BATES GROUP

The Practicalities and Opportunities of Harnessing Technology and Big Data in Regulatory Enforcement and Compliance Practices

"Innovation," "revolution" and "modernization" are often used to characterize technology transformation in the regulatory compliance and enforcement space. While regulators are announcing their efforts to harness data analytics with cutting-edge technology to serve their market oversight responsibilities, financial service institutions are navigating the endless stream of new fintech products and services that purport to "solve" their complex business and enforcement challenges. In this paper, we take an in-depth look at the challenges firms are facing when deploying data analytics in their compliance and enforcement practices and procedures.

Every day, federal and state regulators are dropping new guidance, amending rules, issuing alerts on new investor or emerging market risk, announcing new targeted enforcement sweeps, and publishing examination results on the latest compliance deficiencies.[1] These directives force consideration and reconsideration by firms of their ever-expanding book of processes and procedures. While this governmental activity is intended to protect investors, enable firms to compete on a level playing field or facilitate the growth and stability of the financial markets, they require that firms expend significant resources to ensure compliance and respond to compliance deficiencies.

The application of sophisticated technology and data analytics serves both regulators and firms alike, but reliance on it adds additional costs, complexity and new risk, which, in turn, restarts the cycle of government intervention requiring response. Often lost in these "Fintech" and "Regtech" conversations is the reality that financial service providers are operating businesses in a competitive environment and must produce for their clients every day, in real time.

Now more than ever, financial institution decision makers need to think about how best to take advantage of their systems and data analytics programs without making expensive strategic mistakes. That is where we start our conversation with Alex Russell, Managing Director with Bates Group's White Collar, Regulatory & Internal Investigations Practice, someone fluent in the latest tech offerings and big data analytics applications, but who spends his days solving real financial firm compliance and enforcement problems—issues with real business and investor client consequences.

How Should Clients See the Regulators' Embrace of Data Analytics?

Bates Group: *Thanks for joining us today, Alex. Let's start with some of the basics. Financial services is a heavily regulated marketplace, and institutions of all sizes have always grappled with compliance and enforcement issues. Effective use of big data and analytics is now touted by regulators as the critical tool necessary to oversee that market. You serve clients who are the subject of that effort. How do they see it?*

Alex Russell: Perhaps the best way to answer that is by considering how firms actually interact with regulators. Our clients are chief compliance officers, general counsel, and outside counsel who are well aware of the reach and the advantages that big data and analytics provide examiners and enforcement officials. They come to us when they need a practical solution to an immediate or anticipated problem—when they need to improve or amend a system, solve a legacy system integration issue, or defend against a claim or deficiency raised in an examination, most often around quantifying the potential impact to investors. To the extent that they are concerned with broader regulator strategies, it is only to better prepare their firms to respond to what they hear may be coming down the road. In this regard, we are a good source for them, and we often serve to help them understand how their peers are handling similar issues.

But, when they call us, it is usually for something immediate and concrete. Often, it's a call about an internal issue, possibly coming from a head of compliance, saying: "We're collecting certain data, for a certain compliance or business purpose, but it's not very useful, or it's not as useful as we think it should be." Sometimes, a compliance officer may call because something just doesn't feel right to them.

They could have a suspicion that something is just not working the way that it should or that some established controls and processes are being exploited in some way. In those instances, they may just want an assessment to determine if the system has vulnerabilities that can be exploited.

Calls from general or outside counsel, on the other hand, are usually about a concern that has escalated to a point of some urgency. These calls often pertain to pulling data from a firm's systems for the purpose of responding to requests from regulators, or for information that can be useful in an enforcement action, or sometimes even as the basis of a settlement to litigation where the regulator mandates that an

"Sometimes, a compliance officer may call because something just doesn't feel right to them."

independent third party be brought in, or where the firm, of its own volition, wants to prevent similar problems happening again down the line. Lawyers tend to see the advantage of a separate, dedicated outside team that has the bandwidth, the capacity or the skills to get to specific information quickly or address certain systemic problems, without disrupting the normal processes of an internal team.

So, in many ways, even financial firms that are in the regulators' sights are focused on the same thing they always have been: responding to specific inquiries and improving their systemic capabilities to do the right thing. Both compliance officers and counsel are seeking ways to utilize the same set of available tools as the regulators are using to address—or stay one step ahead—of their compliance and enforcement concerns.

What Data?

BG: *What kind of "data" are we talking about? Without getting into the minutiae, what are you searching for when a firm reaches out to you?*

AJR: That depends on the focus of the concern presented and the many different perspectives on what constitutes relevant information. Consider all the categories of information a financial institution holds. Most people understand data used in the compliance and enforcement context as the transactional information: reams of data files that allow analysts to review the flow of activity going through the firm, relevant time periods, specific products or services, branch office activity, or even the activities of a specific financial adviser.

Another type of "data" held by the firm are the rules and procedures governing trading activity. For example, what are the system alert parameters that are, or should be, applied to a trade? What are the specific supervisory procedures at issue, are they designed appropriately, and are there conflicts with other internal areas? How do the firm procedures differ from the regulatory standard? To answer certain questions, you have to be able to go deep into multiple types of information held by the firm to understand the story of what is actually happening.

Further, there's information—data—connected to how the firm surveils, monitors and controls the flow of activity in their compliance processes and procedures. What are the surveillance and alerting elements of firm systems intended to catch proscribed activity, or what are the rates of true versus false positive flagging? And so forth. All of these are subject to analysis. Identifying the relevant data (for any particular

"A separate, dedicated outside team ... has the bandwidth, the capacity or the skills to get to specific information quickly or address certain systemic problems, without disrupting the normal processes of an internal team."

assignment) is key to a successful outcome, but it requires experience to know where and how to look for it and a variety of skills to work with it.

Focusing on Outcomes

BG: *How do you move from a conversation about a problem area, say, a compliance deficiency or a potential violation, to a strategy for addressing it, and then to a team executing on it?*

AJR: Clients generally know what they want as an outcome: a working system doing what they want it to do, mitigation of downside risk, and specific information to limit damages. How sophisticated they are in the details of system architecture is less important to us than truly understanding their concern and the outcome they seek (which can, sometimes, evolve into something well beyond their initial request). There is no substitute for reaching that understanding with the client, and it is incumbent on our team to ask the questions of them necessary to design a strategy that can deliver the outcome they want. But, it takes experience to know what to ask. And it takes a lot to build a team with the diverse data skills necessary to go from first conversation to the delivery of those outcomes.

Our team uses knowledge of system architecture and design, the latest in data analytics, and skills for compiling, cleaning, manipulating, and transforming data to create a strategy to produce what the client wants or needs. This may be opaque to many, but it is important to know that these tools, this capacity, is not the domain of one "good computer person." It relies on the combined knowledge and experience of a deliberately assembled team, dedicated to dealing with regulatory inquiries, enforcement or litigation matters. Obviously, I am proud of the team at Bates, but at the end of the day, what we've found in our own experience, year-after-year, is that there really isn't an effective substitute for human judgment and bringing background knowledge and skills-based expertise to bear on a particular issue.

What Do We Not Know?

BG: *Clients come to you for your technology and analytical expertise. How do you bridge the gap in subject matter expertise?*

AJR: Our best results come out of a clarity of purpose, which comes from knowing the subject, designing an effective method of inquiry and having the skills to execute on it. When we confront issues where there is a gap in our understanding

"It takes experience to know what to ask. And it takes a lot to build a team with the diverse data skills necessary to go from first conversation to the delivery of those outcomes."

and need additional expertise to be certain of our path, we are fortunate to be able to rely on our colleagues in different practice groups at Bates. For example, we might bring in anti-money laundering or compliance or litigation experts to ensure that we ask the right questions and attack a problem from all sides. We have nearly 200 financial industry experts at Bates, so it is quite the brain trust to be able to tap.

Similarly, if we are uncertain as to what the best practices today are in any given area of inquiry, like revenue sharing or 12b-1 fees, we can reach out to our compliance colleagues and say: "This is what we are seeing. How does it align with what you would expect?" They may wind up partnering with us to make sure that the client gets the best possible information that's as current to the moment as possible for their particular inquiry. For example, we handled a compliance matter concerning the recalculation of certain aspects of fees and performance metrics for a firm. The client asked us a holistic question about what we thought of the level of fees that they were charging. It was, in essence, a benchmarking question on their fee rates and the components that went into those fees relative to the industry at large. We had a point of view on that because we see that kind of information regularly, but we don't have as broad of a view as our compliance group does. So, we partnered with the Bates Compliance practice team to provide that benchmarking in addition to our own observations and experiences. That's actually a very common occurrence for us.

The same is true for issues involving anti-money laundering where we've partnered with our AML & Financial Crimes team. One client had asked us to evaluate anti-money laundering monitoring systems and to do some fine-tuning related to transaction monitoring. The client asked, "Do you think we've got appropriate threshold programs? Is this the right point at which we should be triggering our reviews, or are we leaving opportunities for potential exploits of the system as it stands today?" Again, we have a view into that, but not nearly the breadth of view that our AML team can bring to the table, so we asked them to share their views and we bolstered our approach accordingly.

Off-the-Shelf Compliance?

BG: *How should compliance officers at financial institutions respond to fintech firms offering out-of-the-box solutions?*

AJR: There are many off-the-shelf solutions out there. We stay well informed as to these products and sometimes even adapt

"Our best results come out of a clarity of purpose, which comes from knowing the subject, designing an effective method of inquiry and having the skills to execute on it."

some features they employ to what we may already be doing. Some of them may even complement our services, and when we find one that may reasonably apply to a particular client circumstance, we do not hesitate to recommend it.

We also hear about new tech from our clients. I'll regularly get calls and emails saying: "We've been approached by company ABC that claims to be a new player in this market space, what do you think of them? Have you heard of them before? Or would you like to have a conversation with them to help us evaluate whether they might be useful to us?" We view market innovations—whether it's new fintech or new standards for big data analysis—in terms of whether it would solve or exacerbate a problem for our client. (Sometimes the answer is both.) Ultimately, we do not shy away from new technology that augments what we're doing and the value we are adding for clients. And remember, all the latest fintech product solutions will need to be monitored, tuned, evaluated, and tailored to the particular activities of the financial institution, otherwise, they're ineffective from the outset.

That said, financial firms should be wary of buying fintech without considerable due diligence, particularly on how it would interact with other systems within the institution. Many of these products were first developed from other analytic tools that were being sold in the market, so the product may be fine, but the fintech company can't provide any perspective on how it would sit within the financial institution itself, or how it might relate to all of the other systems, procedures and processes that are in place within the financial institution. We've had experience coming in to do reviews for a firm after the purchase of off-the-shelf fintech software and, in one circumstance, found that three quarters of the alerts that had been flagged by the new system were irrelevant.

We are frequently asked to fix the gap between tech that maybe solved some legacy-related issues and actual performance. A tech solution isn't worth anything if instead of spending your time reviewing trade corrections, you're spending it reviewing alerts that the system is flagging for trade corrections. Besides being very expensive, that is not what you want it to be doing. That's not a benefit in terms of value for the firm's compliance or surveillance teams. We understand, of course, that decisions to buy fintech systems are made across a number of functional areas across a firm. We understand how large those decisions are for the firms that we deal with.

"A tech solution isn't worth anything if instead of spending your time reviewing trade corrections, you're spending it reviewing alerts that the system is flagging for trade corrections."

Repairing a Legacy

BG: *You mentioned the frequency of issues related to integrating legacy systems. Can you elaborate on that?*

AJR: That is one of the big challenges we see firms facing. It's a byproduct of the way financial services firms have grown through mergers and acquisitions over time. There are generally any number of competing legacy systems—earlier versions of systems—that were expected to "solve" the same kinds of issues for the firm as a whole, and for its various subdivisions after the merger or acquisition. Often, the client issue gets raised after a regulator asks a question that cuts across all the entities falling under the umbrella of a single financial institution. Those systems were often not constructed to ever communicate with each other because they were designed to serve a specific function within a singular entity which was later acquired by a much larger entity. This presents many problems for clients, none of them small.

One of the things you always hear from fintech providers is, "Well, of course, we can do that, you just need to direct all of the data into our system." The problem with that approach is that the fintech overlay may integrate with one or two of the legacy bank systems, but it rarely ever integrates with all of them. So, even when a firm decides to purchase a new fintech approach, they are often stymied because they don't have a way to feed all of the relevant data and information into it as a result of the way the multiple current systems are structured. That weakens the value the fintech is providing, since the complete picture isn't available for them to draw insights.

Compliance Priorities

BG: *What really happens when a firm wants to ensure that it is complying with new rules on, say, holds on senior transactions?*[2]

AJR: We happen to have a lot of experience with that particular issue.[3] We would first go through a process of looking at compliance or financial crimes systems, looking at the available data points to make sure the firm is capturing key risk indicators. We might interview relevant employees to be able to really understand what they have in place and where we see gaps, and then would build a custom model for the client in which we integrate multiple data types in order to be able to identify higher risk activity. We would likely assess information flows—that is, the way the data is getting fed to the appropriate compliance and supervisory personnel—so that they can meet

"Even when a firm decides to purchase a new fintech approach, they are often stymied because they don't have a way to feed all of the relevant data and information into it as a result of the way the multiple current systems are structured."

or exceed the standards that they are going to be held to vis-à-vis this group of investors.

For holds specifically, one of the things that's always clear is that there is a lot of grey area, which creates risk for the firm. If the firm applies a hold that turns out to be a legitimate transaction, there's risk for the firm. We often help firms alleviate that risk by helping to create very defined tools both from an analytics sense and a process sense. These tools provide a safeguard to allow a firm to defend standards for how they evaluate transactions and how they collect and evaluate the best data available in real time.

Working with Data in Enforcement

BG: *Let's say that after examination, a regulator determined that holds were unnecessarily placed (or failed to be placed), causing real loss for an investor. What then?*

AJR: From a legal defense perspective, there will always be value in understanding the available data. Where a hold was applied and it wasn't appropriate, you need to prepare rigorously established, procedural support documentation from data. You would need to demonstrate, if possible, that the system and decision-making flowing from it was in fact appropriate, based on the facts that were available. In other words, based on the circumstances and the procedures in place, it looked like the hold was appropriate and justified.

That doesn't mean that the firm may not have to do some client remediation, and we would be able to support those calculations—for example, hypothetical investment performance on what they were trying to purchase, or gross proceeds between the blocked sale they were trying to execute and what they can sell it for today, or if the proceeds were being transferred to pay a loan, calculating the penalty that would be appropriate for the missed loan payment. While we are doing that, we would be looking for how this alert got flagged incorrectly. In other words, we would know, having come to that point of resolution with the client, that this was an example of a false positive, suggesting that not only does the client need to be made whole, but that there is likely a gap in the systems the firm has in place. We would determine where the lines ought to be.

In instances where no hold was applied (the flip side of this hypothetical), we would seek to answer a series of questions: How was it missed? What about this specific transaction might have affected the flag? How do we repair that? Then we would move on to questions of remediation for the investor, given that

"From a legal defense perspective, there will always be value in understanding the available data."

there was potential fraudulent or inappropriate activity that had taken place in their account.

Exam Anxiety

BG: *Why should financial firms call you if they think they have a problem that will be uncovered in an exam?*

AJR: There are three reasons for getting us involved in this scenario:

1) The client wants to convey to the regulator that it is approaching the examination with a third party to demonstrate a good faith effort to get things right. This sends a signal that the client is taking things seriously and is intent on making sure things go well.

2) Working under a best-efforts model, bringing us in acknowledges that internal resources may not have enough capacity to provide responses quickly to examiner inquiries, and we can provide those timely responses and help fast track that process.

3) Everyone is aware that issues uncovered during the course of the examination could turn into enforcement activity as well, so firms benefit from the fact that we've seen the same or similar fact pattern before and how it developed down the road: Did this get cleared with no detrimental outcome? Did it end in enforcement? If so, how severe was the enforcement action? Do we think this is something that's going to turn into a sweep or a self-reporting initiative?

These are the kinds of insights that we can provide even in the infancy of an examination process.

Exam Prep

BG: *How can a client prepare for an examination?*

AJR: Our compliance group typically gets engaged to do mock exams and exam support. From a data analytics perspective, we know that the regulators are going to be taking a hard look at whether or not the policies and procedures—and the systems in place that support those policies and procedures—are effective. In order to do that assessment, you have to be able to provide not only the kinds of insights on policies and procedures that our compliance group can, but you have to be able to look at the results of the alerts that were generated, how those alerts were cleared, who cleared them, was it appropriate, and was it

"It is always wise to know what the data is going to say about your procedures and systems before the regulator does."

cleared in accordance with requirements. Those are all things that are data-related.

It is always wise to know what the data is going to say about your procedures and systems before the regulator does. There's a benefit to knowing, regardless, but knowing it first could either help in the preparation for the exam and provide an ability to take corrective action, or it can give you the confidence to be able to say, "No, we think what we have is more than adequate to the task its designed to serve." That really is our role, whereas the compliance team is the one telling you whether your policies and procedures are meeting the requirements that the regulator is expecting to see.

Building a Better Mousetrap?

BG: *As you describe it, one part of data team's job is to make sure the nuts and bolts are working together, and another part of the job is to ensure that the system is going to provide the content that supervisors need in order to do their jobs. Isn't it true that the part that matters most is the ability to provide proof to examiners or evidence to support a defense in an enforcement action?*

AJR: Yes, that's right. One way to think about it is in terms of building a mousetrap. First question: Does it work? That is, is the contraption mechanically sound? We then move to the second question: Does it produce the desired outcome? We may know the contraption works mechanically, but does it actually catch mice? This leads to the final question: Is it catching the right mice? In this case, the right mice would be the information that the compliance personnel and supervisory personnel need in order to meet their obligations. Those are the three tiers for review.

If the mousetrap is catching the right mice, that success will be self-evident. In other words, it will be exactly matching what the compliance and supervisory personnel were hoping to see. We always ask the client: "What would you—taking for granted all the required pieces of information are there—want this to look like? How do you want this information presented to you? What would be most useful for you, or what would save time in your day-to-day activities? If you had one extra data point that would improve your efficiency, what would that data point be?"

Data and the Human Element

BG: *The more we talk about systems and data, the more you return to the human factor in making them work. Isn't that somewhat ironic?*

"What would be most useful for you, or what would save time in your day-to-day activities? If you had one extra data point that would improve your efficiency, what would that data point be?"

AJR: The thing about large-scale data analysis is that it is, by its nature, a black box. Take machine learning, for example. You are asked to trust the system or the analytical approach that you are applying to a particular problem, and you absolutely have to have a solid understanding of the mechanical nature of the approach or system that you're providing, but also the context in which you are providing it. Even if the analytical side is solid, the context is never going to be knowable by a machine or an algorithm. As a result, the system can send you into some very interesting but unfortunate directions.[4] There is no data analytic success story without thoughtful, intentional human design.

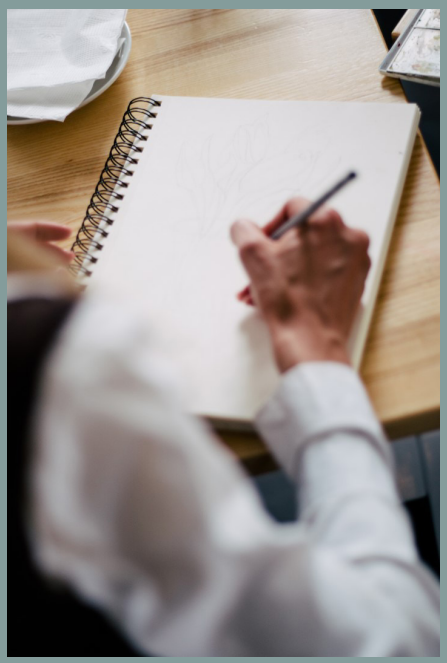
A Big Data Future: Are Regulators Ahead of the Market?

BG: *Final question: Let's return to the original broader question about the advent of big data and data analytics as a means to oversee and regulate the market. Is it ultimately a good or bad development?*

AJR: For chief compliance officers, general and outside counsel, the question is academic. They are working on practical issues every day. But I would say that at this point, regulators no longer have a choice but to use large scale data analytic tools to perform the monitoring and surveillance of the firms they are responsible for. Ultimately, the size of the market and the proliferation of financial data—just the sheer amount of trading data that's generated in a single day—requires the use of new methods of oversight. Transactions have become too voluminous for their old tools to be effective, so they almost have no option but to proceed more analytically. And financial institutions, large and small, will need to respond in kind, if they want to be prepared. They should know more about their own systems than a regulator.

I should emphasize that the use of data collection and analytic methods will serve to inform new regulator strategies, like self-reporting initiatives, a method which serves to take the burden off regulator staff. If a regulator can spot some trend by doing some sweeping analysis across a multitude of firms in a given area that they think may be an industry-wide issue, they can either take the time to examine, make inquiries and ultimately pursue enforcement actions against firms one at a time, or they can set up these self-reporting initiatives that effectively put the ball in the court of the firms themselves to do their own oversight, analysis and diligence. The success of the SEC's 12b-1 share class selection self-reporting initiative, for

"There is no data analytic success story without thoughtful, intentional human design."



example, demonstrated that the regulators can rely on such a strategy. We will, no doubt, see a lot more in the future.

Further, regulators have made it clear in speeches and testimony that they fully expect data analytics to become a cornerstone of the way they proceed with surveillance. Insider trading is a good example. Prior to big data analysis, they were mostly reliant on getting tipped off that insider trading had occurred. They were locked into a strategy that could not effectively deter all the activity they were trying to prevent. Now they can look at trading activity in a given stock across all the firms that are trading in that stock, and they can do so in light of the contextual market movement and news that they're able to pull into their analysis environment. It's relatively easy now for them to spot instances where they can ask, "Hey, we don't know at this point whether you had access to insider information, but we know that you traded options on this security for the first time, one day before a major announcement came out, so we're going to go ahead and ask some follow up questions about that." Going forward, that information will enable regulators to act on a larger scale, but also enable them to catch more perpetrators and potentially have a greater impact on correcting bad behavior.

Conclusion

The long-term shift from largely prescriptive compliance (where regulators would communicate what they were examining for, and market participants would check the boxes) toward a principles-based system (where regulators articulate broad principles—e.g., investor "best interest"—and then assess whether firms fulfill their obligations based on rule guidance, supervision and best practice) has markedly shifted the burdens and costs of compliance and enforcement. That profound shift has been accelerated by the advent of sophisticated technology and data analytics that created new tools for regulators to monitor and address deficiencies and wrongdoing.

In the end, clients must adapt. The last thing firms should want is to have the regulator looking at their data, requesting specific data to look at, and for those firms to have no idea what it is that they are going to be able to pull out of that data. It is critical that firms take a data analytical perspective to their own activity, knowing that the regulators are doing the same.

"The success of the SEC's 12b-1 share class selection self-reporting initiative, for example, demonstrated that the regulators can rely on such a strategy. We will, no doubt, see a lot more in the future."

Endnotes

1 Recently, FINRA issued updated guidance on supervision of third-party vendors, sought feedback on a report by its Office of Financial Innovation ("OFI") concerning broker-dealer approaches to cloud computing, and raised alarms about a phishing campaign using fraudulent FINRA email domains—all phenomenon related to new technology-related products and services designed to help firms adapt to a changing business environment online.

2 FINRA proposed new amendments to rules on the financial exploitation of seniors and other vulnerable individuals. Rule 2165 ("Financial Exploitation of Specified Adults") permits a firm to place a temporary hold on the disbursement of funds or securities from the accounts of adults over 65 or from anyone who the firm "reasonably believes" has an impairment that renders the individual "unable to protect his or her own interests." The proposed amendments would (i) extend the time allowed to place a temporary hold on a disbursement of funds or securities under certain conditions and (ii) allow the placement of a temporary hold on securities transactions where there is a reasonable belief of financial exploitation.

3 Bates has a platform called BIRA (Bates Investor Risk Assessment) that is specifically designed to help firms deal with providing adequate safeguards for seniors, retirees, minors, and anyone with potential diminished capacity, so that they can make sure they are not only meeting their obligations but doing justice to the idea of protecting those most vulnerable investors.

4 See Alex Russell article "Errors, Biases and Algorithms," published February 4, 2019, in *Fraud Intelligence*.

BATES GROUP

Contact

Alex Russell

Managing Director, White Collar, Regulatory and Internal Investigations

971-250-4353

arussell@batesgroup.com

Bates Group

5005 Meadows Road,
Suite 300
Lake Oswego, OR 97035

503-670-7772

contact@batesgroup.com