillance data is fragmented and inconsistent, requiring cleansing and standardization before models can be trained reliably. Without this preparation, AI risks amplifying weaknesses instead of fixing them. Talent is scarce as well, with financial institutions competing against technology firms for experienced NLP engineers and data scientists.

Governance is non-negotiable

Strong governance is now an expectation. Regulators want rigorous model risk management, ongoing monitoring, and clear escalation procedures. Validation and periodic testing is required, along with the ability to override or disable models if performance degrades. "Explainable AI" is emerging as a baseline: firms must be able to articulate not only how a model works but also why a specific alert was or was not generated.

AI is enhancing surveillance by reducing false positives, improving triage, and accelerating investigations, but it is far from a cure-all. By 2027, firms should focus on explainability, governance, and integration into human workflows to ensure AI delivers real improvements to compliance programs.

Build or buy?

Sourcing strategies vary significantly by institution size. Tier 1 banks, with the necessary resources and technical talent, are increasingly exploring bespoke in-house builds to integrate within their existing compliance frameworks. This approach offers greater customization and control but also carries substantial execution risk: large programs can consume years and still fall short. Institutions pursuing in-house development should take care not to waste time reinventing capabilities that proven vendor solutions already provide.

A more common approach among Tier 2 firms is to rely on vendors while pressing for tighter integration into existing infrastructure. Smaller Tier 3 institutions, which lack the scale for proprietary solutions, appear to also be turning to managed services and turn-key solutions as a cost-effective way to fulfill surveillance obligations.

It is important to remember that outsourcing does not absolve responsibility. Surveillance executives remain accountable for quality, meaning vendor management and oversight remain essential. Managed services can extend capacity, but firms must ensure that external providers meet regulatory standards and integrate cleanly into internal processes.

Reshaping Compliance Teams

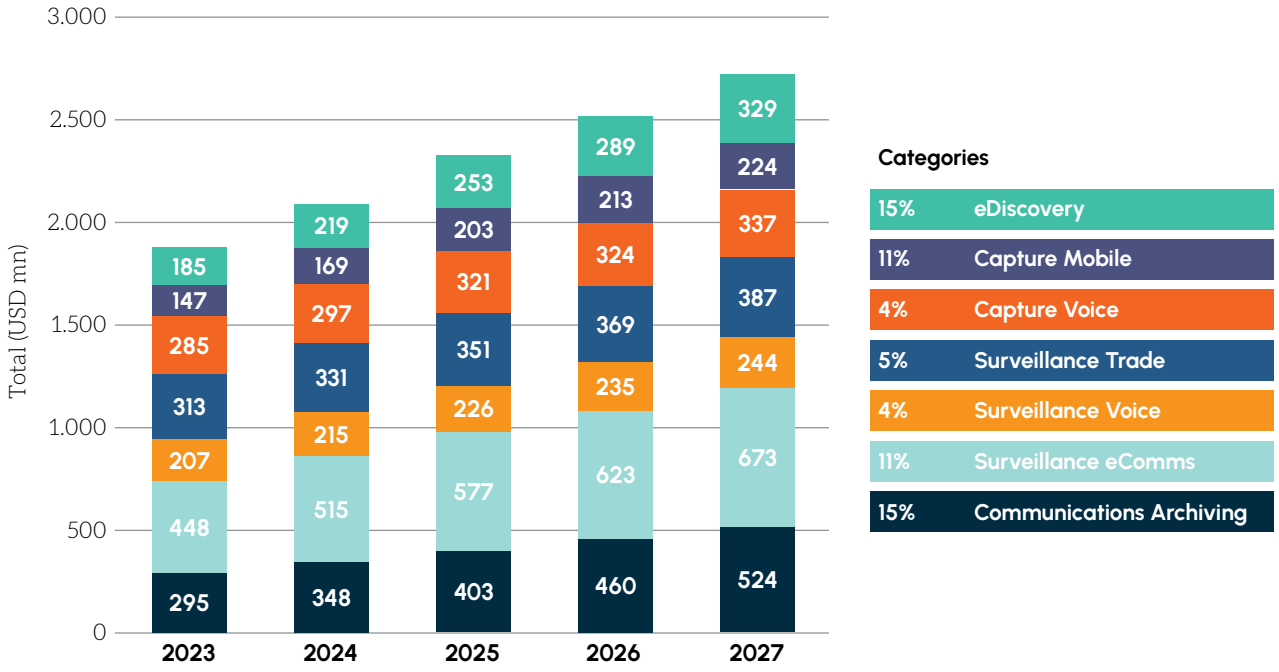
Tight budgets and expectations

The confluence of regulatory pressure and technological change is reshaping how firms organize and resource surveillance. But while expectations remain high, budgets are under pressure. Boards now expect measurable improvements in oversight without proportional increases in spending. To meet this challenge, institutions are rethinking operating models, reducing reliance on headcount, and hoping to deploy technology—especially AI—to deliver more effective monitoring at lower cost.

Even so, Opimas projects total spending on capture, archiving, surveillance, and eDiscovery solutions in capital markets to exceed US$2.7 billion by 2027. Large investment banks spend over US$5 million annually on these technologies, while the largest asset managers spend around US$3.5 million each. However, the combined aggregate spend by smaller institutions exceeds Tier 1 totals on both buy and sell sides.

Communications surveillance (US$577M) is the largest market segment, followed by communications archiving (US$403M). Spending on eDiscovery and archiving is growing fastest (15% YoY), followed by communications surveillance and mobile capture (11% YoY). Spending on voice capture and trade surveillance is growing at a slower 4–6% rate annually.

Figure 7 Total spending on capture, archiving, surveillance, and eDiscovery in capital markets through 2027



Source : Good Jobs First, Opimas analysis

Figure 8 Total surveillance spend by type and size of institution and across surveillance categories in 2025

		Broker-Dealer - Tier I	Broker-Dealer - Tier II	Broker-Dealer - Small	Asset Managers - Tier I	Asset Managers - Tier II	Asset Managers - Small	Exchanges and ATSs	Regulators	**Total**
Communications archiving		36	98	100	52	32	86	1	0	**403**
Surveillance	eComms	51	180	172	70	47	54	1	2	**577**
Surveillance	Voice	17	95	67	18	16	14	0	0	**226**
Surveillance	Trade	42	138	73	17	18	29	29	5	**351**
Capture	Voice	8	49	131	21	20	83	0	0	**312**
Capture	Mobile	10	36	74	18	17	49	0	0	**203**
eDiscovery		14	74	81	21	17	45	2	0	**253**
Total (USD mn)		**177**	**669**	**697**	**217**	**165**	**359**	**33**	**8**	**2,324**

Source: Opimas, interviews with vendors and institutions, vendor financials

Offshore to nearshore

The structure of compliance teams is also changing. Large offshore teams once handled first-pass reviews of alerts, but these roles may disappear if AI takes over triage. Instead of reviewing thousands of false positives, human analysts may be able to focus on a smaller, higher-quality set of alerts. As one compliance executive put it, he hopes that "instead of 5,000 false positives, we (will) get 200 alerts that deserve the attention of (a few) very talented human reviewers."

Nearshoring may also grow as firms shift toward smaller but more skilled teams located closer to headquarters, where regulatory alignment and data security can be better controlled. This suggests that roles themselves may evolve from fewer entry-level analysts to more data scientists, model governance specialists, and investigators capable of handling nuanced misconduct cases. The era of solving compliance challenges by throwing bodies at the problem is fading away.

Looking Forward to 2027

The next few years will likely be defined less by new regulations and more by how firms adapt to the changing enforcement and technology environment. US regulators will continue to set the pace, with steady enforcement and a sharpened focus on cooperation. Globally, fragmentation will deepen, forcing institutions to design region-specific frameworks rather than rely on a single global standard. Crypto and digital assets will remain a flashpoint, expanding the scope of surveillance and testing firms' ability to extend controls to new markets.

Technology choices will be decisive. Cloud remains attractive, but sovereignty and security concerns make hybrid models and data transfer strategies essential. Recent breaches underscored how fragile over-reliance can be. AI, meanwhile, is expected. Its value lies in reducing false positives, improving investigations, and freeing staff for higher-order analysis, but only when paired with strong governance and human oversight.

This authorized reprint has been prepared for Arctera.
For more information, please reach out at info@opimas.com.

About Arctera

Arctera, a business unit of Cloud Software Group, is the leading global provider of compliance and governance solutions that enable firms to unleash game-changing technologies into their organizations while minimizing risk. Created in 2024 from Veritas Technologies, Arctera helps the biggest companies in the world monitor and control exactly how their information is being accessed, used and shared. The Arctera Insight Platform is able to capture data from over 130+ different content sources, and more than 280 AI policies help firms streamline compliance and adapt to evolving regulations.

About Arctera

Arctera, a business unit of Cloud Software Group, is the leading global provider of compliance and governance solutions that enable firms to unleash game-changing technologies into their organizations while minimizing risk. Created in 2024 from Veritas Technologies, Arctera helps the biggest companies in the world monitor and control exactly how their information is being accessed, used and shared. The Arctera Insight Platform is able to capture data from over 130+ different content sources, and more than 280 AI policies help firms streamline compliance and adapt to evolving regulations.

Learn more: arctera.com
Connect:
Contact: press@arctera.com

A0090 11/25