ACA COMPLIANCE GROUP

Best Practices for Implementing a Holistic Surveillance Program

INTRODUCTION

You probably remember "connect the dots" worksheets from when you were a child. A page filled with tiny number dots in a mysterious shape that only revealed itself when you drew a line from one dot to another.

This is the same type of activity that financial services firms need to be doing today to effectively detect, prevent, and remediate potential misconduct within their own operations. With the sheer amount of data generated each day — from trading and market data, to electronic communications and calls with experts, to employees' own personal trading activities and business dealings, the chance of missing potential risk is high if the right connections aren't made among all the relevant data points at play.

While most firms invest significant resources in developing sound compliance programs, their efforts may be siloed, or focused on each individual data point in a way that prevents seeing a complete picture of activity and behavior. In other words, a firm may have mechanisms in place to catch potential issues in specific areas, but it may not have the ability – or the resources in-house – to catch the web of more complex problems that can only be seen after piecing together multiple data points.

That's where connecting the dots comes in, and it's what holistic surveillance can do when used properly and as intended.

This white paper will discuss:

- what holistic surveillance is — and isn't
- why holistic surveillance matters
- the benefits of holistic surveillance
- how to build a holistic surveillance program
- what are the valuable components of a holistic surveillance program
- peer insights to help your firm benchmark its approach to compliance and surveillance

TABLE OF CONTENTS

WHAT IS — AND ISN'T — HOLISTIC SURVEILLANCE?

"Holistic surveillance" is a phrase that is often used without a proper understanding of what it means. It is frequently used synonymously with automated surveillance, when in fact purely automated surveillance can miss a lot and is anything but "holistic."

True holistic surveillance is a combination of technology and human expertise that takes structured and unstructured data from multiple sources, connects the data points, runs sophisticated analytics using technology, and has dedicated surveillance analysts that review and investigate the results.

At its core, holistic surveillance looks across previously uncorrelated data sets to uncover activity that a bad actor wishes to remain hidden. For example, a reasonably profitable personal trade may not raise a red flag on its own, but when paired with a meeting with that company in the prior week, it could. And while a trade surveillance system alone may not flag that risk, a holistic surveillance program that is analyzing both structured and unstructured data (trades, calendars, meetings, and more), would.

WHY DOES HOLISTIC SURVEILLANCE MATTER?

No firm wants to be the last to know about market abuse among employees — many firms fear that regulators have more information than their compliance teams.

Regulators globally continue to focus on identifying and punishing insider trading and other misconduct, and they are investing in developing and improving their own technology and data analytics capabilities to support this priority.

Regulators can now process market data faster and more efficiently than ever to uncover market abuse and other financial crime. For example:

- The SEC's National Exam Analytics Tool (NEAT), which enables examiners to crunch large volumes of trading data, now supports blotter data validations, anti-money laundering, options, and reviews of broker-dealer information.
- The SEC's Market Information Data Analytics System (MIDAS) is also used for reviewing specific market activities.
- The FCA's Market Data Processor (MDP) System, which is the mechanism by which the FCA receives market data types including daily transaction reports, presents the FCA with the opportunity to interrogate trading records for suspicious activities.
- The MDP also interfaces with the European Securities and Markets Authority's (ESMA) Transaction reporting exchange mechanism (TREM), which allows the FCA to exchange transaction reports with other National Competency Authorities (NCAs) to allow their own surveillance activities to occur.

> **"No firm wants to be the last to know about market abuse among employees — many firms fear that regulators have more information than their compliance teams."**

With this level of technological and analytical sophistication in the hands of the regulators, firms need to be more proactive than ever in identifying potential problems before the regulator does. Add to this the regulators' expectation that compliance professionals should supplement their expertise with surveillance technology, and compliance teams around the globe are feeling the pressure to keep pace.

This is one area where the regulators may be ahead of most in the industry.

Implementing a holistic surveillance program can help.

THE BENEFITS OF HOLISTIC SURVEILLANCE

The benefits of holistic surveillance are many:

- to provide a comprehensive, top-level view of activity and behavior across your firm
- to increase operational efficiency by incorporating technology
- to augment and provide support to your firm's compliance team by outsourcing time-consuming and otherwise manual day-to-day tasks
- to get the deep analysis and critical element that only human expertise can provide
- to help mitigate actual and perceived risk through targeted monitoring, surveillance, and forensic testing of your firm's compliance program
- to help ensure your firm is meeting today's broader and deeper regulatory obligations

BUILDING A HOLISTIC SURVEILLANCE PROGRAM

The framework for a holistic surveillance program generally includes the following steps:

Step 1: Conduct an initial risk assessment

To begin building any surveillance program, your firm must first assess the risks it is trying to detect. These may depend on your firm's size, complexity of business, investment model/strategies, and regulatory geography and climate.

For example, in the United States, firms registered with the SEC are required to monitor for rule 206(4)-7 violations and have adequate policies and procedures in place to prevent the violation of federal securities laws. Firms licensed with the UK's Financial Conduct Authority ("FCA") have the market abuse regulation ("MAR"), which has increased the amount of possible activities that investment management firms must detect. Once the risks are understood, your firm's compliance team can begin to focus on the specific activities that bear the most risk.

For example, "bottoms up" fundamental traders will face more scrutiny over the misuse of material non-public information ("MNPI") if they meet with experts or issuers, versus a quantitative trading shop where concerns would primarily lie with manipulation of underlying data or models. Firms that do not trade, e.g., private equity managers, must monitor employees' personal trading in ways that suggest profits could be accrued from information gained due to a wall crossing, or to identify cases where they might have traded on information related to a public-to-private buyout or public company acquisition or divestiture.

Step 2: Aggregate and optimize the data

After the initial risk assessment, you need to first define the data that requires surveillance and monitoring for potential risk. Depending on your firm, this could include:

- order management systems (trade blotters)
- portfolio accounting systems
- electronic communications (email, IM, text, social media)
- employees' personal trading activities
- employees' outside business activities and web presence
- logs of meetings and calls with experts
- logs of meetings with public company management
- gifts and entertainment
- research calendars
- and more

After defining the data at hand, your firm should collect the data and make sure it's formatted in a way that can be made usable to the surveillance team and software algorithms. For example:

- Do transactions and open or canceled orders make it to a format that is machine readable and representative of the time of creation?
- Do personal trades get linked to portfolio trades and meeting calendars?

- Is a common global security master in use?
- Do your firm's analysts record all meetings that take place via bankers, brokers, and expert networks?
- Are you storing all e-communications, or could some happen through unapproved or unarchived communication channels?

As electronic communications (email, text, IM, etc.) have proliferated, compliance risks have grown.

Figure 1 shows the results of a recent ACA webcast poll in which 70% of respondents said they are engaging in electronic communications surveillance on a quarterly basis. And additional 13% reported doing so on a semi-annual basis.

Of course, even with an adequate holistic surveillance program in place, a bad actor can find the means to avoid basic surveillance (such as by using a personal phone). Nevertheless, your firm has a responsibility to take reasonable measures to collect as much data to support surveillance as practical. And, depending on the unique risks facing your firm that were outlined in your initial risk assessment, these data points may or may not be relevant and useful for the analysis.

How often are you engaging in electronic communications surveillance?

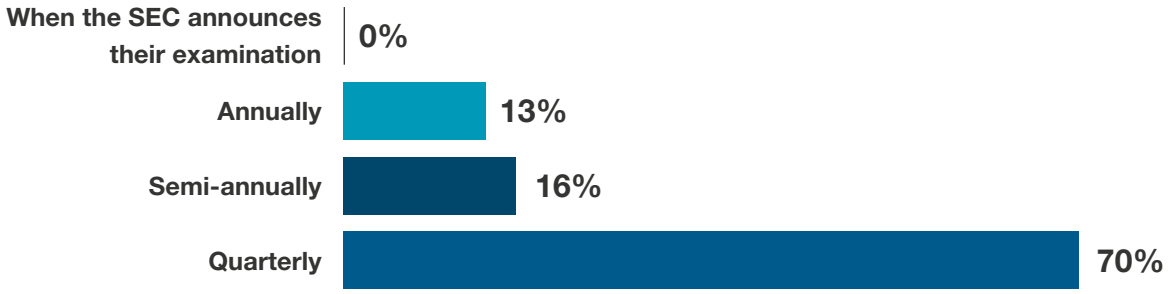


Figure 1

Step 3: Conduct forensic testing around the data

Once the risks are identified and data is accessible, you can develop a testing program.

Effective anomaly detection is a combination of art and science, and this is where machine learning, natural language processing, and artificial intelligence can all assist. Figure 3 shows the results of a recent ACA webcast poll in which 28% of respondents said they are already using artificial intelligence as part of their technology solution, or planning on doing so, within one or two years.

But anomaly detection cannot rely on machine algorithms alone. Human expertise is required to train the algorithms and to identify scenarios that the algorithms haven't been designed or trained to detect. The algorithms used to analyze the data sources feeding a holistic surveillance framework can only detect what they've seen in the past, and while that will catch a significant percentage of the misconduct that takes place, there may be novel approaches that the algorithms will miss.

> **A critical part of ensuring your firm's holistic surveillance program is sound is the use of forensic testing, where anomalies and risks can be analyzed, and this is where human expertise matters the most.**

Technology has greatly advanced the ability to rapidly identify true outliers. Firms should recognize the risks of attempting a manual review of the multitude of tests necessary. Automated anomaly detection has seen the greatest advancement and usage of AI and machine learning and is sometimes synonymous with surveillance, when it is only one step in the process.

How soon do you expect artificial intelligence to affect your business?

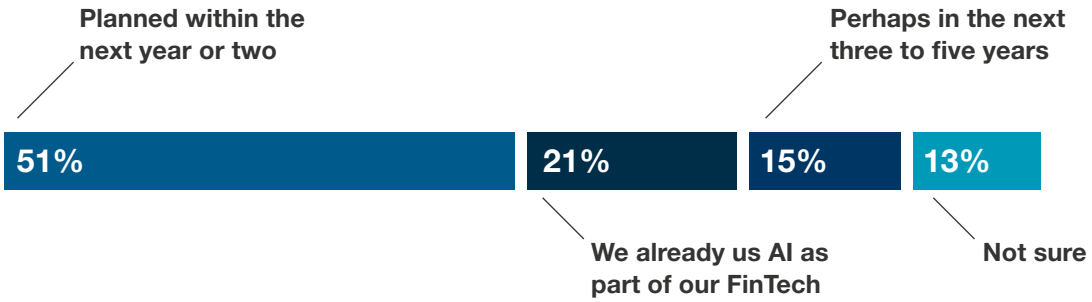


Figure 2

Step 4: Detect and investigate items of interest

To be proactive, firms need to make sure the outcome of any compliance investigation is fed back into the risk identification, data collection, and algorithmic detection components of the surveillance program: if new risks are identified, if further data could help avoid a false positive, or if an algorithm needs to be tweaked to be more accurate in the future, the program needs to "learn" from the investigation's results.

One way to continually fine-tune your firm's holistic surveillance program is to focus on the phases of detection and investigation, which is where we have seen the regulators deepest focus, and where they have highlighted deficient activity.

Some examples of detention and investigation include:

- **Fundamental Trading.** Many traders like to tweak positions around earnings. If a firm's trade surveillance system flagged a trade around earnings—and the Chief Compliance Officer (CCO) knows that meeting senior management is an attribute of the investment process—then reviewing notes from that meeting should be part of any investigation. Firms should also make sure to check any personal transactions around the same security.
- **Quant Shops.** In a quant firm, the CCO is typically not a programmer. Yet the firm's programmers not only set the models but engineer the surveillance, which can lead to a problematic situation, where the fox is essentially guarding the compliance henhouse.

  To address this potential risk, the regulatory view is not that the CCO should be able to read code, but that the CCO should have a program in place to understand the concepts of the trading model(s), an ability to ensure it is acting as marketed, and an ability to identify if it veers from expectations.

  Just because the computer is generating investment decisions does not exclude the firm from surveillance, or from the concerns of personal trading ahead of or around model decisions.
- **Firms trading harder-to-value securities.** Often a model is used for valuation, and while a firm's CCO may not be able to re-engineer the model, they need to be comfortable with the inputs to that model and the sources of the inputs.

  For example, is valuation based on actual trade data, or just a broker's suggestion or indication? Is a single broker used or multiple? Is marking conservative/middle/aggressive correct, as each may have different implications? From a supervisory perspective—does the firm have tests in place to ensure the inputs are being ingested accurately and not changed mid-process?
- **Firms using expert meetings.** Assuming a firm is tracking and surveilling (ideally chaperoning) expert meetings, is it also monitoring for expert usage against personal trading? Beyond concerns with personal trading on MNPI, the use of fund research dollars for personal betterment is problematic.
- **Allocations.** When monitoring for fairness in allocations, does your firm test against the full data set of trade allocations, or review a partial sample of trades to identify unfair allocations or bugs in allocation algorithms?

Step 5: Determine the path to resolution

Resolving identified issues is more art than science. Your firm's policies and procedures must guide the process, but past behavior, intent, and other qualitative factors will dictate the best path forward.

In many cases, we've observed that the outcome of an investigation is that there is insufficient insight or evidence to determine investment rationale. Compliance officers would be wise to plan ahead to avoid this outcome: work with your PMs and analysts to build a process that allows you to get comfortable with how they are justifying investment decisions.

Every analyst and PM will do things differently, and it's impossible (and unnecessary) for the compliance function to fundamentally alter how the research teams have operated for many years. You do not need to change their process, but you should have access to it and get comfortable that you could identify when it seems like they (even a computer) did

WHAT ARE THE VALUABLE COMPONENTS OF A HOLISTIC SURVEILLANCE PROGRAM?

Your firm's holistic surveillance program should be tailored to the specific needs of your firm. Based on the risks assessed and the data aggregated previously, elements to consider incorporating into your firm's program include:

- **Trade surveillance technology and analysis.** A critical place to start is to make sure that your firm is adequately and systematically analyzing its trading activity. Surveillance technology applies algorithms against trade and position data as well as historical market information to produce "Items of Interest" for focused follow-up investigation.
- **Electronic communications surveillance.** Your firm should systematically monitor and examine electronic communications within the broader context of trades and other activities that might trigger compliance issues, based on your firm's specific risks.
- **Expert network call chaperoning.** Monitoring conversations or meetings that might impact trade decisions can be harder than just monitoring trades because meetings, phone calls, and other verbal communications aren't by nature quantified entities. Instead, to incorporate verbal communications into a holistic surveillance program, your firm should consider expert network call chaperoning, where surveillance analysts can chaperone consultations and document any inconsistencies with policies and procedures, as well as provide reports of any red flags. The meeting logs from chaperoned meetings can then be combined with other sources of information to strengthen the analysis of your firm's trading activity.

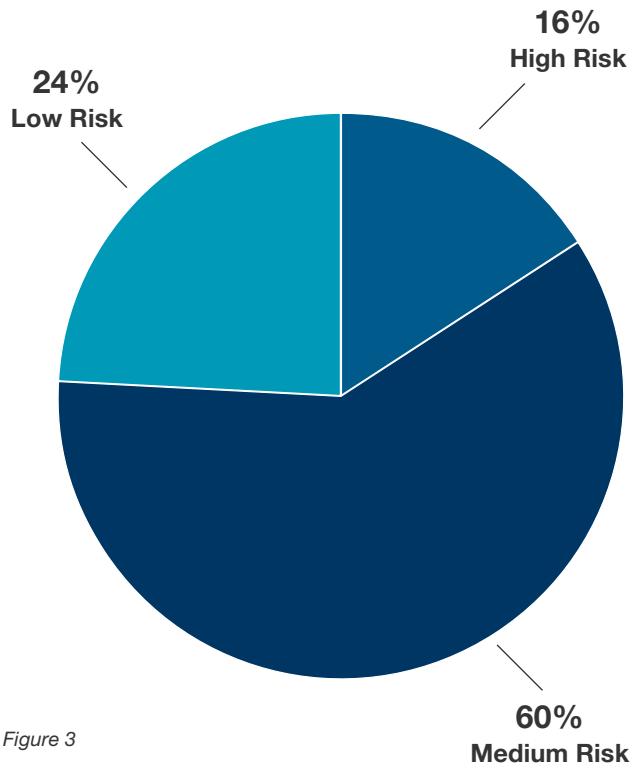
"Resolving identified issues is more art than science. Your firm's policies and procedures must guide the process, but past behavior, intent, and other qualitative factors will dictate the best path forward."

- **Social media and online presence surveillance.** Your firm's corporate and even employees' social media or online activities can pose compliance or reputational risks to the firm. A holistic surveillance program should include a monitoring of regulatory guidance on the use of social media by investment advisers and their employees.
- **Employee compliance/code of ethics monitoring.** Personal trading and reported activities of your firm's employees are valuable data points to collect and incorporate into a holistic surveillance program. Such content should be used to help generate a list of items of interest for additional investigation.

In addition, your firm should have a technology solution to help manage code of ethics compliance activities related to employee personal securities trading monitoring, attestations, reporting on gifts, political contributions, outside activities, and more.

Figure 3 shows the results of a recent ACA webcast poll in which 87% of respondents said they use technology to support their firm's code of ethics compliance, while the same poll showed that a total of 76% consider code of ethics violations either a medium risk or high risk to the firm.

How big of a risk area do you consider code of ethics for your firm?



Do you use technology to support your code of ethics compliance?

Figure 3

CONCLUSION

It is important to ensure you implement a true holistic surveillance program in order for it to be effective. Content expertise and critical analysis (from a human) is important to identify your firm's specific risks, to identify the best uses of available data, and to understand how to best tailor algorithmic surveillance to minimize false positives and optimize what is detected. A combination of technology augmented by human expertise is the most reasonable and effective approach to surveillance and mitigating risk.

HOW WE HELP

ACA's holistic surveillance solution combines our surveillance technology solutions with white-glove support from our dedicated compliance and surveillance specialists to provide firms with a comprehensive, efficient, and cost-effective approach to surveillance. By bundling these services together, your firm's compliance team can leverage the benefits of ACA's outsourced services and tech capabilities and get back valuable time to focus on more strategic tasks. Let our team provide the confidence of a complete top-level view of activity and behavior while relieving your compliance function of the burden of day-to-day tasks.

If you are interested in learning more about how we help firms implement holistic surveillance programs, please contact:

Patrick Conroy
+1 (781) 234-5631
pconroy@acats.com

Michael Lehman
+1 (917) 596-4042
mlehman@acats.com

Sean McKeveny
+1 (412) 491-2085
smkeveny@acacompliancegroup.com

ACA COMPLIANCE GROUP

ABOUT ACA COMPLIANCE GROUP

ACA is a leading global provider of governance, risk, and compliance advisory services and technology solutions. We partner with our clients to help them mitigate the regulatory, operational, and reputational risks associated with their business functions. Our clients include leading investment advisers, private fund managers, commodity trading advisors, investment companies, broker-dealers, and domestic and international banks.

Our global team includes almost 100 former SEC, FINRA, FCA, CFTC, NFA, and state regulators, as well as former senior managers and technologists from prominent financial institutions and consulting firms. Through our collective expertise in compliance, cybersecurity, performance, financial crimes, and technology, we understand our clients' business needs and regulatory requirements.

For more information, visit us at www.acacompliancegroup.com

ACA COMPLIANCE GROUP

Surveillance Program Gap Analysis Checklist

The SEC, FCA, SFTC, and FINRA have all issued clear reminders in recent months that firms' surveillance obligations remain intact despite COVID-19-related challenges [Download timeline]. ACA's team of experienced surveillance professionals have developed the following checklist to help you determine whether your firm's surveillance program has gaps and where it may need improvements. This list is not intended to be exhaustive; ACA's team can help analyze the results and determine the best path forward if enhancements are needed.

ATTESTATIONS

- Have you renewed attestations with respect to the following?
  - Policies in a remote working environment
  - Policies and procedures related to receiving and reporting MNPI
  - Policies and procedures related to other market abuse activities depending on strategy
  - Allowable mediums of communication
  - Allowable physical devices (e.g., printers, scanners)

TESTING

- Many firms have relied on in-person contact to guide surveillance – have you adjusted your surveillance process to account for the remote working environment?
  - Are you checking that employees' remote working environments don't produce conflicts of interest?
  - If conflicts of interest are possible from working remotely, are you training employees to ensure they keep information barriers intact?
- Have you reviewed the quality of your program's findings?
  - Are the findings reasonable?
  - Is your overall process risk-based and aligned with each portfolio manager's strategy/style? As a compliance officer, can you fully describe the attributes of each PM's investment thesis and do you have access to those notes/models?
  - Has the number of findings changed due to COVID-19-related volatility?
  - Is your program designed to meet your peer standard or to match your firm's activities in a bespoke fashion?
  - Are you able to adjust parameters across the following areas? Have you adjusted them if necessary?
    - Market cap
    - Asset class
    - Portfolio manager
    - Strategy

TESTING (CONTINUED)

- Assuming an increase in results due to volatility, have you adjusted the parameters to allow for a full review of findings (i.e., not just sampling the results)? Have you or do you plan to reset these parameters?
- What is the protocol for addressing false positives?
- eComms:
  - Have you increased your testing cadence?
  - Have you reviewed industry/peer best practices?
  - Are you tracking and testing all allowable mediums of communication?
  - For employees working from home: have you adjusted the search scope (e.g., Is it comprehensive enough? Is it updated to reflect current potential risks and vulnerabilities? Is it producing too many results - do you need to add filters, etc.?)
  - Are you monitoring the use of personal email accounts for business purposes (e.g., sending documents to personal email accounts for printing while working from home, etc.)?
  - Is Compliance keeping up with the "latest and greatest" social media sites for the finance industry (e.g., StockTwits)?
- Are you tracking all meetings and events where MNPI could be present?
  - Are your employees logging all one-to-one meetings with management while working from home?
  - Does your trade surveillance incorporate the meetings and events tracked?
- If FCA-registered, does your surveillance program address Market Abuse Regulation (MAR) requirements?
- If you have a trade surveillance system in place, is it automated?
- Can you confirm for quant strategies that the system runs as described (i.e., without human override)?
- Do your surveillance reviews include employee personal trading activity?
- Is your investigation process holistic (i.e., incorporates eComms)?

TRAINING

- Have you conducted employee training regarding insider trading, MNPI, etc.?

  Note: To help protect your firm during this challenging time, ACA is providing our web-based insider training course to individuals and up to 100 licenses to firms free of charge until September 4. **Learn more**

- Have you conducted employee training regarding the appropriate, safe, and approved use of business email accounts, BBG chats, IMs, etc., particularly given the related cybersecurity/information security concerns?

07/2020

QUESTIONS?

For questions or to discuss how ACA can help your firm strengthen its surveillance program, increase efficiencies through technology, and ensure your regulatory obligations are met, reach out to your ACA consultant or contact us here.

ACA COMPLIANCE GROUP

Regulators Home in on Market Abuse in the Age of COVID-19

COVID-19-related market volatility and risks posed by employees working from home have financial regulators on high alert across the globe. The SEC, FCA, SFC, and FINRA in recent months have all called out their continuing focus on detecting and punishing insider trading, market abuse, code of ethics violations, and other misconduct.

MARCH 13

» ESMA and certain EU countries lower the net short position reporting threshold.

» **Surveillance Impact:** Firms should confirm that their surveillance system is calibrated to adjust for these changes.

MARCH 23

» The Co-Directors of the SEC's Division of Enforcement issue a statement reminding firms of "the importance of maintaining market integrity."

» **Surveillance Impact:** Firms should review their controls and procedures around MNPI, disclosure controls and procedures, insider trading prohibitions, and codes of ethics.

MARCH 27

» The SFC issues a circular to management companies and trustees and custodians of SFC-authorized funds in relation to the market volatility.

» **Surveillance Impact:** Managers are reminded to closely monitor the dealing and trading of the funds under their management.

APRIL 27

» The FCA reported a 23% increase in market manipulation reports between 2017 and 2019.[1]

» **Surveillance Impact:** Regulators can uncover misconduct in many different ways.

MAY 4

» The FCA's executive director of enforcement and market oversight, Mark Seward, commented on an anticipated increase in market abuse cases due to COVID-19: "Our market-surveillance radar is working at full speed in order to ensure we can see exactly what's happening in the market in real time…No one should be tempted to think they're immune from detection."[2]

» **Surveillance Impact:** The regulators are not slowing down in their enforcement of market abuse despite the challenges of the current environment.

MAY 27

» The FCA publishes Market Watch 63.

» **Surveillance Impact:** Firms are again reminded of their surveillance obligations, especially related to the Market Abuse Regulation (MAR). Firms should ensure their surveillance systems are calibrated to identify these risks.

MAY 28

» FINRA issues guidance on trading supervision in the current remote environment.

» **Surveillance Impact:** FINRA's position on trading supervision is consistent with that of buy-side regulators, indicating a united front among financial regulators on market abuse.

JUNE 23

» SEC's OCIE issues Risk Alert highlighting surveillance deficiencies observed from examinations of private fund advisers.

» **Surveillance Impact:** Private equity and hedge funds are reminded of their regulatory obligations around MNPI and code of ethics, among other areas.

[1] Financial News, *Reports of market manipulation to the FCA rise 32% since 2017*, 27 April 2020

[2] Financial News, *FCA's stark warning: Insider traders will be caught during COVID-19 crisis*, 4 May 2020

For questions or to learn how ACA can help your firm strengthen its surveillance program, increase efficiencies through technology, and ensure your regulatory obligations are met, reach out to your ACA consultant or **contact us here**.

www.acacompliancegroup.com