Regulatory brief

April 2018

A publication of PwC's financial services regulatory practice

RegTech: The future of market abuse surveillance

Market abuse, such as insider dealing, price fixing, and front running, has long plagued the financial services industry, often resulting in enforcement actions and fines. Regulators have responded by requiring firms to monitor for indicators of market abuse in employee trading activity, electronic communications (e.g., emails, chats, text messages), voice communications, and security logs.

Firms have reacted by implementing targeted solutions that address specific areas of surveillance in largely separate systems. While these actions have covered the immediate regulatory requirements, they have resulted in siloed and fragmented activity among compliance departments, which has in turn resulted in firms not having a full picture of their risks.

Although the common perception is that regulation is now on the decline, it is not expected that market integrity enforcement will slow down. In fact, in recent years, regulators have increasingly focused on leveraging new technologies[1] to identify potential misconduct and firms should anticipate that regulators will expect the same of them.

Firms can respond to these regulatory expectations as well as address gaps in their surveillance programs by taking advantage of a wave of new regulatory technologies, or RegTechs, that have been flourishing in the market abuse surveillance space. Although many of the RegTech solutions are still new and not yet scaled, their growth is creating new opportunities for firms to rethink and optimize their surveillance systems and processes.

This **Regulatory brief** outlines challenges in market abuse surveillance and trends in regulatory technology that can help address them.

pwc

What are the current challenges?

At most institutions, market abuse surveillance systems and functionalities were implemented tactically in an effort to address regulatory changes or enforcement actions, resulting in siloed systems that do not provide a full picture of trade behavior. For example, there are solutions that focus solely on analyzing trade transactions, while others look only at electronic communications. However, using one or both of these solutions independently does not provide a holistic view and therefore runs the risk of missing signs of market abuse.

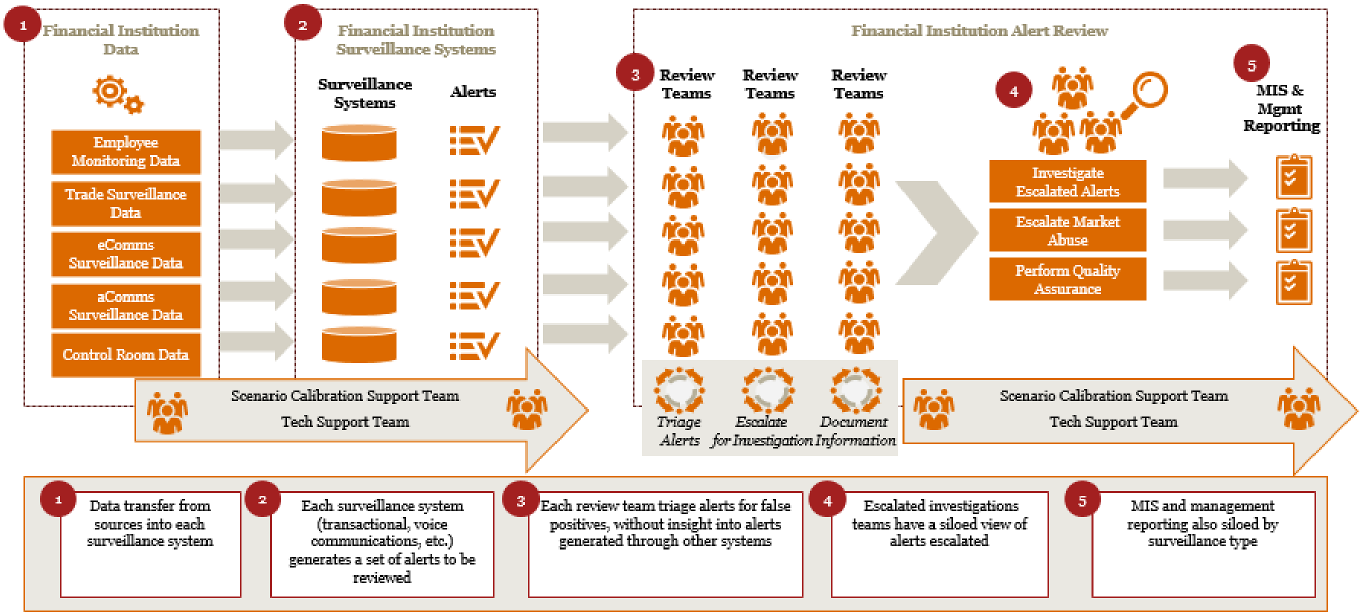
Despite the risks, using independent solutions for different forms of data is currently the norm. In fact, 70% of respondents to a PwC market abuse surveillance survey[2] are using three or more software vendors to execute their surveillance requirements and 75% are unable to review trade alerts alongside contemporaneous electronic communications or voice alerts. Further, alerts generated by multiple systems are typically reviewed manually by separate compliance teams that do not have easy access to each other's information. Such dispersion impedes firms from having a true 360° view of employee behavior and limits the ability to stay ahead of emerging risks.

Adding to the problem, data volumes and sources have also been increasing as the methods that traders use to communicate on a daily basis – from cell phones to chat apps to social media – continue to diversify. Communications surveillance also typically uses lexicon-based search techniques (i.e., those looking for specific words and spellings), which tend to produce high volumes of false positives and potentially miss true suspicious behavior.

Finally, there are challenges associated with high volumes of false positives,[3] some stemming from legacy systems and scenarios (also known as models or rules), which may not be calibrated with the current business landscape and risks. For example, a scenario aimed at looking for spoofing activity may be running with a transactions threshold that may be too low for the current business volume, causing a large number of transactions to alert.

All of these factors prevent effective risk management and drive up the cost and time spent on market abuse surveillance.

Current market surveillance landscape



1 Data transfer from sources into each surveillance system

2 Each surveillance system (transactional, voice communications, etc.) generates a set of alerts to be reviewed

3 Each review team triage alerts for false positives, without insight into alerts generated through other systems

4 Escalated investigations teams have a siloed view of alerts escalated

5 MIS and management reporting also siloed by surveillance type

Currently, surveillance systems focus on separate areas. This results in having multiple systems generating alerts that need to be reviewed by separate teams, each only having access to a narrow data set. This model is inefficient and costly, especially for larger firms

How can RegTech help?

The market abuse surveillance space is one of the fastest growing areas for RegTech innovation. New solutions are using natural language processors (NLP)[4] to enhance communication surveillance as well as machine learning[5] and other artificial intelligence (AI) techniques to improve identification of suspicious activity. Further, cloud technology is emerging as a cost-effective storage solution for increasing volumes of surveillance data[6] these solutions are already showing promise in helping to reduce false positives, centralize firms' surveillance activities, and reduce the burden on investigators.

RegTech advancements can help solve longstanding surveillance pain points and provide the following benefits:

Provide a holistic view: In contrast to siloed systems covering different types of activity or communications, RegTech solutions can be used to consolidate information and give a comprehensive view of all employee activities, independent of what source system originated the data point or alert. Such solutions can help create a view of each employee's risk by looking at multiple factors such as building access, system use, conversations, compliance with training or mandatory time away requirements, and trade activity. RegTech solutions can also provide a more comprehensive view of the circumstances related to a single trade event, such as relevant emails or conversations, and allow alert reviewers to more quickly see the full picture. Ultimately, the goal is to achieve holistic surveillance that can generate alerts based on a combined repository of activity that spans products, channels and communications streams.

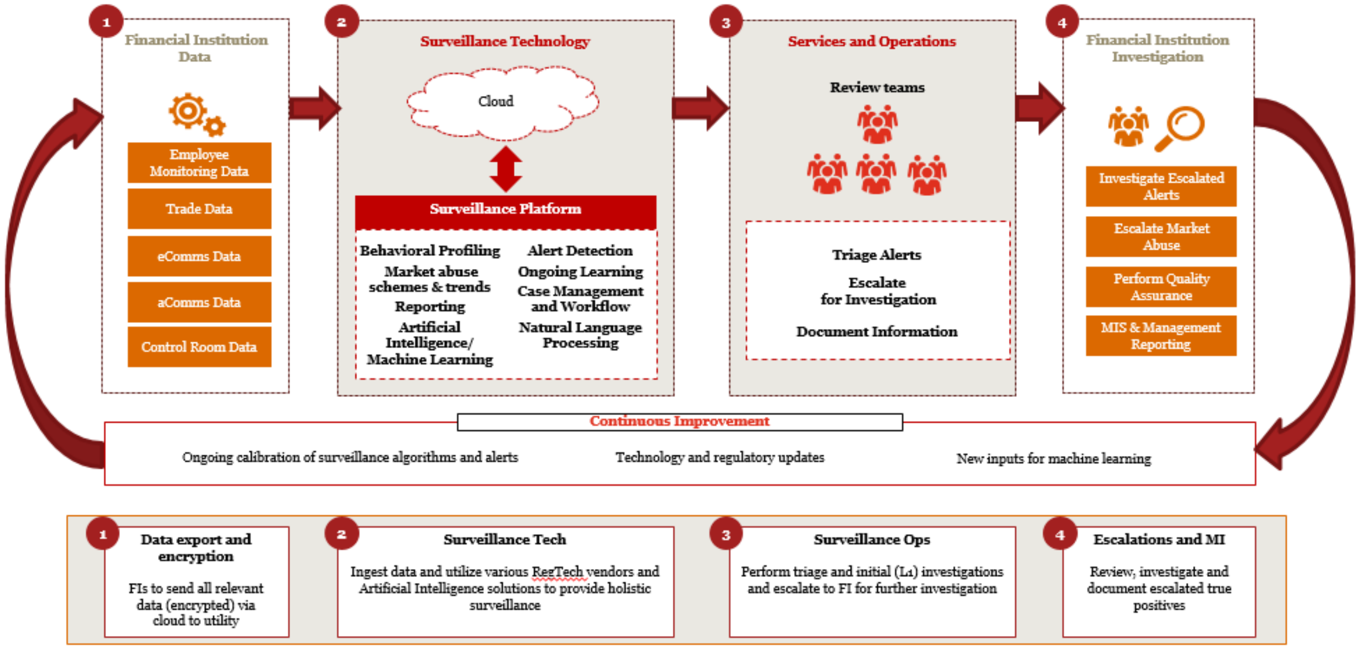
Better identify unusual patterns or trends through behavioral profiling: Emerging solutions can improve behavior monitoring by leveraging machine learning and AI to identify unusual patterns and trends in employee transactions or communications. These technologies have a particular advantage in identifying non-obvious connections between individuals, entities, and events. For example, there are surveillance tools that allow reviewers to see the closeness, frequency, and relevance of links between individuals based on historical communication patterns.

Reduce rate of false positives through more accurate alerts: By creating smarter alerts, RegTech solutions can help to reduce the rate of false positives generated by existing solutions. As described above, one way they do so is by better consolidating and analyzing data points related to a single event. In addition, new solutions are leveraging NLP instead of just using traditional lexicon-based searches in efforts to better analyze communications. Whereas lexicon-based searches do not take into account the context in which the keywords appear, NLP can better derive the meaning behind communications by taking into account factors such as relationships between words and emotive tone.

Provide continuous improvements to accuracy: Firms can use the results of RegTech-based alerts and corresponding investigations to modify solutions according to the validity of the alerts they generate in order to continually improve accuracy. Some RegTechs are already using machine learning techniques to refine alert thresholds and parameters (i.e., automatic calibration), gradually reducing the total volume of false alerts while still capturing activity that should be further investigated. This not only reduces the time spent investigating false positives but also the time needed to manually re-evaluate scenarios and alert parameters.

Redirect resources to higher value-add activities: When the labor intensive review process is reduced as alerts are refined and surveillance systems are consolidated, firms can shift their surveillance teams' focus to more valuable risk management activities. In particular, teams can direct attention away from isolated alert reviews to employee risk profiling analysis, where all employee dimensions and related events are analyzed holistically. They can thereby better assess trends and implement broader solutions to help prevent market abuse.

Future market surveillance landscape



1 Financial Institution Data
- Employee Monitoring Data
- Trade Data
- eComms Data
- aComms Data
- Control Room Data

2 Surveillance Technology

Cloud

Surveillance Platform

Behavioral Profiling
Market abuse schemes & trends
Reporting
Artificial Intelligence/ Machine Learning

Alert Detection
Ongoing Learning
Case Management and Workflow
Natural Language Processing

3 Services and Operations

Review teams

Triage Alerts
Escalate for Investigation
Document Information

4 Financial Institution Investigation
- Investigate Escalated Alerts
- Escalate Market Abuse
- Perform Quality Assurance
- MIS & Management Reporting

Continuous Improvement

Ongoing calibration of surveillance algorithms and alerts

Technology and regulatory updates

New inputs for machine learning

1 Data export and encryption

FIs to send all relevant data (encrypted) via cloud to utility

2 Surveillance Tech

Ingest data and utilize various RegTech vendors and Artificial Intelligence solutions to provide holistic surveillance

3 Surveillance Ops

Perform triage and initial (L1) investigations and escalate to FI for further investigation

4 Escalations and MI

Review, investigate and document escalated true positives

The future of market surveillance will include consolidated data stored in the cloud, smarter alerts, and continuous updates to improve accuracy. This will allow surveillance teams to have a more holistic view of their organizations and perform more forward-looking risk management.

What should firms do next?

Given the potential for more accurate and comprehensive surveillance at lower cost, emerging RegTech solutions are an attractive replacement for existing systems and processes. The road ahead, however, will be bumpy with challenges surfacing from integrating legacy systems, regulatory changes, and risks associated with new companies and technologies. As firms get ready for RegTech,[7] they must go through an extensive process of evaluating their current systems and identifying potential solutions, and then conducting due diligence and thorough testing before fully implementing.

In terms of early actions, firms should be looking at their existing processes, systems, and controls to identify gaps, inefficiencies, and opportunities to improve their surveillance program. Firms can then begin preemptively reorganizing, training, and realigning their teams to prepare for more technology-oriented processes. As they are conducting this evaluation and reorganization, firms should develop and monitor productivity metrics to facilitate better management of resources and testing of potential RegTech solutions.

As firms then begin to research RegTech solutions, they will find that it is not easy to identify suitable candidates due to the high volume of choice available and the relative nascence of some RegTechs. While the anti-money laundering space initially dominated the RegTech landscape, the last several years have seen a substantial shift in the market abuse surveillance solution landscape, with some technology companies sunsetting their products, some legacy vendors using new technology in an attempt to achieve better results, and others joining partnerships or making acquisitions.

Ultimately, firms may consider outsourcing some of their surveillance functions, such as initial alert review, documentation, and disposition. It is also possible that the surveillance function will move to a utility model, where both technology and operations will be provided by third parties to a number of firms on a subscription basis.

Despite the challenges and uncertainty around transitioning to alternative solutions, firms should begin to understand the new technologies and how they can improve not only their current market abuse surveillance programs, but create a more holistic risk management program for the future.

Endnotes

1. For example, the Securities and Exchange Commission has mandated the development of the Consolidated Audit Trail, which will be one of the world's largest data repositories that will contain a complete record of all equities and options traded in the US. For more information, see PwC's *Regulatory brief, Consolidated audit trail: the CAT's out of the bag* (June 2016).
2. See PwC's *2016 Market Abuse Surveillance results.*
3. In market abuse surveillance, false positives refer to events (e.g.: transactions, communications) that were incorrectly classified by a surveillance system as high-risk, generating a false alert/notification of suspicious activity.
4. Natural Language Processing refers to a computer's ability to understand written and spoken language.
5. Machine Learning refers to the ability of computers to learn a task that it is not specifically programmed for by identifying patterns in data and applying what it has learned from that data to new data or to draw inferences from datasets.
6. See PwC's *Financial services digital publication, Get your head in the cloud* (August 2016).
7. See PwC's *FS tech publication, Get ready for RegTech* (October 2017).

Additional information

For additional information about this **Regulatory brief** or PwC’s Financial Services Regulatory Practice, please contact:

Dan Ryan
Banking and Capital Markets Leader
646 471 8488
daniel.ryan@pwc.com
@DanRyanWallSt

Adam Gilbert
Financial Services Advisory Regulatory Leader
646 471 5806
adam.gilbert@pwc.com

David Choi
US RegTech Leader
646 471 6748
david.d.choi@pwc.com

Roberto Rodriguez
Director of Regulatory Strategy
646 471 2604
roberto.j.rodriguez@pwc.com

Julien Courbe
US Financial Services Advisory Leader
646 471 4771
julien.courbe@pwc.com
@juliencourbe

Mike Alix
Financial Services Advisory Risk Leader
646 471 3724
mike.alix@pwc.com

Frank Badalamenti
US Financial Crimes Unit Principal
646 818 7158
frank.badalamenti@pwc.com

Contributing authors: Grace Vogel, Diana Moutela, and Douglas Turitto.

To learn more about financial services regulation from your iPad or iPhone, click here to download PwC’s Regulatory Navigator App from the Apple App Store.

Follow us on Twitter @PwC_FinServ

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. PwC US helps organizations and individuals create the value they’re looking for. We’re a member of the PwC network of firms in 157 countries with more than 223,000 people. We’re committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com/us.