Enforcement Risks Reshaping Compliance Strategies

Keeping pace with heightened scrutiny from government investigations

July 2019

Bloomberg Law®

Bloomberg Law®

Bloomberg Law Special Reports

The environment of oversight and compliance faced by business has grown dramatically in recent years, so companies must be prepared for matters that will require investigation and response. This report examines some of the prominent areas where recent and ongoing developments are bringing significant change, details how affected organizations are managing the process, and considers some of the wider economic and social factors that may be brought into the matrix.

Join us on Aug. 7 for our Special Report webinar, Minimize Risk Exposure: Strategies for Leading Internal Investigations

About Bloomberg Law

Bloomberg Law® helps legal professionals provide expert counsel with access to action-oriented legal intelligence in a business context. Bloomberg Law delivers a unique combination of Practical Guidance, comprehensive primary and secondary source material, news, timesaving practice tools, market data, and business intelligence.

For more information, visit pro.bloomberglaw.com

everlaw

H5

Contents

HOW QUICKLY CAN YOUR REVIEW TEAM FIND THE FACTS THAT MATTER?

Quickly assess the facts of your investigation, build your case strategy and prepare for depositions without breaking the bank. **H5 Key Document Identification℠** provides key documents you need quickly, accurately and within your budget.

Ready to learn more?

Contact us at info@h5.com or visit us at h5.com

H5

And CFTC Makes Three: Commodities Regulator Joins Foreign Bribery Enforcement

By Carlyn Kolker

A recent policy directive could ensnare more companies in cases involving allegations of foreign bribery, forcing lawyers to grapple with the implications of another U.S. regulator joining the fight against international corruption.

In early March, enforcement director James McDonald announced that the Commodity Futures Trading Commission would bring actions over foreign bribery under the Commodities Exchange Act, his agency's primary enforcement tool. He enumerated several instances of potentially corrupt acts that the CFTC might pursue, such as paying a bribe to obtain commodities business or manipulating benchmark rates.

The next month, Glencore announced it was the subject of a CFTC investigation, according to Bloomberg Law.

That makes the CFTC the third U.S. agency to wield enforcement authority over foreign corruption. The Justice Department and the Securities and Exchange Commission both have extensive staff devoted to enforcing the Foreign Corrupt Practices Act, the 1977 law that prohibits bribery of foreign officials to obtain business.

In announcing the new directive at a gathering of white-collar crime specialists in New Orleans, McDonald emphasized that his agency will work alongside the DOJ and SEC in pursuing bribery-related actions.

The effect was nearly immediate: A little more than a month after McDonald's speech, on April 25, Glencore, the world's biggest commodity trader, announced it was the subject of a CFTC investigation into whether it violated sections of the CEA, according to Bloomberg Law. The trader already is being investigated by the Justice Department for potential FCPA violations, as well as by Brazilian authorities, for possible bribery of foreign officials and money laundering.

The Glencore investigation shows that "this is not an empty gesture by the CFTC," said Philip Nichols, a professor of legal studies and business ethics at the University of Pennsylvania's Wharton School.

Given the CFTC's specific areas of expertise, companies could face deeper investigations into allegations of foreign bribery. CFTC staff members are highly knowledgeable about areas that are less familiar to SEC or DOJ investigators, including mineral extraction and complex financial instruments such as derivatives and futures contracts.

"The commodities industry is a relatively opaque industry," Nichols said. The CFTC "can bring tools to enforcement and knowledge that the Department of Justice, for no fault of its own, doesn't have."

Attorneys who practice at the intersection of commodities and enforcement are waiting to see how the directive will play out in practice. It remains to be seen how tough the regulator really will be, especially with companies that are not required to register with the CFTC. In his March remarks, McDonald said the agency will reward non-registrants for cooperation and self-reporting by not levying any penalties. For non-registrants, this is good news.

"There's this baseline presumption of no action; I think that ostensibly gives comfort to end users, rather than rattling them now that there's this new conversation," said Matt Kluchenek, a partner at Mayer Brown who represents both firms and individuals in commodities enforcement matters.

At the same time, a broad range of sectors that fall under the CFTC's purview could be implicated by the new directive — commodities arbitrage, for instance, or cryptocurrency trading.

"It's not industry-specific," said John Nowak, a partner at law firm Paul Hastings and a former federal prosecutor. "It could cover any industry. If the foreign corrupt practice related to or touched upon the CFTC's jurisdiction, you could potentially run into the CFTC's enforcement arm."

Companies may need new structures and practices to emphasize compliance.

The CFTC's new policy directive will likely place a greater burden on companies to keep and improve their records to show they are complying with anti-bribery measures.

"A practical measure of what this is going to mean for U.S. firms is more reporting requirements," said Nichols of the University of Pennsylvania. Financial firms that finance or insure commodities will see additional layers of reporting, adding to standard anti-money laundering paperwork required for bank regulators, he predicted.

Companies may also have to implement new structures and practices to emphasize compliance with CFTC enforcement measures.

"In terms of how this might impact clients, it reinforces my view that compliance personnel need to think more holistically and not narrowly in terms of foreign corruption," Nowak said. "If you are only looking to check the box with the FCPA, you may be missing other violative conduct."

The CFTC's foray into bribery investigations comes as the regulator is touting its overall enforcement prowess and its ability to partner with other agencies. In testimony to a House of Representatives subcommittee in May, CFTC Chairman Christopher Giancarlo boasted that under his watch, enforcement has been "among the most vigorous in the history of the CFTC" — with more actions, more penalties, and the pursuit of larger matters. The CFTC filed 83 enforcement actions in 2018, the most since 2012, according to the enforcement arm's November 2018 report.

The aggressive stance and escalating enforcement actions have put companies on notice that the agency won't shy away from going after conduct it sees as running afoul of foreign bribery laws.

"From an enforcement perspective, the CFTC has been aggressive — in terms of types of the cases they bring and the sanctions they seek," said Kluchenek of Mayer Brown. "I think that's the perspective in the marketplace."

Companies can expect more of that increased enforcement as the agency flexes its muscles in a new arena.

Carlyn Kolker is a reporter who has covered the legal industry for more than 15 years.

Everlaw helps clients, like Zenefits, move up in the world

Zenefits believes in empowering people to work their best. Their HR software now serves over 10,000 customers globally. And when Zenefits's legal team needed to up their game, they turned to Everlaw.

Everlaw is a cloud-based litigation application that enables teams to collaborate on internal investigations and positively impact legal outcomes. Everlaw combines speed, security, and ease-of-use into a unified, comprehensive SaaS platform. We enable legal teams to investigate issues thoroughly, uncover truth quickly, and present their findings clearly.

Discover, reveal, act.

everlaw

To learn how Everlaw can grow your business, click here or visit us at everlaw.com.

Intense Fraud Scrutiny Challenges Health Care Industry

By Lisa Singh

Government fraud investigations are more frequently targeting the health care industry, with an increasing number of lawsuits and enforcement efforts nationwide. To minimize investigator scrutiny, experts say, businesses should revisit the appearance and substance of transactions.

"Any company that deals with opioids will continue to be a focus," said Paul Kalb, a partner with Sidley Austin who specializes in health care fraud.

"We've seen this as a focus for the last several years, and they [regulatory bodies] will be empowered to continue to investigate and prosecute [those] whom they think – fairly or unfairly – may have been instrumental in the opioid crisis."

This past year saw an increase in opioid fraud cases filed under the False Claims Act against drug companies, as well as prescribers and treatment centers, according to Bloomberg Law. The impact is far-reaching.

"What we are witnessing, in the opioid situation, is really a broad-based set of investigations – some against manufacturers, some against distributors, and some others against individuals," Kalb said.

The federal government also could intervene in whistleblower suits.

Several complaints by states have charged drug manufacturers with Medicaid fraud and violation of the False Claims Act on the basis that manufacturers espoused off-label uses of their products, said Richard Ausness, a law professor at the University of Kentucky.

Finding additional legal avenues, Oklahoma will be the first state to go to trial against opioid manufacturers based on the application of nuisance laws, a strategy employed by states against tobacco manufacturers in the 1990s.

In addition, Ausness said, "Private individuals are continuing to bring *qui tam* actions, and the federal government may feel compelled to intervene in some of them."

Among notable cases, federal authorities recently prosecuted the founder and former chief executive of the specialty pharmaceutical company Insys on racketeering charges, following a whistleblower lawsuit filed by a former company sales representative in 2013. The company agreed to pay $225 million to settle fraud charges, and days later filed for Chapter 11.

Companies should expect similar enforcement action, experts say.

"The Department of Justice tends to run the same play over and over again," said Kalb of Sidley. "If it has achieved success in a particular investigation or prosecution, it's relatively likely to try the same thing again."

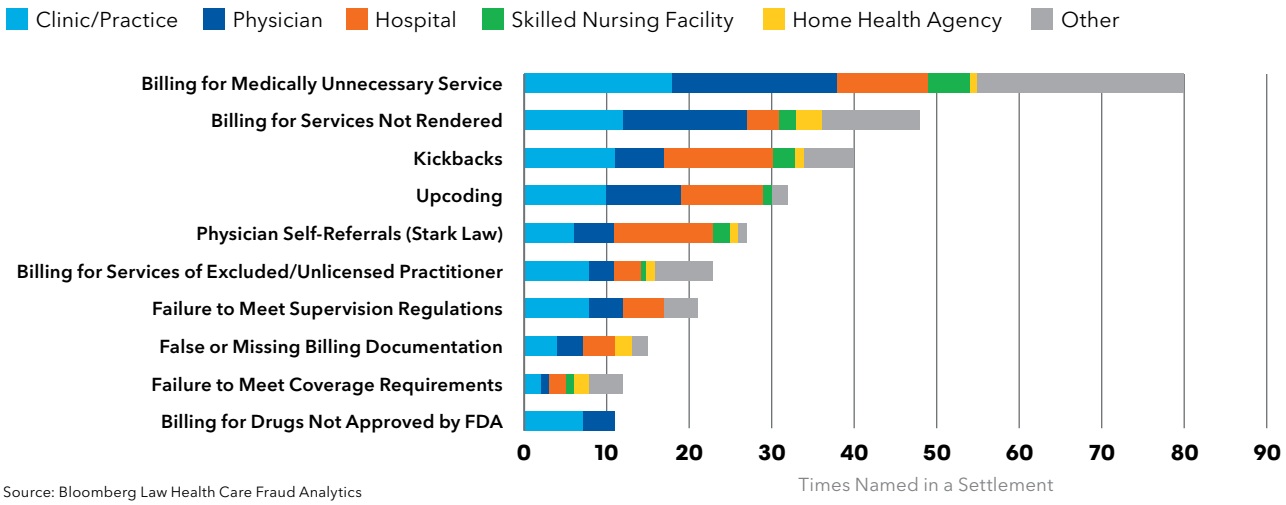
Few companies may be comparable to Insys. "That's your textbook, made-for-television movie," said Peter Pitts, former FDA associate commissioner and current president of the Center for Medicine in the Public Interest.

Yet the current climate – Pitts likens it to "looking for a bad guy, when it's really a systemic problem" – leaves companies in the crosshairs of potentially overzealous enforcement, he said.

Even if a company escapes whistleblowers, it may face increased scrutiny, hastened by parallel enforcement efforts – such as the Appalachian Regional Prescription Opioid Strike Force, formed last fall, to prosecute medical professionals and others tied to illegal opioid deals.

"Historically, most government enforcement has been driven by individual whistleblowers," Kalb said. "What we're seeing in the opioid crisis is enforcement driven by public concern. Prosecutors who are attuned to that concern may very well be driven by it in their investigative efforts."

Common Violations by Provider Type (2017-2018)



Source: Bloomberg Law Health Care Fraud Analytics

More than 1,600 lawsuits have been filed by U.S. cities and counties against manufacturers and distributors. To position for one large settlement, the consolidated case, known as National Prescription Opiate Litigation, has been transferred to the court of U.S. District Judge Dan Polster in Cleveland. The first trials are scheduled for October.

Separately, among states with the most opioid deaths, West Virginia recently accepted $37 million from pharmaceutical distributor McKesson to settle charges of mishandling pain medication, even as the company admitted no wrongdoing.

The pharmaceutical industry could face liability topping $50 billion, according to Bloomberg Law.

"The reality is sometimes investigators are looking not so much to get a conviction but to drive an out-of-court settlement," Pitts said.

Similarly, Oxycontin manufacturer Purdue Pharma reached a $270 million settlement with Oklahoma's attorney general, and similar suits are pending in other states. More recently, Teva Pharmaceutical Industries settled with Oklahoma for $85 million. State attention now centers on Johnson & Johnson.

In all, the pharmaceutical industry could face liability of more than $50 billion, according to Bloomberg Law. The prospect of additional lawsuits and regulatory action calls for long-term thinking, experts say.

"General counsel need to point out that the benefits of short-term profits from increased sales will be more than offset by lawsuits and regulatory fines if companies engage in fraudulent marketing practices or fail to adequately monitor product sales," Ausness said.

Data integrity is also paramount.

"Companies, particularly senior leadership, need to understand their own data," said Kalb of Sidley. This includes assessing whether the product is being sold and prescribed appropriately, as well as whether stakeholders are submitting correct information to the government.

"The government will choose its targets based on information, and will look for problems in the data they have," Kalb said, citing, as one example, coding by Medicare Advantage providers. Beyond the opioid crisis, participants will continue to trigger government scrutiny, given the relative newness of the program, he added.

With such high stakes, companies must be informed by a keen understanding of this enforcement environment, experts say.

"The rules are nuanced, and understanding how government prosecutors interpret them is, therefore, very important," Kalb said. "The key for companies, in this heavily regulated space, is to do their best to understand not only where the government is focused today, but where it's likely to focus tomorrow."

Lisa Singh is a writer specializing in business and technology matters.

Tech Solutions Emerge as Global Compliance Becomes More Complex

By Ellen Sheng

Multinational companies are grappling with a shifting legal environment. Legal and compliance professionals are juggling increasing demands on matters as disparate as corruption, human rights, and how to access data held in other jurisdictions.

This proliferation of regulatory and reporting requirements is behind a thriving new industry: regtech, or regulatory technology. Companies in heavily regulated industries such as financial services, health care, and life sciences have become early adopters of this technology, which might be considered fintech's younger sibling.

Cost savings is a big reason for regtech's appeal. According to a recent report by Bain, compliance costs make up 15% to 20% of operational expenses at most major banks. In a recent survey of banks by Grant Thornton, 78% of respondents said the cost of compliance is "very high or high," while 62% rated the cost of compliance with capital requirements "very high or high."

Costs aren't expected to decline anytime soon. Another report, by JWG and Marklogic, puts the cost of compliance at 4% of revenue, and estimates costs will increase to 10% of revenue by 2021.

Besides the cost savings, regtech is helping companies speed up the compliance process. Whether it's about HIPAA, FINRA, or EU regulations around GDPR, the increasing number of issues makes doing business across jurisdictions more complicated.

New technology is changing the way companies approach compliance, as well as shifting the way law firms and compliance departments operate. There's been a "massive buildup of people, technology, and investment" in compliance and risk management, said Tom Nicolosi, a principal in Deloitte's risk and financial advisory regulatory and operations practice.

While cost is a leading reason for adopting regtech, greater efficiency is arguably just as important.

"The compliance function was always on the back end," said Ilieva Ageenko, managing director for financial services at Grant Thornton. In financial services, large banks historically used experienced staff and in-house compliance, but the process is slow, and it's becoming more challenging to keep up with new technology.

"Now everything is moving so fast, everything is digital," she said. "All the technology is moving faster, and the compliance function has become the bottleneck."

Heavily regulated industries have been early adopters of regtech.

That bottleneck has become an expensive problem at companies dealing with new regulations that require going through a lot of contracts to ensure compliance.

For instance, banks are now dealing with the elimination of LIBOR, which has been used in lending for decades. Roughly $200 trillion worth of financial products are tied to LIBOR. The Securities and Exchange Commission has asked companies to evaluate how the end of LIBOR would affect their business. This means companies need to go through lending agreements from 20 years ago to find out how the agreement was structured and calculate how the new benchmark rate could affect the cost of borrowing.

Similarly, new consumer protection regulations from the Consumer Financial Protection Bureau are forcing banks to go back and review old agreements to ensure the bank is in compliance.

"Lots of these contract reviews were done by people. Now you're starting to see some experimentation," Nicolosi said.

Banks and other companies, as well as law firms, are adopting new technology to help with the increased workload, according to Bloomberg Law. As commercial loan or litigation agreements are digitized, regtech providers can use natural language processing to review contracts. Westpac Banking Group in Australia recently engaged law firm Allens to review work done by artificial intelligence compliance software, to test if robots can read laws accurately.

Companies are also adopting regtech to keep on top of new regulations and e-discovery. Where this used to be done by having someone monitor websites, now some tools use machine learning to scrape websites, identify regulatory change, and alert relevant employees.

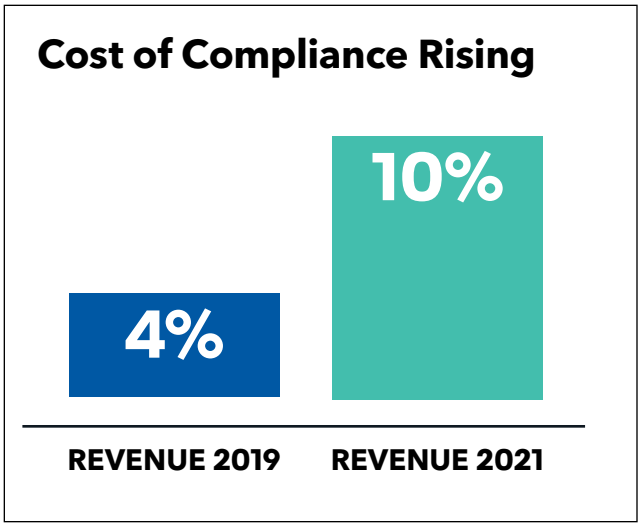
As technology plays an increasingly important role in compliance and risk management, companies are seeking out different skill sets.

Banks and law firms are adopting new technology to help with the increased workload, according to Bloomberg Law.

In the past few years, "compliance and risk are building a technology strategy, and that's not something you'd traditionally see. Skill sets are different now," Nicolosi said. "There are more employees that have a doctorate in statistics, or they are engineers or process folks."

But while technology is changing the way legal and compliance professionals work, he said technology isn't going to replace people.

"Companies will always need lawyers. The jobs may be changing but, at least where we are today, it can't replace human judgment."



Recognizing the technology's importance, companies increasingly are partnering with, investing in, or acquiring regtech providers, which are often startups. Many financial services firms have venture capital investment arms that are focused on technology that the firms might integrate into their operations. Banks are also creating regulatory sandboxes to experiment with new technology in a limited, controlled environment.

"Many of them have less system security," Ageenko said of the regtech providers. "Sometimes they have a good solution … but they don't have the maturity for easy integration. Something that I always advise to any financial organization is to do an assessment and identify areas that have good use cases for regtech."

Ellen Sheng is a writer and editor with a focus on business, finance, fintech, and U.S.-Asia investments.

Courts Create Uncertainty on Securities Cases

By Shaheen Pasha

A pair of cases taken to the U.S. Supreme Court could alter the legal landscape for Securities and Exchange Commission fraud litigation. In the balance is investors' ability to recoup losses from corporate wrongdoing and the potential to spark further litigation.

The Supreme Court took a wider view of who could be held liable in fraud schemes.

One case in particular already has caused a stir among industry players. The court recently decided in *Lorenzo v. SEC* that a defendant could be held liable for taking part in a scheme to defraud investors, even though he was not the primary "maker" of the false statements to shareholders.

The newest ruling departed from a trend of Supreme Court decisions that narrowed the scope of who could be held liable in fraud scheme cases.

The case revolves around an investment banker, Francis V. Lorenzo, who was charged with fraud for disseminating information about the health of a startup's finances. Lorenzo said he simply forwarded the deceptive emails with his signature along to shareholders, though he was not the primary author.

He argued that under the 2011 Supreme Court ruling in *Janus Group v. First Derivative Traders*, private plaintiffs cannot sue an individual for putting out false or misleading information that another had put into a statement. Lawyers for Lorenzo argued that his boss had been the one responsible for the fraudulent content, and to charge Lorenzo as a primary plaintiff in the scheme nullified the *Janus* ruling and could result in a flurry of securities litigation.

In a majority opinion, the current justices disagreed. They relied instead on the SEC's long-held stance that not penalizing distributors of fraudulent statements would severely undercut the regulator's enforcement authority. The new ruling reaffirmed the commission's powers and might give private investors more leeway to pursue legal action against a wider group of defendants for fraud, according to Bloomberg Law.

"The *Lorenzo* ruling was a bit of a surprise," said Thomas Krysa, shareholder with Brownstein Hyatt Farber Schreck. "In some ways, it's like the SEC has come full circle from how it handled such cases before *Janus*. I think you'll see the SEC be fairly aggressive and charge more people with primary liability. Once they push the envelope, that will give tail winds to private litigants to do the same."

Krysa said, however, that he believed courts would push back against an onslaught of private litigation in the wake of the recent ruling. "*Lorenzo* gives litigants a hook to allege primary liability and be more aggressive" in charging defendants, he said, "but much depends on how widely the courts interpret the ruling."

While *Lorenzo* might shift the legal landscape based on a firm ruling, the Supreme Court's decision not to take a duty-to-update case may also have ripple effects.

In *Hagan v. Khoja*, three former drug executives pleaded the Supreme Court to hear arguments that they were not liable for defrauding investors when they declined to inform shareholders that initially successful obesity drug trials were showing more negative results in later trials.

Private investors sued biotech company Orexigen Therapeutics and its executives after the company filed for bankruptcy protection in 2018. Plaintiffs claimed the company had a duty to update its shareholders when the new trial data "diminished" the validity of the previous data. The U.S. Court of Appeals for the Ninth Circuit agreed with the plaintiffs, furthering a divide among the circuit courts over a defendant's legal duty to update, according to Bloomberg Law.

A firm ruling on the issue from the Supreme Court could have clarified defendant liability in such cases, said Ken C. Joseph, managing director and head of global disputes at consulting firm Duff & Phelps. "By denying cert, the court left a lot of open questions rather than setting the record straight on duty to correct. It opens the door for litigants to go forum shopping in such cases."

The Ninth Circuit furthered the divide over the duty to update, according to Bloomberg Law.

In its ruling, the Ninth Circuit parted ways with other circuit courts by deciding a corporation has an obligation to update a statement of historical fact, even if it was accurate at the time it was issued. This ruling is at odds with the Seventh Circuit's stance, which has rejected the existence of any duty to update shareholders. While the First, Second, Third, Fifth, and Eleventh Circuits all believe there is a limited duty to update, it wouldn't apply in Orexigen's case.

Joseph said the general default among circuit courts is that there is no legal duty to update. Even the Ninth Circuit decision leaves room for interpretation over how widely its ruling would apply to similar cases.

Without clear guidelines from the Supreme Court defining the circumstances under which a duty to update exists, there will likely be more litigation to test the boundaries, Joseph said.

Shaheen Pasha is a writer and journalism professor, focusing on legal and financial issues.

Circuits Vary on Duty to Disclose

Obligated to update:

9th

Limited duty to update:

1st 2nd 3rd 5th 11th

No duty:

7th

Amid Growing Pressure, Companies Ratchet Up AML Compliance

By Stephanie Cohen

Financial institutions, including cryptocurrency businesses, are in a race to refresh anti-money laundering programs to ensure effective compliance, or risk facing heightened penalties for failing to pinpoint suspicious activity.

As regulators' expectations for compliance increase, companies are confronting the fact that there is no one-size-fits-all strategy for AML compliance.

"Every day is a new adventure in AML," said Suzanne Lynch, director of the Financial Crime and Compliance Management program at Utica College and previously a vice president for security and risk management at MasterCard Worldwide. Lynch noted that "compliance is getting more difficult," and that "immense pressure is being put on banks."

BSA enforcement actions have reached nearly $1.5 billion in penalties a year, according to Bloomberg Law.

The thing that keeps compliance people up at night, Lynch said, is the question, "Are the regulators going to find something I didn't see?"

AML compliance is a complex field that is watched over by the industry's watchdog, the Financial Industry Regulatory Authority. Under FINRA Rule 3310, known as the Anti-Money Laundering Compliance Program, affected firms must develop and implement an AML program in line with the requirements of the Bank Secrecy Act.

They also have to report suspicious activities that can lead to money laundering and terrorist financing, such as securities fraud and market manipulation. Financial institutions are required to enact compliance systems that can be "reasonably expected" to detect and report suspicious activities.

"An effective [compliance] system is an evolutionary process," said Brian Frey, a partner at Alston & Bird. That process involves constant surveillance and updating.

A failure to flag suspicious client behavior can lead to millions and even billions of dollars in fines today. BSA enforcement actions soared to unprecedented levels between 2009 and 2018, reaching nearly $1.5 billion in penalties a year by the end of the period, according to Bloomberg Law. In the 2018 totals, 13 banks paid $1.3 billion combined for having lax controls against money laundering, helping clients evade taxes, or violating U.S. sanctions. In 2012, HSBC was ordered to pay a total of $1.9 billion when it failed to prevent money laundering by Latin American drug cartels and facilitated trading with sanctioned countries. The Department of Justice in 2018 also created a Task Force on Market Integrity and Consumer Fraud to pursue cases involving money laundering, cryptocurrency fraud, and other financial-related crimes.

In the financial technology space, "the level of scrutiny is only going to increase as regulators and the government understand it more," Frey said.

Compliance experts point to a lack of specificity in some of the guidelines as a possible pitfall for firms. For example, FINRA issued a notice in May providing examples of money laundering "red flags" for firms to "consider incorporating" into their AML programs. The guidance, covering securities trading, deposits of securities, customer due diligence, and insurance products, included 97 red flags organized into six sections, up from 25 in 2002, RegTech Consulting noted.

But FINRA also acknowledged that it was not providing an "exhaustive list" of cautionary activities and that firms needed to be aware of emerging risk areas, such as activity in digital assets.

"The existing guidance, from my point of view, is not sufficient," Frey said. "There is a desperate need for more regulatory guidance."

Much of the recent pressure on financial institutions to ramp up their compliance and data integrity follows the rollout of the Financial Crimes Enforcement Network's Customer Due Diligence Requirements for Financial Institutions rule. The CDD rule, which went into effect in May 2018, amends the BSA and is designed to help regulators identify bad actors and then go after them.

The crux of the CDD rule is a new requirement for financial institutions, including banks, mutual funds, and broker dealers, to verify the beneficial ownership of any entity that opens accounts. This rule is meant to ensure firms understand the nature and purpose of customer accounts that are opened.

Over the past year, FINRA's main focus has been identifying whether financial firms have developed procedures around this new rule, Jason Foye, director of FINRA's AML investigative unit, said May 14 in a FINRA discussion. "Expectations will increase over time."

The nature and widely divergent size of financial institutions also make compliance with the CDD rule more challenging. The Credit Union National Association, which represents America's credit unions and their 115 million members, wrote to Sen. Mike Crapo, R-Idaho, on May 21, urging lawmakers to "strike the right balance between the costs to financial institutions, like credit unions, and the benefits to the federal government" from the CDD rule.

"The reality is the cost of technology for monitoring and ensuring compliance with BSA/AML laws and regulations is disproportionately burdensome on smaller and less complex institutions, such as credit unions," wrote Jim Nussle, president of CUNA and a former member of Congress.

Investments in technology will play a central role in improving compliance as "transactions are becoming systemically faster," and "financial firms have to be able to verify transactions even faster than before," Lynch said.

Technology is crucial because compatible software and databases are necessary to incorporate details of voluminous routine transactions, said Pam Marple, a shareholder in Greenberg Traurig. But at the same time, technology alone isn't a "magic fix," she said.

"For most companies, effectively monitoring for AML red flags requires both robust technology and a strong centralized mandate from top management," Marple said.

Firms are exploring how to embed AI in the workflow/ decision process.

Artificial intelligence-based systems and machine learning are expected to bolster compliance programs at financial institutions. Credit Suisse's U.S.-based securities business, which was fined $16.5 million by FINRA in 2016 for ineffective anti-money laundering programs, told FINRA that the use of AI in monitoring trades may be a promising way to augment and assist trade surveillance teams, analysts, and investigators.

The Securities Industry and Financial Markets Association, a trade association, acknowledged in a May 2019 report that to continue to increase usage, firms are exploring how to embed AI in the workflow/ decision process, but cautioned that AI will need to be used in tandem with the work of trained professionals.

"Since AI is the technology in the raw, firms need to consider where the data came from and how the model operates, understand how to supervise it and ensure AI is working with professional decision making, not replacing it," the report said.

But AML compliance and technology will not succeed without strong support from management.

"Technology is only effective when it is coordinated among often nonconforming and decentralized platforms and with metrics across varying country management," Marple said. "Accomplishing these feats almost always requires centralized mandates and resources."

Federal regulators have acknowledged that some banks are becoming increasingly sophisticated in their approaches to identifying suspicious activity by experimenting with artificial intelligence and digital identity technologies. But so too are those seeking to hide money. "Hiding the money has become far more complex," Lynch said.

Stephanie Cohen writes about regulatory policy.

Bloomberg Law®