The Definitive Guide to Modern Trade and Communications Compliance

NICE · ACTIMIZE

This authorized reprint was prepared for NICE Actimize.
For more information, please reach out at info@opimas.com.

Anna Griem

June 2022

TABLE OF CONTENTS

INTRODUCTION

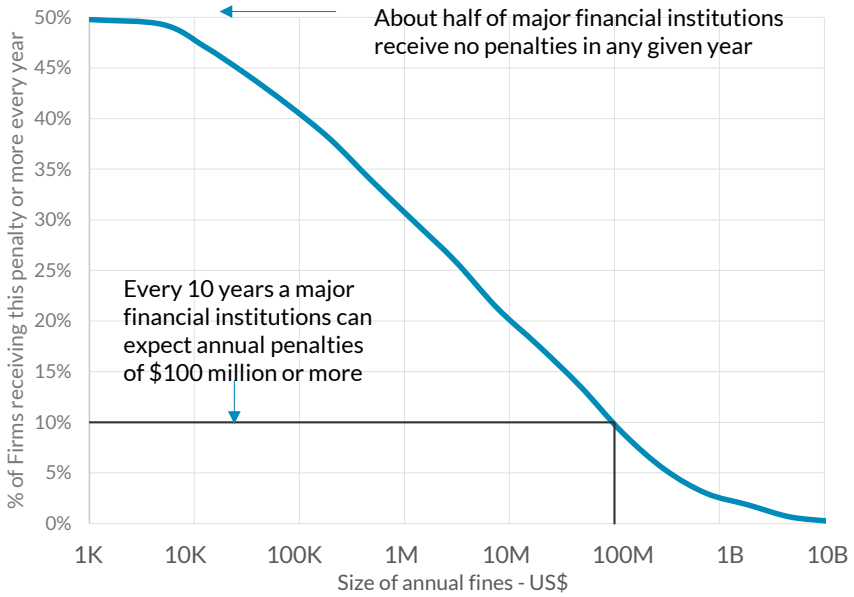
Designed to be a guide for individuals responsible for their firm's compliance program, this report spotlights the pivotal issues related to trade and communications surveillance today. This research includes an assessment of the cost of violations to financial institutions, shares the problem zones that are top of mind for compliance teams, and grades the performance of financial services firms across six key elements of successful programs, including:

1. Regional configurability
2. Accurate alert generation
3. Automation wherever possible
4. Thorough and efficient investigations
5. Capture coverage
6. Technical agility

Findings shared in this report have been collated from Opimas' discussions with over 200 financial institutions regarding their compliance programs and priorities over the past year.

FINE EXPECTATIONS

FIGURE 1. PERCENTAGE OF FINES IN THE UNITED STATES, BY SIZE IN USD



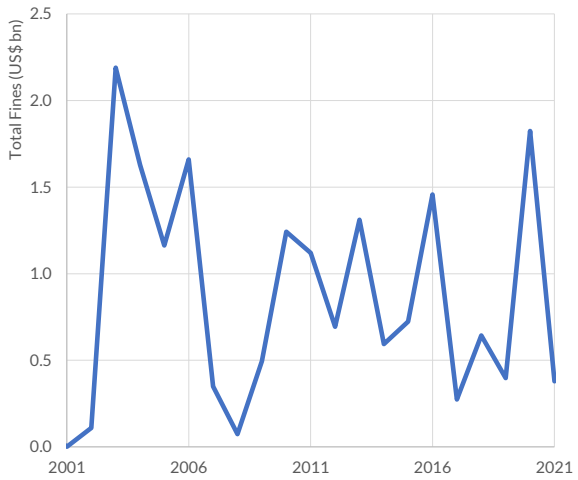
Source: Regulators, Good Jobs First. Opimas analysis

Many financial conduct infractions that receive regulatory attention are met with fines as low as US$5k and nearly half of all financial institutions receive no penalties in any given year. But financial services firms are right not to be too optimistic in assessing their odds.

Caution is sensible because a significant portion of fines for misconduct in financial services reach eyewatering amounts. At the extremes, penalties extend into the billions. In fact, *every 10 years, a major financial institution can expect annual penalties of $100 million or more - just from US regulatory and judicial bodies.*

A global total for fines issued is difficult to pin down due to varied categorization standards between jurisdictions, but Opimas estimates that the United States is at the root of nearly half of total fines issued for financial crimes globally, suggesting that fine totals regularly hit $10bn annually.

FIGURE 2. TOTAL FINES – SEC



Source: SEC, Good Jobs First, Opimas analysis

Global regulators eased up a bit on fines handed out in 2021 compared to the year before. At the Securities and Exchange Commission (SEC) this downshift was also noted (Figure 2). The likeliest explanation for this slowdown is quite simple and no cause for optimism. Due to the severe global response to the pandemic, many regulatory investigations stalled, resulting in fewer enforcement notices and fines. In outbound communications, regulators have promised to make up for lost time.

Germany's BaFin (Federal Financial Supervisory Authority) stated that *"starting in 2022, BaFin will assume sole responsibility for financial reporting enforcement. We will be sending twice as many staff members into action as in the two predecessor teams put together: approximately 60 employees will be working in BaFin's financial reporting enforcement directorate. All in the interests of ensuring a clean capital market."*

Similarly, the United Kingdom's Financial Conduct Authority (FCA) wrote in an outbound email that it would rev up its efforts. *"Since (last year), we are being tougher on firms who want authorisation to operate in the UK, using data more systematically to ask the firms we supervise more rigorous questions and using our enforcement and intervention powers more actively, pushing the boundaries where we need to."*

The United States is taking the same path, with the SEC proclaiming its readiness with *"we're good to rock and roll (into 2022)."*

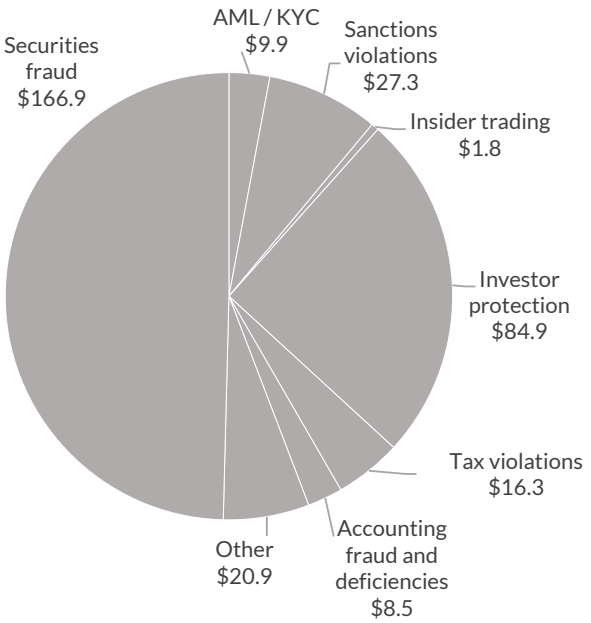
The message is consistent regardless of jurisdiction.

PENALTY TYPES

About half of the fines that have been issued to financial institutions by US regulators and judicial bodies since the year 2000 were attributed to various types of securities fraud, though there are several other categories of infractions that have received stiff punishments. Trade and communications surveillance programs are particularly useful for detecting and preventing several of these violations, including AML / KYC, sanctions violations, market abuse / insider trading, and other investor protection issues.

In addition to these traditional areas of financial misconduct, firms are aware of further exposure to penalties and reputational damages due to other types of misbehavior, including harassment and discrimination scenarios.

FIGURE 3. TYPES OF FINANCIAL OFFENSES IN THE UNITED STATES SINCE 2000 BY TOTAL PENALTIES ISSUED (USD BILLIONS)

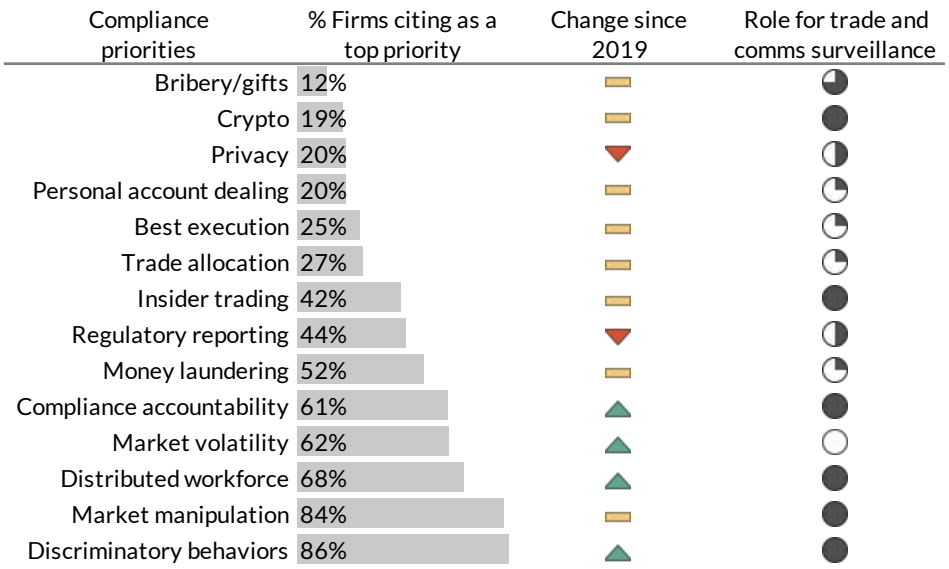


Total 2000 to present: $336.5 bn

Source: Regulators, Good Jobs First, Opimas analysis

TOP PRIORITIES IN COMPLIANCE

FIGURE 4. SURVEILLANCE ESSENTIAL FOR MANY COMPLIANCE PRIORITIES IN 2022



Source: Opimas analysis. Interviews with over 200 financial institutions

In addition to the traditional priorities for compliance teams, novel concerns have jutted to the top of the list. Firms appear to be concerned about appropriately monitoring distributed workforces, preventing discriminatory and harassing behaviors, and establishing protocols to ensure compliance procedures and teams themselves are regularly tested and held accountable. Careful surveillance can play a pivotal role in helping compliance officers achieve their goals.

Compliance teams also expressed concern, echoed by regulators, about geopolitical uncertainty and potential market volatility. Changing market patterns can create uncertainty and potentially obscure avenues by which bad actors might try to manipulate the market. Data volumes are also less predictable in volatile conditions, potentially requiring rapid adjustments to surveillance efforts.

Surveillance teams appear not to be too preoccupied with crypto for the time being, likely because traditional financial services have yet to enter this asset class en masse. This is despite the hype and a handful of painful fines - crypto-trading platform, BitMEX and crypto payments solution Bitpay, fielded multimillion-dollar fines for neglecting money laundering obligations.

However, as noted in Opimas report "Crypto Infrastructure Solution Landscape", even crypto players have made significant investments in RegTech, with spending on AML / KYC and surveillance solutions doubling over the last year.

Even if traditional institutions continue to avoid crypto, it is likely that compliance officers and investigation managers familiar with regulators and surveillance tools will get poached by crypto firms desperate to legitimize themselves to regulators.

Surprisingly, privacy regulations like the General Data Protection Regulation (GDPR) appear to be deprioritized despite the draconian potential fine schedule for infractions. However, if even a single big fine is issued, this will quickly change.

WHAT MODERN SURVEILLANCE PROGRAMS MUST CONSIDER

With increased regulatory requirements and penalties over the past decade, financial institutions have long ago abandoned what were once rather lackadaisical approaches to compliance.

Still, with piecemeal supervisory requirements added year after year, and technological capabilities playing catch-up, many compliance efforts are far from in their ideal state. While the sell side tends to outperform the buy side and larger institutions tend to have invested more than their smaller counterparts, important gaps remain everywhere across key trade and communications surveillance programs elements. In Figure 5 and in the following sections, firms are invited to compare how peers self-evaluate and identify where opportunities for improvement can still be found.

FIGURE 5. PERCENTAGE OF FIRMS ACHIEVING IDEAL STATE

	Broker-Dealers - Tier I Present as clearing member or primary dealer in at least 10 markets globally	Broker-Dealers - Tier II Present as clearing member or primary dealers in 4 - 9 markets globally	Broker-Dealers - Small Other broker dealers	Asset Managers - Tier I Assets under management >$250bn	Asset Managers - Tier II Assets under management $25-250bn	Asset Managers - Small Assets under management <$25bn
#	30	450	7,000	70	250	9,000
Regional configurability	85%	76%	76%	70%	50%	33%
Accurate alert generation	45%	42%	30%	40%	32%	20%
Automation wherever possible	60%	50%	45%	58%	48%	32%
Thorough and efficient investigations	65%	40%	28%	45%	32%	8%
Capture coverage	85%	74%	68%	82%	72%	58%
Technical agility	65%	60%	55%	25%	18%	10%

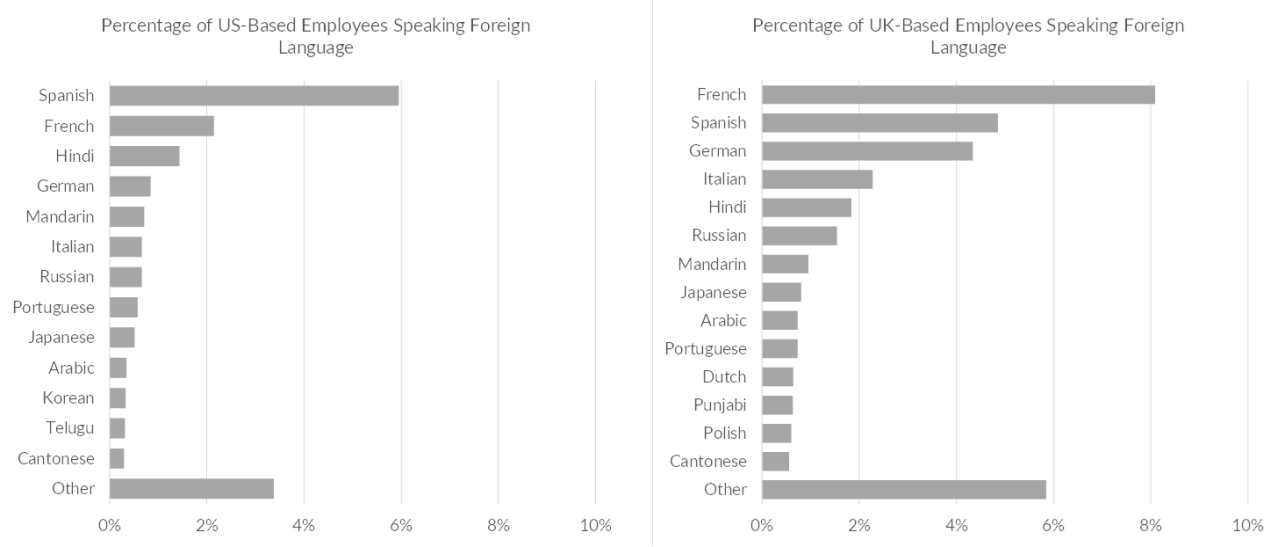
Source: Opimas analysis. Interviews with over 200 financial institutions

REGIONAL CONFIGURABILITY

Every jurisdiction has distinct requirements, which firms must carefully mind and ensure their surveillance programs are flexible enough to manage. Common problem zones include varied prioritization of privacy versus retention, different definitions of real-time or T+1 trade monitoring, and even capabilities for surveilling a multilingual workforce. While the largest broker dealers have made significant efforts to address their firm's global needs, problems persist.

Even at the worlds' largest sell-side institutions, only 25% of firms interviewed expressed satisfaction with the automation of their surveillance across multiple languages. This is problematic given how common it is within financial services for employees to be multilingual, even in mostly English-speaking countries (see Figure 6). This invites the risk that conversations cannot be fully monitored if conducted in another language.

FIGURE 6. LANGUAGE SURVEILLANCE UNDERSCORES GAP IN GLOBAL COVERAGE



Source: Opimas analysis. LinkedIn

ACCURATE ALERT GENERATION

Most firms rely on rules and lexicon-based methodologies to create the alerts that are reviewed by compliance teams. Many firms even conduct only manual searches of archives during active investigations, and don't do much that would be considered proactive. Tuning these alerts to a useful level requires careful navigation of languages, trader jargon, etc. as well as tailored asset-class-specific strategies and navigation of market conditions in trade surveillance. Even with careful construction, the alerts can be wildly useless and even counterproductive.

Very few firms are satisfied with the quality of the alerts they produce. Firms striving for the best possible surveillance results, and a manageable number of alerts, should carefully combine classic lexicons, metadata, trade and order information, as well as more cutting-edge techniques that enable language identification, entity recognition, sentiment analysis, noise deduping, topic identification, clustering, and more.

Supervised and unsupervised machine learning should be applied to better categorize communications and trading activity that warrant attention, helping to save time. These techniques can also be used to implement a system of scoring alerts for riskiness, which can further help to prioritize investigations for analysts.

However, artificial intelligence and natural language processing (NLP) approaches, while full of potential, are often held back for a few reasons. In addition to some of the underlying technologies not yet being fit for service, they are often built on limited training data that must be kept private and require extensive personalization for each use case. This often makes the scaling of these advanced approaches across multiple firms quite difficult.

Modern models are becoming increasingly effective with less training data. Additionally, ML can be used to learn which messages are not business-related and suppress these alerts. Automating the classification of disclaimers and exclusion lists, and swerving marketing messages also improves the efficiency of a surveillance program and simplifies the management thereof.

Sophisticated models can also help deepen understanding of an individual's behavior and communication habits – enabling a surveillance analyst to recognize changes, increase the risk scoring of the employee, and heighten surveillance when appropriate.

Ensuring alerting methodologies are tailor made for particular asset classes and instrument types, and not relying only on rules-based alerts, is essential to reducing time-consuming false positives. Applying the same rules to examine equities and bonds, for instance, produces a deafening number of false positives.

Equally important, alerts should take the entire trading activity into account – several market abuse scenarios are not apparent when monitoring a single asset class individually. This is particularly difficult to achieve at institutions where alerts are managed by separate trade surveillance platforms.

The best surveillance solutions leverage all techniques discussed above to gain a comprehensive understanding of an activity, resulting in a more accurate risk assessment with less time-wasting alerts and improved detection of suspicious patterns.

AUTOMATION WHEREVER POSSIBLE

To optimize investigation managers' user experience and the soundness of surveillance efforts, a program ideally makes use of automation everywhere possible, including at least for:

- Checks of recording and surveillance systems to make sure they remain operational
- Workflow improvements
- Investigation thoroughness
- Language transcription and translation
- Data visualization and configurable dashboards
- Trade reconstruction
- Regulatory reporting requirements

Only 60% of the world's largest sell-side firms report achieving a meaningful degree of automation across their surveillance programs, leaving considerable room for improvement.

THOROUGH AND EFFICIENT INVESTIGATIONS

Very few financial institutions feel they expertly manage their investigations. In fact, only 8% of smaller asset managers describe having efficient investigation processes in place following detection of a suspicious activity. The majority take a very passive approach. Many firms admit to relying overwhelmingly on man-hours when required to investigate a suspicious event or alert in detail. This is far from the ideal state, which would seek to efficiently automate the process of creating a

single alert/timeline of the full event that took place, including all relevant information across trading, communication, and market activity data.

For all the complaints that are heard about poor quality alert generation, less attention has been paid to what is done to properly investigate an alert and document decisions made along the way. The end goal for compliance teams is to finetune detection of suspicious activity, and then triage investigations as efficiently and repeatably as possible. Few are currently at this stage.

Regulations have also served as the impetus for getting ones house in order. The Markets in Financial Instruments Directive II (MiFID II) demands that all pre-, at, and post-trade data, including related text and voice communications, be stored in an immutable, but retrievable format for at least 5 years. Retrievability is key to meeting these requirements. One approach is to store all required data in a single repository or data lake, overlaid with search capabilities to allow ad hoc retrieval in response to regulatory requests. But this is not a trivial exercise, and requires consistent indexing of recorded data to transactions, linking together voice messages, SMS, IM, Skype, and all other required channels.

Even where an institution's surveillance efforts are siloed, it is a regulatory requirement to be able to produce this comprehensive report in short order. Institutions able to automate trade reconstruction reports in a timely manner can make use of these throughout daily investigations. Those who continue to rely on manual, people-intensive assembly, will struggle.

COMPLETE DATA CAPTURE

Some of the data sources that must be recorded or captured for surveillance purposes include: the company's archiving systems, eComms (email, chat, etc.), aComms (fixed line, turrets, VoIP, etc.), collaboration tools (OneDrive, GoogleDrive, Sharepoint, etc.), unified communications (Microsoft Teams, Zoom), structured data (trade and orders, market data, employee, control room, etc.), mobile (SMS & voice), over-the-top (OTT) chat and voice apps like WhatsApp and WeChat, social platforms, video communications, and management of files shared as attachments.

Many firms also suffer from poor quality recordings, where voice files become distorted following compression.

Remote working has especially driven an increased adoption of collaboration tools and video communications. In parallel, use of OTT chat and voice apps like WeChat and WhatsApp have also become more commonly requested for use at work.

The trade side is no less complicated, with the addition of market data being essential for different asset classes. In addition to the complexity of managing the data, making use of market data for surveillance efforts often comes with an additional fee.

These channels are not at all straightforward to comprehensively capture or to monitor without losing their native significance and drowning the analyst in distractions.

While most firms report feeling reasonably confident that they are recording and capturing the bare minimum of what is required, few feel they have a closed loop entirely. Many firms still rely on policies of managing complicated to record communication channels by banning their use, a practice deployed with decreasing confidence following the $125mn fine given to JP Morgan for failure to capture and preserve WhatsApp communications and personal email messages.

TECHNICAL AGILITY

Programs are particularly effective when interaction is possible across otherwise siloed data streams and business systems, including active directories, trade and order data, case management systems, eDiscovery systems, personal account dealing, gifts and entertainment, insider and restricted lists, badge logs, and more. Surveillance programs built with technical agility and openness to integration will best allow users to adapt to changing requirements moving forward.

Additionally, customizable detection logic allows firms to better tune alerts, but also track market, business, and regulatory changes that must be kept abreast of.

Deployment flexibility is also key, with the Cloud enabling more agile model development and updates, and rapid unfurling of new capabilities. Cloud has the added advantages of reducing server footprint, making rapid scaling possible, and allowing the centralization of management of recorder estates, etc.

Siloed infrastructure is a particular problem for buy-side players, with only 25% of the biggest asset managers claiming to have the above-described technical integration and built-in flexibility.

FINAL THOUGHTS

While communications capture, trade, and communications surveillance solutions have come leaps and bounds in the last five or six years, compliance teams still struggle with gaps in coverage, inaccurate alerts, disjointed investigations, and siloed and inflexible systems.

With the damages that can be expected from regulatory penalties and reputational costs, improving surveillance efforts as much as possible is essential. Compliance teams should feel encouraged to think big picture about how to improve record retention and surveillance efforts, including by radically integrating systems.

About the Report's Author

Anna Griem is a senior analyst in Opimas' equities trading practice and has published reports on a variety of topics related to surveillance and regulatory technologies.

About Opimas

Opimas is a management consultancy focused on capital markets, serving leading financial institutions around the world. Our specialisation allows us to bring our expertise to bear from the very beginning of projects, to provide insight and craft strategies for our clients more quickly, without sacrificing quality. In addition, Opimas continuously invests considerable resources, representing about one third of our revenues, in market research. This investment allows us to create a pool of intellectual capital on issues of strategic importance to our clients.

Uniquely in the consulting industry, Opimas pursues an entirely open approach to knowledge sharing, providing our clients direct access to our entire pool of intellectual capital. This gives our clients the latitude either to support their strategic decisions independently, while relying on our knowledge base, or to engage directly with our consultants on a project basis.

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers' and investors' assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.