Replacing the Engine While Flying the Plane

Banks and regulators recognize that in financial crime compliance innovation is imperative

Brandon Daniels
President, Exiger Tech
Exiger is a global regulatory and financial crime, risk and compliance company. Exiger arms financial institutions, multinational corporations and governmental agencies with the practical advice and technology solutions they need to prevent compliance breaches, respond to risk, remediate major issues and monitor ongoing business activities. Exiger works with clients worldwide to assist them in effectively managing their critical challenges while developing and implementing the policies, procedures and programs needed to create a sustainable compliance environment. A global authority on regulatory compliance, the company also oversees some of the world’s most complex court-appointed and voluntary monitorships in the private and public sectors. Exiger has four principal business units being: Exiger Advisory; Exiger Diligence; Exiger Government Services; and Exiger Tech, including AI-based automated due diligence solutions DDIQ and Insight 3PM. Exiger operates through offices in New York City, Silver Spring (DC Metro), Toronto, Vancouver, London, Bucharest, Hong Kong, and Singapore.
When six of the largest market participants in an industry are each fined over a billion dollars in ten years, something is broken. The question is, ‘what is broken?’ In anti-money laundering (AML), counter-terrorist financing, and sanctions controls, this question sits in the crosshairs of regulators and financial institutions alike.

Although the current system of law enforcement and financial institution cooperation continues to identify a small fraction of financial crime, growing operational risk, the scale of data and inefficient resource allocation pose serious challenges to the sustainability of the old approach. As the problem reaches an unfathomable magnitude, regulators and industry stakeholders are collectively realizing, you can only fight fire with fire and an automated approach that leverages today’s expertise is now necessary to cost-effectively tackle financial crime and data challenges.

AN UNSUSTAINABLE SYSTEM

The demand on financial institutions to contribute to the identification and apprehension of criminal activity creates operational risk for both law enforcement and financial institutions. This risk manifests itself in a myriad of ways, including cost, delay, and inconsistency, posing a threat to the original objective. The nature of the challenge is rooted in the volume and complexity of data and an inability to assess data with the current technology infrastructure, originally designed to manage a completely different problem set.

When met with an insurmountable amount of data in incomprehensible formats, the next question is, ‘what can we do about it?’ Given current constraints, the answer has been to throw money, in the form of tens of thousands of people, at the problem. The Bank Policy Institute found that despite the 14 largest banks spending roughly $2.6 billion a year fighting financial crime, less than 1% of illicit funds in the financial system have been confiscated. [1]

The picture of risk prevention is not much better on the regulatory side. Suspicious activity reporting (SAR) increased twenty-fold [2] between 2012 and 2017, reaching over two million SARs, but regulators only use about 4% of what they receive. [3] Clearly there has been little pay-off for a significant expansion in resources and effort.

It is difficult to declare the current infrastructure obsolete, though. Material cases are still identified and prosecuted through the system. For example, seven drug traffickers were imprisoned and over £1.5 million was seized in a recent money laundering case in the United Kingdom (UK) as a result of the ardent efforts of Santander Bank cooperating with law enforcement. The scope of the problem, however, is stretching resources to the limit and pushing regulators and financial institutions to an inflection point.

**RECOGNIZING TECHNOLOGY AS A ‘NEED-TO-HAVE’**

At the end of 2018, turbulence in the industry reached a crescendo with over $26 billion in fines levied. Multiple regulators stepped in with endorsements, guidance, and best practices for the use of innovative compliance solutions. Regulators encouraged the industry to embrace artificial intelligence (AI), analytics, and other emerging technologies, recognizing the necessity of automation to a sustainable compliance engine.

A tectonic shift came in a joint statement in December from The Financial Crimes Enforcement Network (FinCEN), Federal Reserve, Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA) and Office of the Comptroller of the Currency (OCC). The statement highlighted the ability of private sector innovation to help banks identify and report money laundering, terrorist financing, and other illicit financial activity.

The statement clarified that pilot programs and the results that they generate, that otherwise may not be achievable using current processes, will not inherently lead to supervisory action. This is a major step forward for large banks that are traditionally conservative in exploration activities for fear that comparison to the existing programs may draw criticism.

Commenting on the joint statement, Sigal Mandelker, Treasury Under Secretary for Terrorism and Financial Intelligence, said, “As money launderers and other illicit actors constantly evolve their tactics, we want the compliance community to likewise adapt their efforts to counter these threats.”


This message uniquely captures the sentiment that the use of advanced technology is not a nice-to-have, for the benefits of efficiency and efficacy, but is a need-to-have as hostile foreign governments and criminals actively invest in AI.

The US statement further elevated the call sounded by other progressive global regulators. In November 2018, the Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) Industry Partnership, including the Monetary Authority of Singapore (MAS) and the Singapore Police Force, published a white paper encouraging adoption of data analytics-driven solutions, tapping the experiences of financial institutions and offering practical suggestions to implement a new approach to financial crime compliance.[6]

The paper provided one of the strongest endorsements for a departure from manual processes, pointing to a 50% reduction in false positives and a 5% increase in true positives in activities such as transaction monitoring and sanctions screening. MAS Assistant Managing Director and ACIP Co-Chair Ho Hern Shin said the organization “strongly encourages” the use of data analytics to combat financial crime.

The Financial Conduct Authority (FCA), one of the first regulators to highlight automation’s potential to upend outdated and outmoded approaches to AML compliance, has continued to advance the case for AI. In the past, the FCA has pointed to the potential for emerging technologies to have a “transformative impact” on crime prevention and compliance costs.

A LEVEL-HEADED VIEW OF AI

The FCA has more recently provided the industry with a level-headed view of compliance technology. In a speech last November, Rob Gruppetta, FCA Head of Financial Crime, said, “We’re always looking for ways to help us do a better job, and we’re not afraid to use new technologies to turn the tables on criminals.” He cautioned, however, “[w]hile the building blocks of AI have started to emerge, sound principles for putting them together haven’t been developed yet. So as a regulator, a degree of skepticism about innovations like AI is rational.”[7]

This word of caution does not contradict the overwhelming efforts of regulators to push for a stronger, sustainable, compliance environment, but it does add complexity to the question, ‘what can we do about it?’ At the center of this discussion is the examination of the benefits and risks of AI in the compliance space. Even in the context of complex systems, data extraction, decisions and decision rationale building into AI applications must be transparent and explainable.

The Personal Data Protection Commission (PDPC) in Singapore, a leader in this area, released the Model AI Governance Framework (Model Framework). This, and the Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of AI and Data Analytics released by MAS, has accelerated the maturity of global regulatory guidance.

However, the idea that models must be understood, controlled, and auditable is not new. When the Federal Reserve and OCC issued Supervisory Guidance on Model Risk Management (SR 11-7) in 2011, they acknowledged that the use of models in banking “come with costs,” including resources to properly develop and implement models and potential financial losses from decisions based on models that are incorrect or misused. This guidance is still accurate today. In the context of major regulatory controls, the potential loss associated with an error that is repeated millions or billions of times could be significant.

**START WITH INTELLIGENCE BEFORE TACKLING ARTIFICIAL INTELLIGENCE**

In order to guard against this risk, there are three principles that are relevant to any institution. First, start with intelligence, then move to artificial intelligence. AI models are extremely dependent on educated and experienced expertise. Process mapping, data labeling, and outcome assessment are all critical to benchmarking and improving model performance and must be driven by experts.

Second, if you can’t explain it, you can’t check it. For the foreseeable future, financial institutions will be asked to rely on AI systems that have built-in
applications for “explaining” the decisions made and the features relied on to make those decisions.

Finally, you have to know your data. All AI systems are built off the garbage-in-garbage-out principle, first cleanse and define your data, then rely on it to drive consistent, auditable, and accurate decisions.

This year is likely to see continued momentum from financial institutions and regulators behind the deployment of AI as all stakeholders coalesce around its necessity. But as financial institutions move toward automation, they must focus on technology that drives beneficial and explainable outcomes. Replacing an engine mid-flight is tricky enough, don’t gamble with one that you can’t control.
For more information, contact:

Brandon Daniels
President, Exiger Tech
bdaniels@exiger.com