Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

EU expands controversial AML Blacklist

Regulators give nod to AI, emerging tech for AML

AI in decision making and accountability

U.S. considers export controls for AI

Artificial intelligence joins the AML crusade

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. http://www.complianceweek.com

onfido

Onfido is the new identity standard for the internet.
Our AI-based technology assesses whether a user's government-issued ID is genuine or fraudulent, and then compares it against their facial biometrics. That's how we give companies like Revolut, Zipcar and Bitstamp the assurance they need to onboard customers remotely and securely. Our mission is to create a more open world, where identity is the key to access.

Inside this e-Book

EU expands controversial AML Blacklist 4

Regulators give nod to AI, emerging tech for AML 6

AI in decision making and accountability 9

U.S. considers export controls for AI 10

EU expands controversial AML Blacklist

Jaclyn Jaeger explores the European Commission's new blacklist of countries with AML deficiencies.

The European Commission has adopted a proposed blacklist of countries it identified as having significant deficiencies in their anti-money laundering and counter-terrorist financing regimes. "The aim of this list is to protect the EU financial system by better preventing money laundering and terrorist financing risks," the Commission said. The EU list of high-risk third countries was first published in 2016, under a mandate by the Fourth Anti-Money Laundering Directive (AMLD 4).

When the Fifth Anti-Money Laundering Directive (AMLD 5) came into force in 2018, it expanded the criteria for spotting high-risk third countries, including the availability and exchange of details on the beneficial owners of legal persons and legal arrangements. "This will help better address risks stemming from the setting up of shell companies and opaque structures which may be used by criminals and terrorists to hide the real beneficiaries of a transaction, including for tax evasion purposes," the EC said.

Other criteria under AMLD 5 include: criminalisation of money laundering and terrorist financing; customer due diligence and recordkeeping requirements; reporting of suspicious transactions; the powers and procedures of competent authorities; their practice in international cooperation; and the existence of dissuasive, proportionate, and effective sanctions.

The new list, published on 13 February 2019, is the first to use the stricter criteria of AMLD 5 and a new method-ology developed by the Commission to identify high-risk countries. The Commission said its new methodology complements the efforts of the Financial Action Task Force—the global standard-setting body for combating money laundering, terrorist financing—by addressing risks that are specific to the European Union. "The result is a more ambitious approach for identifying countries with deficiencies posing risks to the EU financial system," the SEC said.

The list has been established based on an analysis of 54 "priority" jurisdictions. The countries assessed meet at least one of the following criteria specific to the European Union: They have systemic impact on the integrity of the EU financial system; they are reviewed by the International Monetary Fund as international offshore financial centres; or they have strong economic ties with the European Union.

The new list now includes 23 countries, including 12 countries listed by the FATF. An additional 11 jurisdictions have been identified by the Commission, including the U.S. territories of Puerto Rico, Guam, American Samoa, and the U.S. Virgin Islands, as well as Afghanistan, Iraq, Libya, Nigeria, Panama, Puerto Rico, Samoa, and Saudi Arabia.

Sixteen listed countries are already on the original EU list. The Commission also delisted several countries previously included on the EU list: Bosnia-Herzegovina, Guyana, Lao PDR, Uganda, and Vanuatu.

Many have pushed back on the EU's blacklist. In a statement, the U.S. Department of the Treasury said it has "significant concerns about the substance of the list and the flawed process by which it was developed."

The FATF already develops a list of high-risk jurisdictions with AML deficiencies as part of a careful and comprehensive process. "Because of the FATF's work, virtually all countries around the world are subject to a rigorous peer-review methodology that examines the legal frameworks to counter illicit finance as well as how effectively jurisdictions implement them," Treasury said. "These reviews are an intensive process involving careful review of the legal framework, extensive fact gathering, and onsite visits in which assessors engage in robust, iterative dialogues with assessed jurisdictions."

The European Commission's process for developing its list contrasts starkly with FATF's thorough methodology, Treasury said. "Beyond our concerns with the listing methodology, the Treasury Department rejects the inclusion of American Samoa, Guam, Puerto Rico, and the U.S. Virgin Islands on the list."

"The commitments and actions of the United States in implementing the FATF standards extend to all U.S. territories," the Treasury added. "Moreover, the Treasury Department was not provided any meaningful opportunity to discuss with the European Commission its basis for including the listed U.S. territories.

The Treasury Department added that it does not expect U.S. financial institutions to take the European Commission's list into account in their AML and counter-terrorist financing policies and procedures.

European financial institutions, however, must apply enhanced due diligence on financial operations involving customers and financial institutions from listed high-risk third countries. Customer due diligence corresponds to a series of checks and balances that financial institutions must use where there's a high risk of money laundering or terrorist financing. Enhanced due diligence measures include extra checks and monitoring of those transactions by banks to prevent, detect, and stop suspicious transactions.

AMLD 5 clarifies the type of enhanced due diligence measures that European financial institutions must conduct, including: obtaining additional information on the customer, the beneficial owner(s), the intended nature of the business relationship, the source of funds and source of wealth of the customer and the beneficial owner(s), and the reasons for the intended or performed transactions; obtaining the approval of senior management for establishing or continuing the business relationship; and conducting enhanced monitoring of that relationship by increasing the number and timing of controls and selecting patterns of transactions that need further examination.

"Coupled with the recent updates implemented in the 5th EU Money Laundering Directive, the extended list is likely to lead to enhanced checks and control over transactions with these countries," says Chris Laws, global head of product development, compliance and supply solutions at Dun and Bradstreet. "It's more important than ever for businesses to have robust compliance processes in place both for Know-Your-Customer and Know-Your-Vendor activities," Laws says. "Access to detailed information, such as beneficial ownership and people with significant control, is vital to tackling money laundering and an enhanced level of scrutiny of all business relationships is essential to identify and mitigate any potential risks." ■

Regulators give nod to AI, emerging tech for AML

Federal bank regulators are encouraging banks to use Artificial Intelligence and other emerging technologies to bolster their AML compliance programs. **Joe Mont** reports.

With what has the potential to accelerate and expand the use of emerging technologies—including artificial intelligence, machine learning, and robotic process automation—federal banking regulators and the Treasury Department's Financial Crimes Enforcement Network have issued a joint statement intended "to encourage depository institutions to consider, evaluate, and responsibly implement innovative approaches to meet their Bank Secrecy Act/anti-money laundering compliance obligations."

The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, FinCEN, the National Credit Union Administration, and the Office of the Comptroller of the Currency recognized "that private-sector innovation, including adopting new technologies and finding new ways to use existing tools, can help banks identify and report money laundering, terrorist financing, and other illicit financial activity."

"New technology, such as artificial intelligence and machine learning, can provide better strategies for banks of all sizes to better manage money-laundering and terrorist-financing risks, while reducing the cost of compliance," FDIC Chairman Jelena McWilliams said in a statement.

Financial institutions are becoming increasingly innovative and sophisticated in their approaches to BSA/AML compliance, commensurate with their risk profiles, the regulators wrote. For example, some banks and credit unions are experimenting with digital identity technology to enhance their programs.

In response, each of the federal banking regulators has established, or will establish, programs to support the implementation of responsible innovation and new technology in the financial system. "While bank management should continue to follow existing protocols for communication with their respective regulators, these projects and offices may serve as points of contact to facilitate communication related to innovation and new technology," they wrote.

The joint statement, issued on Dec. 3, is the second statement resulting from a working group formed by the agencies and Treasury's Office of Terrorism and Financial Intelligence that focuses on improving the effectiveness and efficiency of the BSA/AML regime. On Oct. 3, they issued a joint statement that gave situational consent for inter-bank data sharing.

In the latest guidance, released on Dec. 3, regulators added that they "will not penalize or criticize banks that maintain effective BSA/AML compliance programs commensurate with their risk profiles but choose not to pursue innovative approaches." While banks are expected to maintain effective BSA/AML compliance programs, they will not advocate a particular method or technology.

The statement stressed that the implementation of innovative approaches in BSA/AML compliance programs will not result in additional regulatory expectations.

"Pilot programs undertaken by banks, in conjunction with existing BSA/AML processes, are an important means of testing and validating the effectiveness of innovative approaches," the multi-regulator statement says, adding that while they may provide feedback, pilot programs in and of themselves "should not subject banks to supervisory criticism even if they ultimately prove unsuccessful."

Likewise, pilot programs that expose gaps in a BSA/AML compliance program will not necessarily result in supervisory action with respect to that program. "When banks test or implement artificial intelligence-based transaction monitoring systems and identify suspicious activity that would not otherwise have been identified under existing processes, [we] will not automatically assume that the banks' existing processes are deficient," it added. In these instances, regulators will assess the adequacy of banks' existing suspicious activity monitoring processes independent of any results from the pilot program.

Nevertheless, banks must continue to meet their BSA/AML compliance obligations and ensure the ongoing safety and soundness of the institution.

"Bank management should prudently evaluate whether, and at what point, innovative approaches may be considered sufficiently developed to replace or augment existing BSA/AML processes," the regulators wrote.

Management must also consider and address other factors including, but not limited to, information security issues, third-party risk management, and compliance with other applicable laws and regulations, including those related to customer notifications and privacy. Bank management should be prepared to discuss these evaluations with their respective regulators.

To the "extent necessary and appropriate," FinCEN says it will consider requests for exceptive relief "to facilitate the testing and potential use of new technologies and other innovations, provided that banks maintain the overall effectiveness of their BSA/AML compliance programs."

Compliance expectations

Treasury Department Under Secretary Sigal Mandelker provided additional commentary on the push for AML technology upgrades during a Dec. 3 speech at the American Bankers Association' Financial Crimes Enforcement Conference.

When responsibly deployed, institutions experimenting with artificial intelligence and digital identity technologies are seeing increased efficiencies and improved effectiveness. "They have helped us identify potential front companies acting for North Korea and Iran," he said. "I have also heard encouraging reports that new technologies are helping banks reduce the rate of false positive alerts, which can free up resources to focus on more impactful activities."

The recent regulatory statement recognizes "the value of trial and error," Mandelker added, reiterating that innovative pilot programs in and of themselves should not subject banks to supervisory criticism, even if those ultimately prove unsuccessful. Likewise, pilot programs that expose gaps in an AML compliance program "will not necessarily result in supervisory action with respect to that program."

The Treasury Department is also encouraging its international partners "to take urgent action to strengthen their AML/CFT frameworks for virtual currency and other related digital asset activities," he said. "The lack of AML and Combating the Financing of Terrorism (CFT) regulation of virtual currency exchangers, hosted wallets, and other providers—and, indeed, of the broader digital asset ecosystem—across jurisdictions exacerbates the associated money laundering and other illicit financing risks."

While the United States "regulates, supervises, and brings enforcement actions relating to virtual currency and other digital asset financial activity, many more countries must follow suit," he said, adding that this is a priority of international outreach, including through the Financial Action Task Force.

Expectations in enforcement actions

Mandelker took the opportunity to address how new technology will be considered in an enforcement context.

"I know from my time in the private sector that the compliance community parses every single word that comes out of a government agency, especially as part of an enforcement action," he said. "That is a good thing. It means that compliance professionals care about getting it right. At the same time, it is incumbent upon us as regulators and policymakers to help you in that effort by making our expectations clear."

For example, to aid the compliance community in strengthening defenses against sanctions violations, Treasury's Office of Foreign Assets Control will be detailing the hallmarks of an effective sanctions compliance program. Among those qualities:

» ensuring senior management commitment to compliance;
» conducting frequent risk assessments to identify and mitigate sanctions-specific risks within an institution and its products, services, and customers;
» developing and deploying internal controls, including policies and procedures, to identify, interdict, escalate, report, and maintain records pertaining to activity prohibited by OFAC's regulations;
» testing and auditing to identify and correct weaknesses and deficiencies; and
» ensuring all relevant personnel, particularly those in high-risk areas or business units, are provided tailored training on OFAC obligations and the compliance program.

"Going forward, these types of compliance commitments will become an essential element in settlement agreements between OFAC and apparent violators," Mandelker said. "Implementation of these commitments will ensure that companies are aware of their OFAC obligations and dedicating sufficient time and resources towards compliance. These resources must go far beyond merely screening the Specially Designated Nationals and Blocked Persons List."

Moving in the right direction

The multi-regulator policy on technology improvements to AML programs was an "unprecedented step" and "great news for banks, who until now have been forced to use antiquated detection systems that generate tens of thousands of alerts each month with 90-plus percent false positive rates, and often fail to identify real crimes," says James Heinzman of ThetaRay, a global cyber-security and big data analytics company that offers an AI solution for financial crime and fraud detection.

"I think the regulators clearly acknowledged that the existing systems just aren't working, and they have to do something different," Heinzman says. The new guidance, he says, will encourage new technology by making it clear that adoption will not necessarily trigger new liabilities for executives in general, and CCOs specifically.

"A concern banks had was if they bring in this new technology, and it finds a bunch of bad stuff that they can't find with existing systems, were they going to get in trouble? Were they going to come in and say, 'Well, you should have found this stuff earlier?' I think the regulators really understood those concerns," Heinzman says. "That is why this is really important guidance. They have recognized that banks struggle with legacy technologies that are not working."

Heinzman notes that the regulatory stance regarding enhancing existing controls with new technologies offers a path for banks to test emerging technologies "to find the ones that really work and leverage them to replace the legacy technology over time."

"Banks are transforming their back offices and moving on to digital platforms," he adds. "When they do that, are they going to carry a 20-year-old legacy system that gets bolted onto a very shiny new digital platform? Probably not. There's a lot of compatibility issues."

Regulators have "given banks some latitude to try different approaches for achieving compliance," Heinzman says. Legacy systems "are flooding banks with false positives and SARs, but a large portion of them are not relevant."

"Compliance isn't the number of Suspicious Activity Reports that you file. Compliance is about finding the bad guys and stopping the activity," he adds, touting the benefits of cutting-edge technology. "We are selling technology, but it's not about the technology. It's not about math. It's not about algorithms. It is really about how we stop human traffickers, terrorists, and drug cartels. How do we stop them from exploiting our financial institutions to launder money and finance financial crime? That's the bottom line." ■

AI in decision making and accountability

Neil Hodge explores AI's impact on corporate decision making.

BRUSSELS—EU data regulators increasingly concerned that management accountability will be impaired if firms delegate too much of their responsibility for decision making to machines. They also admit that this "grey area" presents problems for them about how best to hold companies to account if algorithms, AI, and machine-learning technologies are largely responsible for how personal data is used (or misused).

Speaking at the 40th International Conference of Data Protection and Privacy Commissioners in October, U.K. Information Commissioner Elizabeth Denham said that companies' ability to ensure transparency, fairness, and accountability "remain core" to how personal data is used—and protected—in the digital world, adding that "regulators can't tackle these issues on our own." She also said that firms need to "think seriously" about how they explain to customers and stakeholders that machines are in charge of how people's data is used and for what purpose.

"Companies need to explain to customers, their boards, investors, and regulators why algorithmic solutions are being used to make important decisions, and to what extent," said Denham. "They also need to explain what controls are in place to ensure that the decisions made due to these algorithms are in the company's best interests and that personal data is not being misused in the process." She added: "few companies think about this, currently."

Giovanni Buttarelli, European Data Protection Supervisor, had earlier told attendees at the conference of the need to understand the ethics behind increased around AI usage and how technologies use data to inform decision making. "We are fast approaching a period where design, deployment, and control of new technologies and technological processes are delegated to machines," he warned.

Buttarelli flagged several areas in which algorithmic decision making has been left to machines, such as in killer drones and criminal sentencing, and by social media companies "whose unaccountable algorithmic decision making has been weaponised by bad actors in ethnic conflict zones, with at times appalling human consequences, notably in Myanmar."

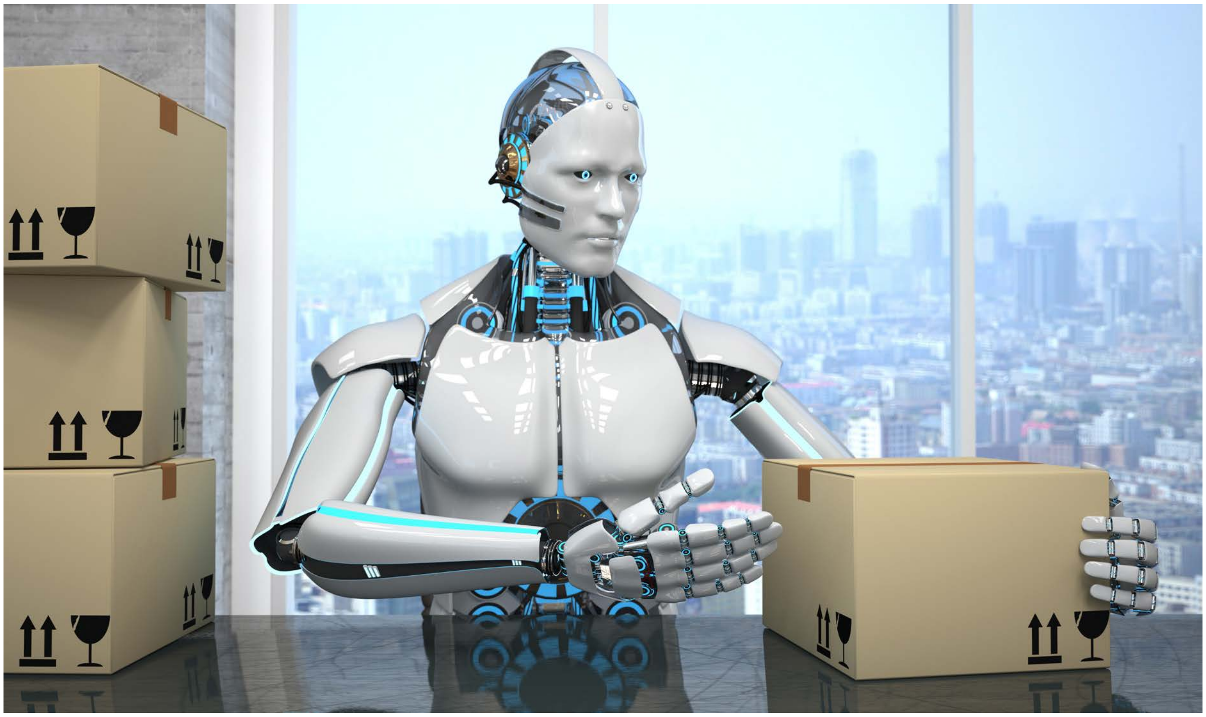
Regulators have already agreed a response. On 23 October data commissioners from several EU member states, as well as Canada, Hong Kong, Argentina, and the Philippines, agreed to a set of guiding principles regarding ethics, monitoring, and enforcement on AI. These underlined that developments and increased use of the technology need to ensure fairness, transparency, and accountability and that users must retain control over their own data.

Leading tech companies are beginning to question their use of personal data, as well as how technology uses it. Apple CEO Tim Cook told attendees that "advancing AI by collecting huge personal profiles is laziness, not efficiency" and said that "platforms and algorithms that promised to improve our lives can actually magnify our worst human tendencies."

In May, Facebook announced that it's testing a tool called "Fairness Flow" that it hopes can determine whether a machine learning algorithm is biased against certain people based on race, gender, or age.

Pascale Fung, professor at the Department of Electronic & Computer Engineering, Hong Kong University of Science and Technology, urged caution when considering regulating algorithms and their development and use.

"When people talk about regulating algorithms, I don't know what they mean," she said. "In terms of design, the same algorithms that have influenced politics on social media are technically similar in many ways to those that are being used to develop breakthroughs in medicine and research. We must not regulate for the sake of regulating. In the long run that can be just as harmful." ■



U.S. considers export controls for AI

The Commerce Department is proposing what may end up being the government's first regulatory regime for the use of artificial intelligence technology, writes **Joe Mont**.

Citing national security concerns, the Commerce Department is proposing initiatives that could impose the government's first regulatory regime for the use of artificial intelligence technology. Other cutting-edge technologies are also under consideration for enhanced export controls, according to a recently published advance notice of proposed rulemaking (ANPR).

The Commerce Department's Bureau of Industry and Security controls the export of "dual-use and less sensitive military items" through export regulations, described in the Defense Production Act of 1950. These responsibilities include the Commerce Control List.

Congress, with the Export Control Reform Act of 2018 (ECRA), authorized the Commerce Department to establish appropriate controls on "emerging and foundational technologies." Under the Act, these technologies are defined as those essential to the national security of the United States and are not already described in the Defense Production Act. Emerging and foundational technologies, as mandated by the ECRA, will be determined by an interagency process that considers both public and classified information, as well as information from BIS' Emerging Technology Technical Advisory Committee and the Committee on Foreign Investment in the United States (CFIUS).

In identifying these technologies, the review process must consider: the development of emerging and foundational technologies in foreign countries; the effect export controls may have on the development of these technologies in the United States; and the effectiveness of export controls on limiting the proliferation of the technologies in foreign countries.

Once identified, the Commerce Department has authority to establish controls on the export, re-export, or transfer (in-country) of these technologies. In determining the appropriate level of export controls, it must consider the potential end-uses and end-users of the technology and countries to which exports from the United States are restricted. While there is discretion to set the level of export controls, at a minimum they must require a license for the export of emerging and foundational technologies to countries subject to a U.S. embargo.

"Controls on exports of technology are a key component of the effort to protect sensitive U.S. technology, [and] many sensitive technologies are listed on the CCL, often consistent with the lists maintained by the multilateral export control regimes of which the U.S. is a member," the ANPR, published in the Federal Register in November 2018, says. "Certain technologies, however, may not yet be listed on the CCL or controlled multilaterally because they are emerging technologies. As such, they have not yet been evaluated for their national security impacts."

The notice of proposed rulemaking seeks public comment on the criteria for identifying emerging technologies that are essential to U.S. national security. Due by Dec. 19, they "will help inform" the process, expected to result in proposed rules for new Export Control Classification Numbers on the Commerce Control List.

Specific emerging technologies the Commerce Department wants to evaluate on the basis of "whether they are essential to the national security of the U.S.," include:

- Artificial intelligence and machine learning technology;
- AI cloud technologies and chipsets;
- biotechnology, genetic engineering, and neurotech;
- computer vision (object recognition, image understanding);
- speech and audio processing (speech recognition and production);
- natural language processing (machine translation);
- audio and video manipulation (voice cloning);
- Position, Navigation, and Timing (PNT) technology;
- microprocessor technology, such as Systems-on-Chip (SoC) or Stacked Memory on Chip;
- data analytics technology, including visualization and context-aware computing;
- micro-drone and micro-robotic systems;
- self-assembling robots and molecular robotics;
- brain-computer interfaces; and
- advanced surveillance technologies, such as: faceprint and voice-print technologies.

Public comments are sought on the following:

- How to define emerging technology to assist identification of such technology in the future.
- Criteria to apply to determine whether there are specific technologies, within the identified general categories (or otherwise), that are important to U.S. national security.
- The development status of these technologies in the United States and other countries.
- The impact specific emerging technology controls would have on U.S. technological leadership.

In addition, the Commerce Department is actively seeking "any other approaches to the issue of identifying emerging technologies important to U.S. national security," including the stage of development or maturity level of an emerging technology, that would warrant consideration for export control. ■

Verify at the speed of life.
Undeniably Dani Steel was approved in 15 seconds for a small-business loan.