
Speakers

Roy Pollitt, Managing Director, Exiger

With expertise developed in some of the largest financial institutions and law enforcement agencies, Roy Pollitt brings powerful forensic investigations experience to the Exiger team, with a concentration on the evaluation of AML controls. At Exiger, Pollitt has led multiple AML and Sanctions reviews on behalf of the court appointed Monitor for the DOJ and the FCA. Pollitt has also led a compliance review of a well-known Daily Fantasy Sports company. Pollitt joined Exiger after a distinguished 17-year career as a Special Agent for the FBI in New York City, where he was twice named Investigator of the Year. At the FBI, Pollitt investigated complex criminal cases, represented the FBI as the case agent in multi-billion-dollar international money laundering investigations, and uncovered complex global financial transactions and weaknesses in the anti-money laundering procedures of financial institutions. Before joining the FBI, Pollitt was an Asset Manager with Lehman Brothers Holdings, Inc., and a Senior Audit Accountant in the Arthur Andersen, LLP Financial Services Group. He is a Certified Public Accountant, licensed in the State of New York.

Sean Brewer, Managing Director, Financial Crime Compliance, Goldman Sachs


Beth Davy, Partner, Financial Services and Investigations Groups, Sullivan & Cromwell

Beth Davy is co-head of Sullivan & Cromwell's AML & Sanctions Enforcement and Compliance Group. Her practice focuses on bank regulation and supervision, regulatory enforcement matters and internal investigations. Davy is widely recognized as a leading expert in the areas of anti-money laundering and OFAC sanctions compliance and enforcement. She has represented numerous financial institutions in high profile global investigations involving multiple U.S. government agencies, as well as public and non-public regulatory enforcement matters. Davy has also worked with trade associations and industry representatives on establishment of industry standards.
standards and guidelines in the AML and sanctions compliance area and in the evolution of heightened transparency in the international payments system. Before joining Sullivan & Cromwell, Davy was a senior officer of the Federal Reserve Bank of New York's Legal Department and Bank Supervision Group involved in regulatory and enforcement matters.

**Moderators**

**Matt Kelly**, CEO, Radical Compliance, former Editor of Compliance Week

**David Lawrence**, Founder and Chief Collaborative Officer, RANE

Despite the best efforts of regulators, law enforcement, financial institutions, and corporate compliance departments, the business of illicit finance is booming. A recent Global Financial Integrity study concluded that measurable illicit financial outflows – money illegally earned, transferred, or used – topped the $1 trillion mark in 2013.

Growing concern about the link between the illegal movement of funds and terrorist financing is forcing financial institutions to better understand and screen their customers, vendors, and other third parties. Following the November Paris attacks, New York State proposed new banking rules designed to thwart terrorist financing; banks and other financial institutions would have to certify annually that they have implemented compliance programs and real-time filtering programs to flag potential AML (Anti-Money Laundering) and BSA (Bank Secrecy Act) violations, and senior officers who file what turn out to be judged incomplete or false certifications could face criminal charges.

The use of information and communications networks as tools for facilitating illicit financial flows has become one of the key challenges in tackling the problem. Digital technologies facilitate illicit financial flows at each stage – from earning money illegally, transferring illegal funds, or using them – helping these capital flows evade the watchful eye of financial authorities.

By the same token, technology can also provide tools to trace such financial flows and help detect illicit finance, an appealing proposition for corporations operating in heavily regulated environments that need their compliance programs to cost-effectively provide financial transparency and mitigate risk.

Offering a range of real-world insights and pragmatic legal and GRC perspectives, a trio of experts convened recently to discuss the technology, resources, and expertise required to cost-effectively detect and limit illicit financial flows. Highlights from the discussion follow:

**Regulator Expectations**

- “I think we’re at a turning point where things could be changing in a more positive direction concerning regulators’ expectations,” said Beth Davy. There has been discussion among bank regulators on how to have effective compliance programs, and the general agreement is that broad based financial transaction monitoring systems are not the best way to do that.
- Davy added that regulators often look for model evaluation, which was designed for
issues such as credit risk and is not efficient for anti-money laundering risk. It takes attention away from more effective processes and wastes resources.

- “During an investigation, institutions often do not get credit for being innovative and for all of the good things that they do,” noted Sean Brewer. “They say, ‘We don’t care about what you do well – we care about what you don’t do well.’”

- Brewer said that he has noticed a difference in how new examiners treat companies compared to experienced examiners. Experienced examiners are often impressed by how hard companies work to manage risk, and by how difficult the task at hand is in terms of volumes of transactions that compliance professionals must sort through, whereas new examiners often have higher and sometimes less realistic expectations.

- Davy advised weighing the agendas of different agencies to assure they are all addressed. She admitted that there is some skepticism about benefits of cooperating. “However, I’m not sure we can say you don’t get a benefit from cooperation, because we haven’t seen a case where there wasn’t [some level of] it,” she said. By the same token, she also noted that companies that refused to cooperate at least initially did seem to suffer consequences.

- Roy Pollitt also advised filing more suspicious activity reports (SAR) and not to make the decision for law enforcement. “I’d encourage banks to…not defensively file, but if there’s something that’s sitting on the fence, go ahead and file,” he said. “You don’t know what piece will tie into an investigation.”

- Brewer wished for more guidance from regulators, particularly around bribery. “It’s a nuanced area,” he said. “Hiring someone’s child could be looked at as a favor, and if it’s done to obtain business, then that could be bribery. But banks hire thousands of people a year, and some will have connections.”

- Different regulators can also issue contradictory rulings, added Brewer. In one instance, regulators from the United Kingdom ruled that companies could not take officials to a sporting event, while another regulator approved the practice.

- “What makes regulators and law enforcement happier is when there’s at least a documented effort to share information across borders,” said Pollitt. He added that when banks get punished most severely by regulators, it’s usually because of an identified problem that has been unaddressed for a significant period of time.

**Information Sharing**

- “Information sharing is a hot topic,” said Davy. Many regulators are interested in seeing companies build universal Know Your Customer (KYC) databases and using shared monitoring and screening utilities. However, companies are unsure of the benefits they will receive for investing sizeable amounts of resources into information sharing.

- Pollitt acknowledged that information sharing is costly. A quick fix is to share information manually. Long term, however, proper information sharing would require a major technology investment.

- Improving information sharing within an organization is a daunting but important task. Pollitt pointed out that many organizations still suffer from siloing, in which individual teams do great investigative work but their findings are not collected in a single, cohesive KYC monitoring tool. “If a US branch of a bank stops doing
business with a bad actor but can't share that information with the rest of the bank, they're essentially still doing business with that bad actor,” said Pollitt.

Davy noted that regulators often order companies to implement a plan to share data across the entire organization, possibly not understanding how difficult of a task that is. “Challenges around data privacy are so significant in this regard that it would cost a fortune to get legal advice in each of the countries they operate to start to come up with a plan on how to share that information,” she explained.

Brewer said that, because many companies are built from a number of other institutions with their own databases, perfect coordination is almost impossible without a major overhaul of the company’s information management system.

Fostering a Culture of Compliance

Regulators investigating a company often look for a positive corporate culture that emphasizes compliance. Pollitt noted that one sign of a culture of compliance is that the chief compliance officer is a senior employee who has the ear of the CEO rather than a junior officer who manages the day-to-day work and yields to more senior officers when a crisis arises. He added that another quick indicator of a positive culture is that employees feel empowered to raise alerts internally and see them escalate.

“You can tell immediately if an institution has the right culture if they're immediately able to bring the right people and resources to the table,” said Davy. “I've seen cases where a bunch of lawyers were running the show without real input from the top of the house. That's troubling, and can have serious consequences.”

“As a friend at the DA said, a fish rots from the head down,” said Brewer, implying that culture starts at the top of an organization. The CEO needs to support all compliance work, but the line officers must be involved too. They should have the ability to say no, even when it impacts a client relationship.

“The proof is in the pudding,” said Pollitt. “As a regulator, we may talk to the brass and get one story, but when we go to the people actually doing work it could be a different story.” Bad behaviors could get embedded at the middle level and become very difficult to detect and improve.

Decentralized compliance functions are often ineffective, noted Davy. Compliance needs to be tested at every level and be incorporated into every business decision.

Brewer emphasized the importance of compliance testing. Companies should be able to implement a policy of requiring compliance approval, and test after six months and a year and a half to see how many notifications are escalated into investigations. If the number hasn't increased, then the culture may not be right and investigators may not be learning.

Dealing with Developing Issues

In response to a hypothetical situation in which regulatory authorities want to know within five days if a company has any connection to an emergent story such as the Panama Papers, the experts recommended that companies maintain a rapid response team.

Davy advised that companies have a dedicated group with skills and access to appropriate information and tools that can be sent anywhere in the world. “They
should also have a back pocket understanding of what data privacy and secrecy rules are in all jurisdictions in which you operate,” she added. “You won’t have time to dig in and do that research in five days.”

Pollitt emphasized the importance of not forgoing proper due diligence in an emergency. “Just because you have an account with Panama Papers ties doesn’t mean there’s anything wrong with it,” he said. Response teams should conduct robust due diligence, overlay red flag lists with other well-known scandals and look for connections rather than rushing to report on any individual just because they are on the Panama Papers list.

Brewer agreed that suspicious clients should not be reported too hastily. “Take the name, figure out the touch points, see if they’re in your database, figure out if they're a significant figure, what their connections are, and so on,” he said. If they connect to other suspicious accounts in a significant away, then a SAR should be filed.

RELATED READING
Fraud in $4 Trillion Trade Finance Has Banks Turning Digital, Bloomberg, May 22, 2016

About the RANE Insight Series
The RANE Insight Series is comprised of virtual and real-world events offering unique, practical perspectives from RANE’s leading experts in risk management. From conference calls and webinars to in-person roundtables and conferences, these valuable events provide frequent and timely support to busy professional leaders across all industries. Subscribers gain actionable strategies and direct knowledge on specific, emerging risk issues. The RANE Insight Series is closed to the media and exclusively for the RANE community, affording participants an unguarded opportunity to discuss sensitive topics of concern among peers and the world's top experts in their fields. To learn more and view an upcoming schedule of events or recaps of past ones, please visit www.ranenetwork.com/rane-events or email questions to insight@ranenetwork.com.