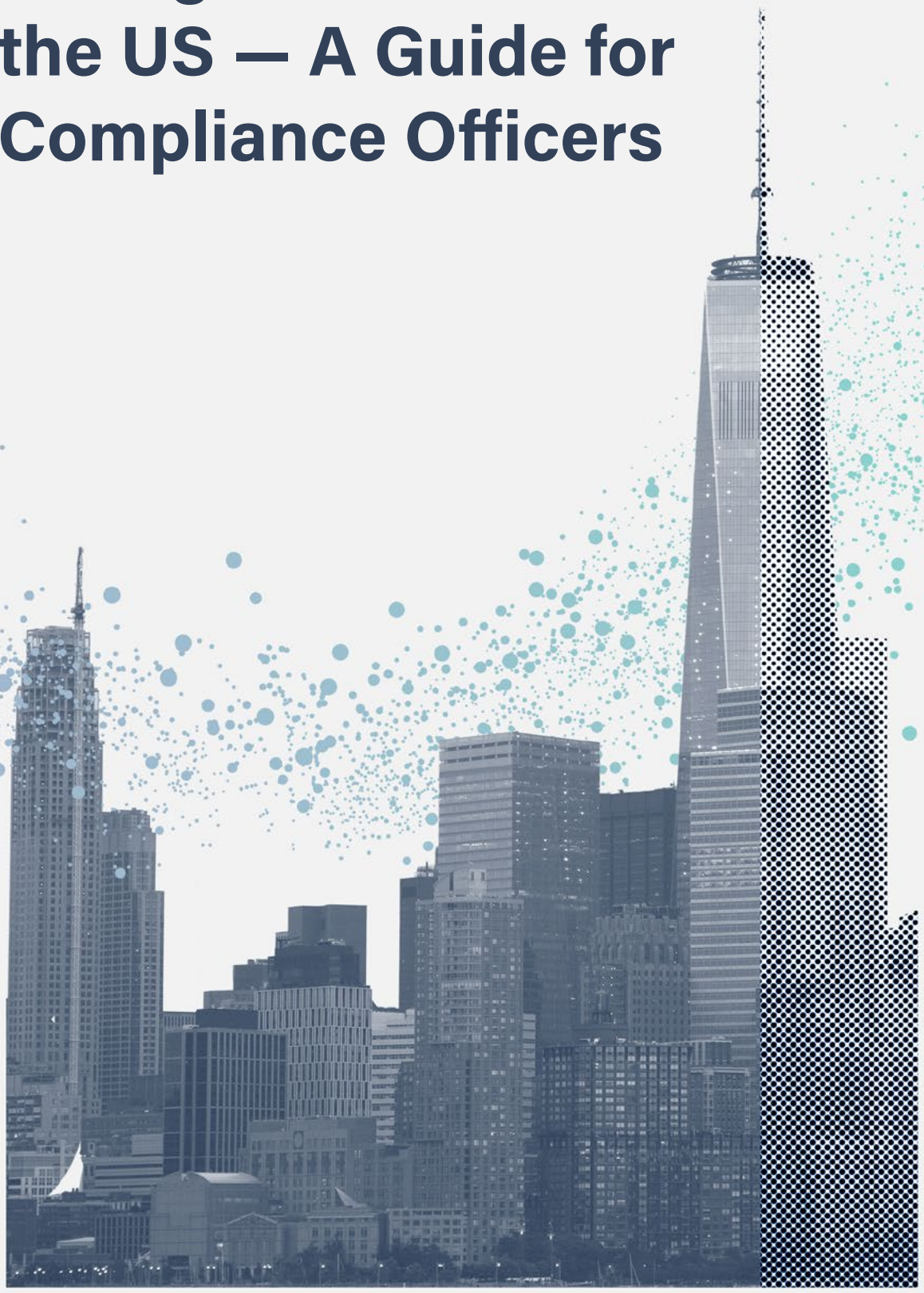
COMPLY ADVANTAGE®

RESISTANT.AI

AI Regulation in the US — A Guide for Compliance Officers



Contents

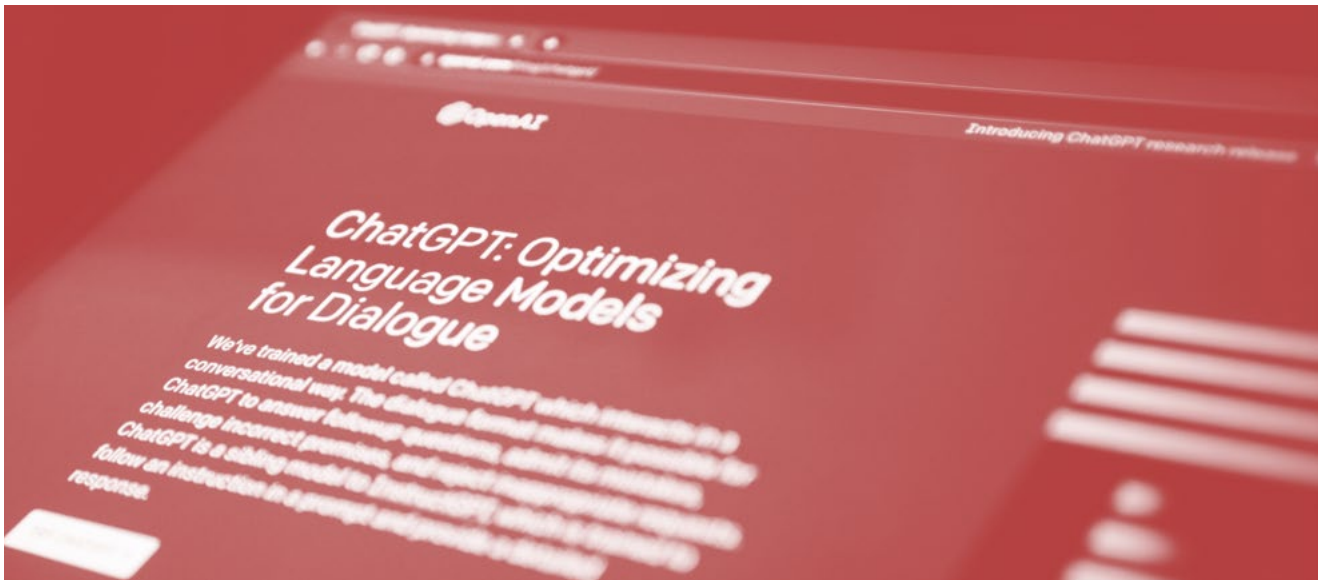
Introduction

2023 may be remembered as the year that ChatGPT went mainstream and when people used artificial intelligence (AI) to clone themselves in virtual settings, fooling their banks and families.[1]

While people are learning how to use AI to gain and share knowledge and increase efficiencies, criminals are also learning how to exploit it. From the use of chatbots to proliferate scams to impersonation fraud using voice-mimicking software, the world is only just beginning to see how AI can be used to profit from crime.[2,3] At the same time, AI is now recognized as a key technology to develop tools to fight crime and money laundering and as a set of technologies that need to be subject to regulation to minimize risks and harms while promoting responsible innovation.[4,5]

AI-based financial crime risk management applications are soaring with clear examples of how and where they can improve efficiency and accuracy. Today, tools are being developed and deployed to support nearly every aspect of a Bank Secrecy Act/anti-money laundering (BSA/AML) program. AI tools can help compliance teams detect risks and patterns that manual processes, traditional rules-based systems, and siloed compliance tools often miss.[6] To date, areas where they have been deployed include customer onboarding using data augmentation, image generation and chatbots for customer service, adverse press and sanctions screening and triaging of alerts, transaction monitoring, and automated reporting to regulators, and the use of large language models, for example, to generate predictive insights based on historical data. The possibilities seem endless.

AI is defined under the US Intelligence Initiative Act 2020 as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to— (A) perceive real and virtual environments, (B) abstract such perceptions into models through analysis in an automated manner, and (C) use model inference to formulate options for information or action."[7] AI effectively automates the execution of actions and tasks traditionally carried out by humans. AI covers a wide array of technologies, including machine learning (ML), natural language processing (NLP), computer vision, the use of large language models, and context-aware computing.[8] AI-based tools can be deployed on-premise or on the cloud, generating a massive market. As a whole, the AI market in the US was valued at around $200 billion in 2022 and is expected to grow to around $2 trillion by 2030.[9]



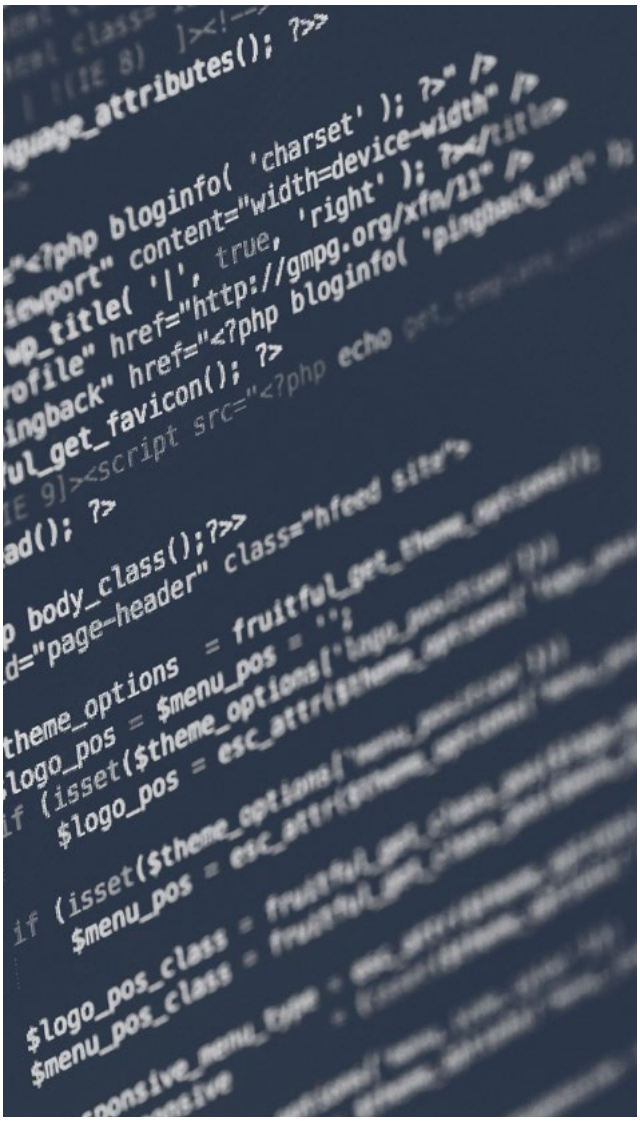
With the drive to digitization during the COVID-19 pandemic, AI adoption skyrocketed. In a survey conducted in 2021, 57% of financial institutions (FIs) indicated that they had AI projects or were looking to implement AI in the next 12-18 months.[10] Reasons for deploying AI include reducing false positives, enhancing behavior analysis through customer segmentation, data enrichment through automation to improve investigations and due diligence, and increasing the ability to detect new risks.[11] A recent survey revealed that 47% of FIs have budget available for AI projects.[12] However, there is a variance in the types of FIs adopting AI, with 62% of FIs having more than $21 billion in assets deploying AI tools compared to only 33% of FIs with less than $21 billion in assets.[13] When implemented properly, AI has led to the identification of more suspicious activity while decreasing the volume of alerts.[14] The introduction of the *Anti-Money Laundering Act of 2020* opened the path for AI adoption in the US by emphasizing the use of "innovative approaches such as machine learning or other enhanced data analytics processes."[15]

On a global basis, the FATF has issued several reports as part of its digital transformation workstream citing the benefits of artificial intelligence as a technology that could improve AML/CFT compliance, increasing efficiencies:[16]

These solutions can automatically monitor, process and analyse suspicious transactions and other illicit activity, distinguishing it from normal activity in real time, whilst reducing the need for initial, front-line human review. AI and machine learning tools or solutions can also generate more accurate and complete assessments of ongoing customer due diligence and customer risk, which can be updated to account for new and emerging threats in real time.[17]

Several partnerships and collaborations are emerging, such as the US-EU Trade and Technology Council and the Global Partnership in AI. AI is being discussed in fora such as the Organization for Economic Co-operation and Development (OECD), the G7, and the G20, and regulators in the EU have issued draft legislation around AI, all of which could offer learnings to the US.

This paper explores the US regulatory environment in 2023, where federal/state laws, regulation and guidance exists, how proposed frameworks are influencing the use of AI by BSA/AML compliance teams, and best practices that BSA/AML compliance teams should consider when adopting AI tools to fight financial crime.



Evolution of the AI legal and regulatory landscape at the national level

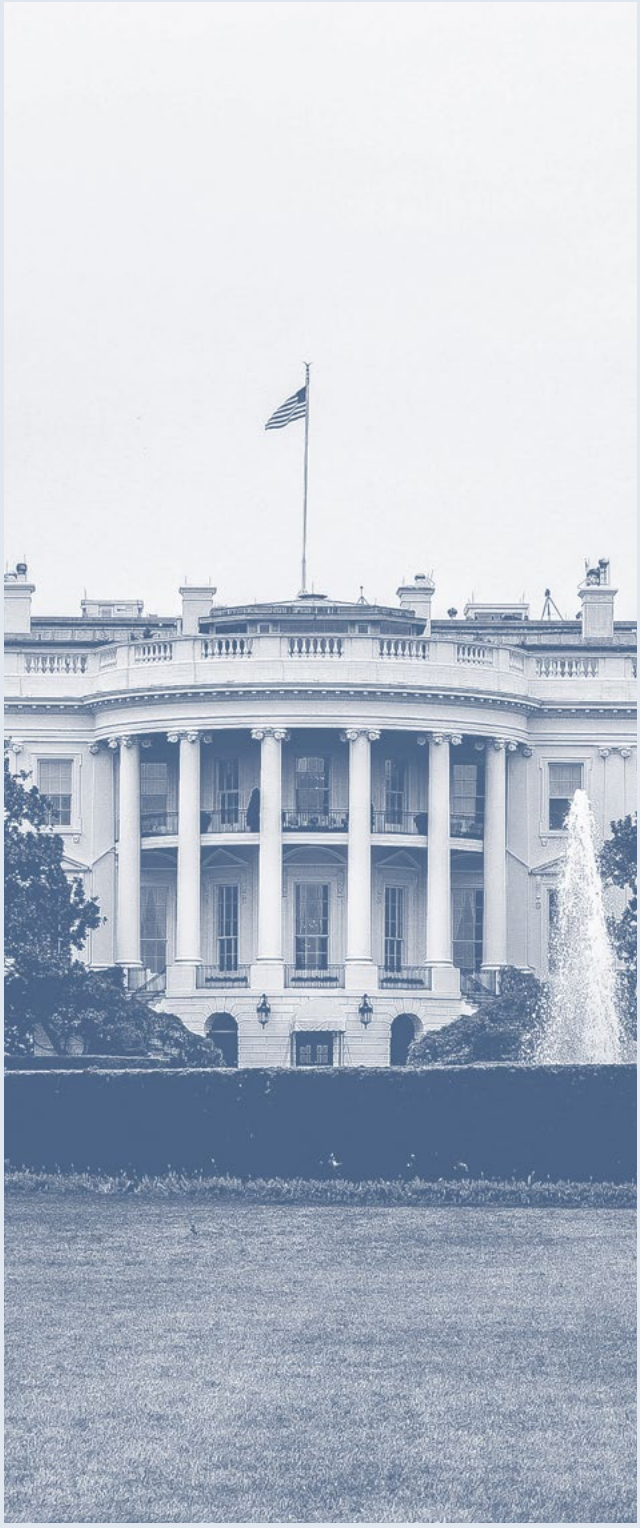
Although AI legislation remains in its infancy in the US, there are numerous initiatives at the federal level relevant to AML/CFT professionals. This includes steps taken by the White House, Congress, regulators, and standard-setting bodies to create a national AI strategy, introduce legislation and guidance, and issue business advisories and frameworks to promote safety, security, and trust in the future development of responsible AI.[18] This work collectively impacts how firms develop in-house AI tools or introduce solutions offered via third parties into their BSA/AML compliance programs. Firms should familiarize themselves with the obligations and guidance issued as they specifically apply to automated systems, bias, and data privacy.

White House Initiatives

The White House recently unveiled an agreement on voluntary AI commitments by some of the largest tech companies.[19,20] The eight commitments fall under the headings of "safety," "security," and "trust" and detail the following actions that firms will look to take: model safety and capability evaluation; greater sharing of information on managing AI risks; investing in cybersecurity and insider threat safeguards; using of 3rd party security checks; applying watermarks to generative AI content; issuing public reports on AI systems including security and societal risks; prioritizing research on risks associated with AI such as harmful bias and discrimination and threats to privacy; and using AI to "address society's greatest challenges."[21,22] While non-binding, firms should look to these as best practice standards to protect consumers and their firms.

The White House also recently released a *Blueprint for an AI Bill of Rights* to protect the rights of Americans.[23] The framework set out in the blueprint focuses on algorithmically generated harmful bias and the need to protect a person's right to privacy. It is applicable to automated systems that "have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services." Given the role that AML/CFT systems and controls play in allowing individuals to access financial, legal, accounting, credit and other services, firms operating in this space should become familiar with the blueprint. The blueprint sets out five principles to guide the "design, use and deployment" of AI. These principles include:

- Safe and Effective Systems – Includes the need for AI systems to go through pre-deployment testing, risk identification and mitigation, ongoing monitoring, mitigating unsafe outcomes and adhering to domain specific standards.
- Algorithmic Discrimination Protections – Includes the need to take proactive steps to design systems in an equitable manner, carry out proactive equity assessments, use representative data for different demographics when designing a system, carry out disparity testing and mitigation and on-going oversight.
- Data Privacy – Includes the need to get consent before data is used, building privacy-by-design features, and safeguards around the use of sensitive data; carrying out pre-deployment assessments in surveillance technologies; and the use of simple data privacy notices.



- Notice and Explanation – Includes providing notices and how automation works in "generally accessible plain language."[24]

- Human Alternatives, Consideration and Fallback – includes offering the ability to opt-out of using automated systems and going through a human-led process, including assessment, remedy and escalation; it also details that automated systems used in sensitive domains (such as criminal justice) should be designed for the intended purpose, allow meaningful access for oversight, require training for persons working with the system, and include human intervention of high-risk decisions, and publicly share "human governance processes" and assessment of their effectiveness.

In 2021, the White House issued an *Executive Order On Advancing Racial Equity and Support for Underserved Communities* requiring federal agencies to identify bias in the deployment of new technologies, such as AI, and to guard against algorithmic discrimination.[25] In May 2023, the White House released an updated Nation AI R&D Strategic Plan, detailing steps to advance the development of responsible AI innovation, which reaffirms the eight key strategies in the 2019 plan and adds the need to "establish a principled and coordinated approach to international collaboration in AI research."[26] In July 2023, the White House announced ongoing work on an Executive Order on AI, revealing limited details but illustrating that AI remains a national priority under the Biden-Harris Administration.[27,28]

Congress

Congress has put forward the *National AI Commission Act*, a bipartisan bill to protect the values and rights of Americans, given the use of AI to advance misinformation campaigns, create deepfakes, enhance biases, and threaten public safety.[29] The Act looks to establish a "blue-ribbon commission" with 20 experts (10 from each party) from industry, government, civil society, and labor to identify and mitigate risks and threats posed by AI. The commission would look to review the current approach to oversight and the regulation of AI by the federal government, issue recommendations on what (and whether a new government agency) is needed to effectively oversee and regulate AI systems, and create a "binding risk-based approach" to identify AI tools that have an "unacceptable" risk and apply risk labels to AI applications.[30]

Congress approved the *National Artificial Intelligence Act of 2020*, which set the framework for the development of strategy and exploration of AI at the federal level.[31] The Act sought to position the United States as a leader in the research and development of AI and "lead the world in the development and use of trustworthy artificial intelligence systems in the public and private sectors."[32] It also looks to prepare the workforce for integrating AI into the economy and coordinate AI-related activities across different agencies in the US. It established a sub-committee on AI and Law Enforcement to provide advice to the president on issues such as bias, including ethical considerations in the use of facial recognition, security of data, and adaptability while mitigating the risk of abuse, and legal standards to address issues linked to data privacy, civil rights and liberties, and disability rights.[33] It also details supporting activities for the Director of the National Institute of Standards and Technology, such as creating best practices and "voluntary standards for trustworthy artificial intelligence systems" to cover numerous activities. These include privacy and security, data management and formats to increase the usability of clean, labeled, and standardized data to train AI, the creation of common computer chips and hardware for AI, safety, and robustness of AI systems, audits, and benchmarks to promote accuracy, transparency, verifiability and safety, documentation of models and systems. It also encourages the creation of "curated, standardized, representative, high-value, secure, aggregate, and privacy-protected data sets for artificial intelligence research, development, and use."[34]

The National Institute of Standards and Technology (NIST) was mandated by the *National Artificial Intelligence Act 2020* to develop an *AI Risk Management Framework* (AI RMF). The AI RMF is a living document that was developed to be agnostic and adaptable to help organizations flag risks and "promote trustworthy and responsible development and use of AI systems."[35] It includes several factors that could increase risks, including the complexity of AI systems, the evolution of the types and forms of data used to train AI systems and the societal influences that affect how AI is designed and deployed. It further emphasizes core concepts in responsible AI, including human centricity, social responsibility, and sustainability.[36] The AI RMF consists of two main parts. Part 1 focuses on how to frame the risks of AI, analyzes risks, and details what makes a trustworthy AI system. This includes ensuring that AI systems are accountable and transparent as well as "valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with…harmful biases managed." Part 2 of the AI RMF describes four processes to help firms manage the risks of AI systems: Govern, Map, Measure, and Manage. Govern is defined as setting a culture of risk management, including clear documentation of risk management policies, processes, procedures, roles, and responsibilities. Map refers to ensuring that the context in which the AI operates is recognized and that risks are identified. Measure refers to ensuring that risks that have been identified are assessed, analyzed, or tracked. Lastly, Manage is about prioritizing and addressing risks.[38]

The Federal Trade Commission

The Federal Trade Commission (FTC) has issued a body of work on AI, including business guidance, warnings, and advisories, and has held hearings on the use of AI. In 2023, it released guidance on how to keep AI claims in check in marketing materials.[39] In 2021, the FTC released a warning to businesses on the use of AI that may inadvertently introduce bias or unfair outcomes in automated decision-making. It flagged three laws for AI developers that address automated decision-making:[40]

- **Section 5 of the FTC Act** - prohibits unfair or deceptive practices, including using AI to influence a sale or use of biased algorithms.
- **Fair Credit Reporting Act** – highlights the potential of an algorithm to result in the denial of services to of certain services or employment, housing, credit, insurance, or other benefits.
- **Equal Credit Opportunity Act** – makes it illegal for a company to use a biased algorithm that results in credit discrimination based on sensitive personal information such as race, color, religion, national origin, sex, marital status, age, or because a person receives public assistance.[41]

In a warning issued to businesses, the FTC shares lessons learned for businesses in using AI.[42] This includes starting with the right data sets, being on the lookout for discriminatory outcomes, and embracing transparency frameworks and independent standards. Firms should also not issue deceptive statements on discriminatory results, be truthful about how data is used specifically for facial recognition algorithms, ensure that the model does "more good than harm," and be accountable for how the algorithm performs.

Additionally, the FTC published a 2020 *Business Guidance on Using Artificial Intelligence and Algorithms*.[43] The guide calls on businesses to be transparent about how automated tools are used to collect sensitive data and may require publication of an "adverse action" notice if using an automated decision tool provided by a third-party vendor to make them aware of their right to see the information collected as part of the process. This is particularly relevant for firms relying on credit bureau agencies using AI to verify addresses and identities. It also recommends that businesses explain decisions to their customers, including risk scores, requiring that they know what data is used and how that data is used when denying business services. This must be balanced with AML/CFT requirements and "tipping off" obligations under the Bank Secrecy Act (BSA). Businesses should also ensure that their decisions are "fair" to guard against discrimination, which may be particularly relevant to classes of customers. The guide also requires that data models should be robust and empirically sound and calls on businesses to be "accountable for compliance, ethics, fairness, and non-discrimination."[44] The FTC has also issued a 2016 report on big data analytics and machine learning[45] citing concerns around exclusion, and has held a hearing on The Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence, and Predictive Analytics exploring ethical considerations around AI.[46]

Federal Reserve and OCC

The Federal Reserve issued *Guidance on Model Risk Management* in 2011 that applies to the deployment of AI by organizations subject to supervision by the Federal Reserve.[47] The guidance calls on banks to remain aware of the negative impact of the decisions made by automated models and mitigate those through proactive risk management. It provides information about model development, implementation, and use, as well as model validation, to ensure that inputs, processing, outputs, and reports developed by a model are executed in line with anticipated business use and objectives and that the model performs as expected. The Federal Reserve also stipulates that firms should have documented governance, policies, and controls around model risk management.

More recently, in August 2021, the Office of the Comptroller of the Currency issued a Model Risk Management document. The document was developed for OCC examiners and provides details on how examiners will carry out model risk management examinations, including principles on model risk management; details on strategic, operational, reputational, and compliance risks (amongst other types of risks); and effective risk management, which also covers governance (including model inventory), model development, implementation and use, model validation, third party risk management and IT systems. This provides an excellent resource for BSA/AML compliance teams looking to build or adopt AI tools.[48]

State-level AI legislation and regulation

As AI law is considered at the federal level, numerous states have issued specific laws that firms should be aware of as they may impact the use of AI in AML/CFT programs. Firms operating across the US should be aware that there has been a 46% increase in the number of AI-related bills introduced by state legislators.[49] The variety of legislation enacted and being proposed has potential implications for federal regulation and could lead to regulatory arbitrage where divergences exist. However, most laws currently enacted relate to data protection, profiling, and automated decision-making and require impact assessments to detect high-risk activity to consumers. Although the language may vary by state, there is some overlap. The laws also cover various topics and set precedents for future AI regulation. This includes topics such as consumer protection, user data and security, the use of bots, preventing bias, and requirements around the use of automated decision systems (ADS) for monitoring of employees to protect employee safety. These pieces of legislation have implications for using facial recognition as part of onboarding and automated decision-making and profiling around risk assessments, triaging of alerts and matches during adverse press and sanctions screening, and transaction monitoring solutions using AI.

The table below summarizes state laws that have been enacted:

	Legislation	Description
California	SB 1001, The Bolstering Online Transparency Act (BOT) (2018)[50]	Defines bots and makes it illegal to use bots to strongly encourage the sale of goods and services.
	California Consumer Privacy Act (2018)[51]	Relates to profiling and automated decision-making, allowing consumers to opt-out, and requires the identification of "significant risks" to consumer's privacy and security.
Connecticut	Connecticut Privacy Act (CTPA) (2023)[52]	Relates to profiling and automated decision-making, allowing consumers to opt-out, and requires data risk assessments to identify "heightened risk of harm."
Colorado	SB 21-169, Protecting Consumers from Unfair Discrimination in Insurance Practices (2021)[53]	Protects consumers from algorithms and predictive models that use external consumer data and information sources (ECDIS) that "unfairly discriminate" to dissuade bias.
	Colorado Privacy Act (CPA)[54]	Relates to profiling and automated decision-making, allowing consumers to opt out of having their personal data processed, and requires that data protection impact assessments (DPIAs) are carried out and the identification of "heightened risk of harm to a consumer."[55]
Illinois	Illinois AI Video Interview Act (2022)[56]	Requires notification on the use of AI and explainability in hiring practices during video interviews.
Indiana	SB5 Consumer Data Protection (2023)[57]	Relates to profiling and automated decision-making and data protection, allowing consumers to opt-out of having their personal data processed.
Maryland	HB 1202[58]	Forbids the use of facial recognition services by employers during interviews without explicit consent.
Montana	SB384, An act establishing the Consumer Data Privacy Act (2023)[59]	Regulates the collection and processing of personal data, profiling and automated decision-making.
New York	Local Law 144 A Local Law to amend the administrative code of the city of New York, in relation to automated employment decision tools (2021)[60]	Introduced reporting obligations and notification on the use of automated employment decision tools (AEDTs) and requires audits to identify the bias of AI-tools used for employment decisions.
Tennessee	SB73[61] HB1181[62] The Tennessee Information Protection Act	Relates to profiling and automated processing and data protection, allowing consumers to opt-out and requires a data protection assessment.in connection to profiling
Texas	HB1844 Texas Data Privacy and Security Act[63]	Relates to profiling and automated decision-making, allowing consumers to opt-out, and requires data protection assessment for high-risk profiling activities.

The table below summarizes state laws that have been proposed:

	Legislation	Description
California	AB331 Automated Decision Tools[64]	Requires an impact assessment of automated decision tools by the developer and deployer of such tools.
Connecticut	SB1103 An Act Concerning Artificial Intelligence, Automated Decision-Making and Person data Privacy (2023)[65]	Looks to establish an Office of Artificial Intelligence, establish a taskforce to study artificial intelligence, develop an AI bill of rights and prohibits the processing of personal data for targeted marketing.
District of Columbia	B114, Stop Discrimination by Algorithms Act of (SDAA) (2023)[66]	Prohibits automated decision making by algorithms based on "protected personal traits" to prevent bias.
Maine	Data Privacy and Protection Act, HP 1270[67]	Data privacy and data protection legislation that requires impact assessments on the use of algorithms. It also requires the creation of a design evaluation of algorithms including the design, structure and inputs of the algorithms.
Massachussetts	Massachusetts Data Privacy Protection Act (MDPPA) SD745[68] & HD2281[69]	Requires impact assessments if a company uses "covered algorithms."
	Massachusetts Information Privacy and Security Act (MIPSA) SD1971[70] & HD3263 (2023)[71]	Requires issuance of a privacy notice to collect personal data and defines additional data privacy rights and requirements for "large data holders."
	H1873, An Act Preventing A Dystopian Work Environment (2023)[72]	Requires that workers are provided with notice before the employer uses an Automated Decision System and review of data accuracy.
	SB31, An Act drafted with the help of ChatGPT to regulate generative artificial intelligence models like ChatGPT (2023)	Looks to introduce operating standards for companies operating large-scale language models, including data protection, informed consent, and regular risk assessments.
New Hampshire	SB 255 relative to the expectation of privacy (2023)[73]	Relates to profiling, automated decision-making and data protection, allowing consumers to opt-out of having their personal data processed and required a data protection impact assessment.
New Jersey	S1402 Prohibits certain discrimination by automated decision systems (2022)[74]	Prohibits discrimination by an automated decision system (ADS) in the provision of financial, insurance or health services.
Oregon	SB619, relating to protections for the personal data of consumers (2023)[75]	Relates to profiling and automated decision-making and data protection, allowing consumers to opt-out of having their personal data processed and required a data risk assessment.
Pennsylvania	HB49[76]	Would require the creation of an AI business registry.
	HB708[77]	Relates to profiling and automated processing and data protection, allowing consumers to opt-out and requires a data protection assessment.
Rhode Island	HB62236 Rhode Island Data Transparency And Privacy Protection Act (2023)[78]	Relates to profiling and automated processing and data protection, allowing consumers to opt-out and requires a data protection assessment in connection to profiling.
South Carolina	SB404[79]	Will prohibit operators on internet-based applications from using "automated decision systems" to place content on social media platforms for users under eighteen.
	HB2060 (2023)[80]	Will look to create an advisory council for AI.
Vermont	H1114 (2023)[81]	Will limit the use of automated decision systems (ADSs) to monitor employees and make employment-related decisions.
Virginia	Virginia Consumer Data Protection Act (VCDPA) (2023)	Relates to profiling and automated decision-making, allowing consumers to opt-out, and requires data protection impact assessment for high-risk profiling activities.

AI in BSA/AML and sanctions compliance programs guidance

With regards to fraud and AML/CFT specific guidance, both the Financial Crimes Enforcement Network (FinCEN) and the Office for Foreign Assets Control (OFAC) have signaled to industry that they welcome the use of AI in financial crime prevention. International organizations, such as the global AML/CFT standard setter, the FATF, have also addressed AI in various publications.[82]

In a 2018 statement that focused on innovation, FinCEN recognized that new technologies, including AI and innovation, could "potentially augment aspects of banks' BSA/AML compliance programs, such as risk identification, transaction monitoring, and suspicious activity reporting."[83] Benefits listed for using AI included strengthening approaches to BSA/AML compliance, enhancing transaction monitoring, and maximizing using BSA/AML resources. FinCEN warned, however, that using innovation and new technologies must align with a firm's risk profile. Moreover, banks must assess whether and when new technology solutions are developed enough to replace or enhance existing BSA/AML compliance programs. Factors to consider include information security, third-party risk management, data privacy, customer notifications, and any other legal or regulatory requirements. Banks should discuss innovative approaches with regulators, and FinCEN comments that engaging with regulators early may generate a better understanding amongst supervisors and also allow them to set expectations around compliance and risk management.

FinCEN further highlighted the importance of pilot programs in "testing and validating" the effectiveness of new tech and innovation.[84] Concerning its own role, FinCEN stated that pilot programs should not lead to criticism from supervisors or supervisory action if they unveil gaps or issues in a bank's BSA/AML compliance program. More specifically, if a bank uncovers suspicious activity using AI-based transaction monitoring that it has not previously uncovered, FinCEN has advised that supervisors will not deem existing processes deficient. FinCEN further indicated that it would "encourage responsible, innovative approaches to BSA/AML compliance programs," including via FinCEN's Bank Secrecy Act Advisory Group.[85]

In 2022, OFAC issued a guidance for instant payments that briefly discusses AI's role in a sanctions compliance program.[86] OFAC recognizes that technology solutions have evolved, are increasingly sophisticated and scalable, and can be used to manage sanctions risk. OFAC encourages using emerging technologies, specifically citing AI tools that may improve sanctions screening while decreasing the number of false positives, to manage sanctions risks. Technology solutions could be particularly useful in the instant payments space, where the value, velocity, and volume of payments continue to increase exponentially. OFAC states that tools should only be introduced following a risk assessment, that there should be processes to allow for the effective review of alerts of sanctions concerns, and that instant payment systems should allow exception processing, allowing enough time to investigate potential sanctions breaches.

OFAC is clear that it encourages "the development and deployment of innovative sanctions compliance approaches and technologies to address identified risks" but emphasizes the need to take a risk-based approach to sanctions risk management.[87] It additionally sets out key components of a sanctions compliance program, which include the following: commitment from management, execution of a risk assessment, setting up internal controls, carrying out testing and auditing, and conducting training. These are further detailed in a Framework for OFAC Compliance Commitments,[88] which must also be considered when developing or adopting sanctions compliance technology solutions. It further references the OFAC Risk Matrix[89] that should be used by firms to assess their sanctions compliance programs and should be taken into consideration when introducing new technology solutions, including AI. These include but are not limited to: the international presence of a firm, customer profile and exposure, products and services on offer, and the size and complexity of the business.

What do the regulations mean for financial crime, and how can firms prepare for their future obligations?

AI-based technologies are being developed and deployed to support nearly every aspect of financial crime compliance today.

The US government's commitment to more effective oversight and greater regulation of AI will impact how firms use AI-based technologies in their financial crime compliance programs. Preparing for this inevitable increase in regulation will require a thorough understanding of current regulatory requirements and a strong awareness of what's on the horizon.

A common goal

While the regulatory landscape is fragmented, there is a common goal across federal and state regulation and guidance: to ensure responsible development and use of AI-based technology and adhere to the core principles of safety, security, and trust.[90]

Steps to prepare for increases in regulation

It is prudent for firms to take action in the short term to put themselves in a strong position to meet future regulations with greater ease. The below are suggested steps:

Increase Knowledge and Awareness of AI

All regulations and guidance clearly show that firms using or developing AI-based technology must understand the risks and limitations associated with applications of such technologies so they can be effectively managed and mitigated.

- Increase the financial crime team's knowledge of AI. Upskilling teams to better understand AI can foster safe and responsible use while ensuring a greater understanding of how to comply with regulatory obligations effectively.
- Assign responsibility for staying informed about emerging AI regulations at the federal and state levels and their impact on existing or proposed use of AI. This should include monitoring regulatory bodies, industry publications, and policy updates to anticipate future changes and ensure the team can fully assess and prepare for such changes.
- Collaborate closely with internal experts and leverage internal expertise such as legal counsel to assess the impact of future regulations on AI in development or use by your financial crime team.

Leverage Existing Frameworks

- A firm's approach to using AI in financial crime can fall under existing risk management practices. Firms should therefore leverage or evolve existing risk management frameworks, where possible. For example, other non-AI-based applications may already be governed and managed internally in line with frameworks applicable to AI-based technologies, such as the Federal *Reserve's Guidance on Model Risk Management and the OCC's Comptroller's Handbook - Model Risk Management*.
- Firms can also draw from relevant external resources on AI to guide their approach, such as the National Institute of Standards and Technology's (NIST) publication on the *AI Risk Management Framework Version 1.0*. These voluntary frameworks are highly relevant to all firms and provide useful guidance in managing the risks of AI and promoting trustworthy AI systems.

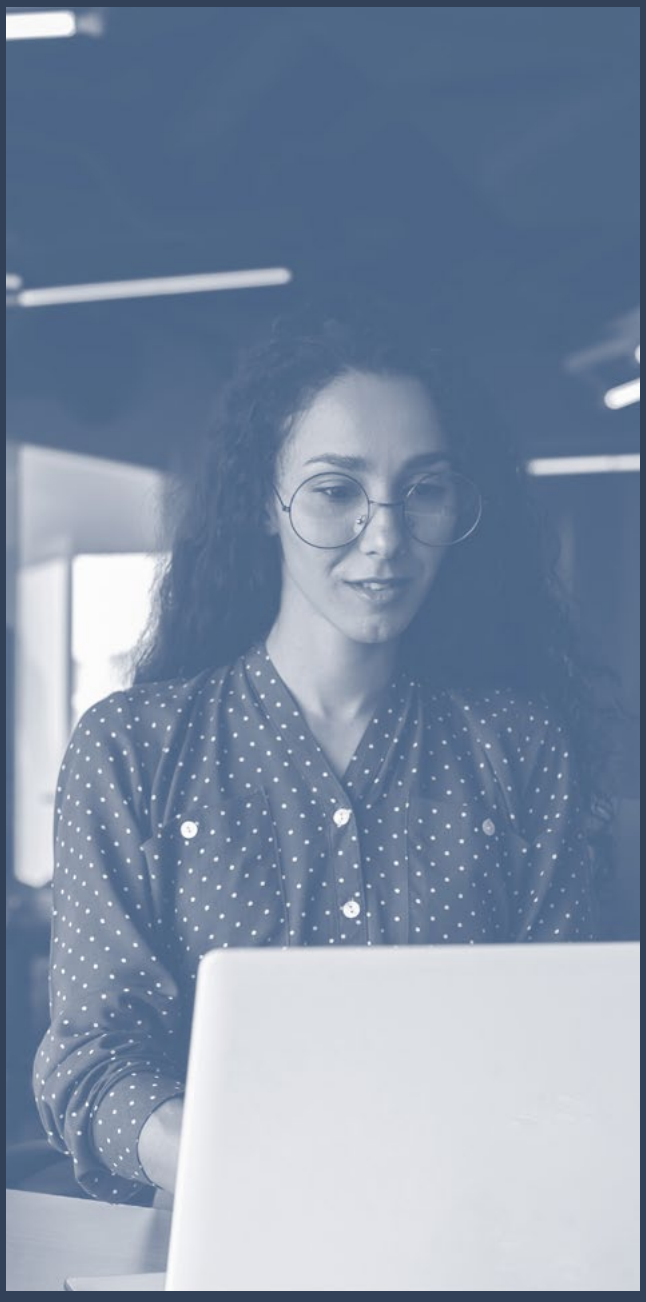
Maintain human centricity

Firms must foster the responsible design, development, and use of AI over time. Keeping humans at the center is key to this - human intervention and oversight reduce the risk of unfair outcomes and build trust. There is very little appetite in the financial crime community for fully unsupervised AI to be brought to bear. Smart organizations will use AI's power to complement and enhance financial crime controls that remain defined by and governed by humans. Responsibility and accountability should always be assigned in all cases of design, development, and use of AI.

Start today to avoid being left behind

Whether firms are using AI in their financial crime programs or not, AI is almost certain to play a role in the future. Taking steps to increase knowledge and understanding will facilitate the adoption of AI tools that can enable a truly risk-based approach to financial crime risk management.

Firms should be proactive and prepared to demonstrate their commitment to responsible, well-governed AI to regulatory authorities. Being able to demonstrate to regulators that effective financial crime risk management controls are in place should be at the forefront of the minds of compliance officers.



Next steps: Best practices for deploying AI-based applications in BSA/AML compliance

When deploying AI-based applications in BSA/AML compliance, firms must ensure that they adhere to the three principles in developing responsible AI: safety, security, and trust.[91] Below are best practices for firms to follow when introducing AI into their BSA/AML and sanctions compliance programs.

1. Obtain senior management support and document governance frameworks

BSA/AML compliance departments must ensure they have senior management support for developing or building an AI tool. Senior management should create an environment that enables "responsible innovation to enhance effective AML/CFT."[92] This includes documenting decisions taken to introduce AI into an organization and having a business sponsor to support the deployment of such tools. Firms should also ensure senior management has an open dialogue with regulators to inform them of the technology solution being introduced into the business and how they manage risks. This should also be run as a formal project, with clear avenues for reporting delays and identified risks and escalation processes to raise issues. Roles and responsibilities for different teams, including responsibility for training, should also be documented.

2. Determine use cases

When determining whether to deploy an AI tool, firms should first identify the relevant use case for AI. This could include the need to clear and/or prioritize adverse press, PEP, or sanctions alerts, identify connected entities, carry out perpetual KYC/CDD, or even improve the ability to detect suspicious activity. Firms should look to identify whether the volumes of customers and/or transactions justify the deployment of AI and whether they have enough data to train and/or test AI models.

3. Identify data sources, data management processes, and internal systems

Firms should identify databases where information is held and assess the quality and cleanliness of data to be used. Where necessary, firms should employ techniques to make data more useable such as systematic data cleansing activities, labeling, and standardizing data in formats that can be used to train AI, where supervised models are used. BSA/AML teams should work with relevant data management and IT security teams to ensure data management processes are in place. This should include data processing risk assessments and an understanding of whether customers can opt out of having their data used. Where the AI will be linked to an internal system, firms should ensure that there is documentation that details connections and interdependencies between systems and any potential issues that may arise.[93]

4. Carry out risk assessments and develop risk management processes for AI

Given the emphasis placed on the risk-based approach to managing AML/CFT risk, firms must ensure that their decision to deploy specific AI models aligns with their documented risk assessment. Firms should document identified risks and controls to mitigate risks. Firms should also consider building risk management processes to identify, track, and measure emerging risks associated with AI. This should include: understanding risk exposure of software, hardware, and data provided by a third party; identifying, measuring, and tracking risks on an ongoing basis; understanding metrics used or developing human baseline metrics to assess AI risks; and recognizing when AI tools have limited transparency or documentation as well as limited interpretability or explainability of processes and outcomes.[94] Firms should also look to understand the safety and robustness of artificial

intelligence systems by understanding steps taken around assurance, verification, validation, security, control, and how AI tools can protect against unexpected inputs and external attacks.[95] Firms should also consider additional resources, such as those issued by the Federal Reserve and the OCC on model risk management.[96]

5. Complete due diligence on your vendor

In addition to carrying out traditional due diligence on your vendor (identify and verify address and registration), firms should look to understand the level of experience in building AI models, ethics applied to developing models, and the context in which it was built and deployed. Firms should ensure that vendors can share documentation around the AI model, which should include "performance metrics and constraints, measures of fairness, training and testing processes, and results."[97]

6. Carry out extensive model validation and bias prevention activities

Firms should look to understand the type of data and demographics used to train the AI system. Firms should seek to understand what steps were taken to include unbiased data to avoid automating prejudice. This includes reviewing the legitimacy and credibility of the data sources used, carrying out model validation extensively, and monitoring models on an ongoing basis.[98]

7. Test AI tools in a secure environment and build appropriate safeguards

Firms should ensure that they test their AI tools as part of a proof of concept or in a sandbox testing environment. They should build in appropriate safeguards for the deployment of AI such as allowing human intervention, human oversight, explainability and transparency, data privacy and data protection measures, and cybersecurity.[99] Firms should also consider how to update or replace legacy systems safely and securely.

8. Carry out ongoing monitoring and assurance

Firms should ensure that they are carrying out ongoing assurance testing and audits to check that AI tools continue to operate safely, return accurate results, remain transparent, and are verifiable. This should include validating that the AI tool continues to operate as expected and should include a review of model design and documentation. Audits should also consider any product changes, client types, or markets and assess whether the AI tool remains relevant to new environments.

How do ComplyAdvantage and Resistant AI approach AI-based financial crime risk detection?

One of the distinguishing features of our solution is how we address explainability. Our solution has been designed with explainability at its core, and our approach to detecting financial crime - the ensemble approach - has explainability features embedded to provide full transparency into the potential financial crime risks surfaced by AI. This allows the end user to fully understand and assess the risks, ultimately building the user and the organization's confidence in AI.

Each model output has human-readable explanations of why the behavior was flagged. This builds trust and supports inclusivity and fairness, as the models and their results can be more effectively governed and scrutinized - the additional information provided helps the analyst or developer better understand the model and identify potential bias.

Table of State Legislation

	Legislation	Description	Status of Legislation
California	SB 1001, The Bolstering Online Transparency Act (BOT) (2018)[100]	Defined bots and makes it illegal to use bots to encourage the sale of goods and services	Enacted
	California Consumer Privacy Act (2018)[101]	Relates to profiling and automated decision-making, allowing consumers to opt out, and requires the identification of "significant risks" to consumer's privacy and security	Enacted
	AB331 Automated Decision Tools[102]	Requires an impact assessment of automated decision tools by the developer and deployer of such tools.	Pending
Connecticut	Connecticut Privacy Act (CTPA) (2023)[103]	Relates to profiling and automated decision-making, allowing consumers to opt-out, and requires data risk assessments to identify "heightened risk of harm"	Enacted
	SB1103 An Act Concerning Artificial Intelligence, Automated Decision-Making and Person data Privacy (2023)[104]	Looks to establish an Office of Artificial Intelligence, establish a task for to study Artificial Intelligence, develop an artificial intelligence bill of rights and prohibits the processing of personal data for targeted marketing.	Proposed
Colorado	SB 21-169, Protecting Consumers from Unfair Discrimination in Insurance Practices (2021)[105]	Protects consumers from algorithms and predictive models that use external consumer data and information sources (ECDIS) that "unfairly discriminate" to dissuade bias.	Enacted
	Colorado Privacy Act (CPA)[106]	Relates to profiling and automated decision-making, allowing consumers to opt-out of having their personal data processed, and requires that data protection impact assessments (DPIAs) are carried out and the identification of "heightened risk of harm to a consumer"[107]	Enacted
District of Columbia	B114, Stop Discrimination by Algorithms Act of (SDAA) (2023)[108]	Prohibits automated decision making by algorithms based on "protected personal traits" to prevent bias	Proposed
Illinois	Illinois AI Video Interview Act (2022)[109]	Requires notification on the use of AI and explainability in hiring practices during video interviews	Enacted
Indiana	SB5 Consumer Data Protection (2023)[110]	Relates to profiling and automated decision-making and data protection, allowing consumers to opt-out of having their personal data processed	Enacted
Maine	Data Privacy and Protection Act, HP 1270[111]	Data privacy and data protection act that requires impact assessments on the use of algorithms. It also requires the creation of a design evaluation of algorithms including the design, structure and inputs of the algorithms.	Proposed
Maryland	HB 1202[112]	Forbids the use of facial recognition services by employers during interviews without explicit consent	Enacted
Massachussetts	Massachusetts Data Privacy Protection Act (MDPPA) SD745[113] & HD2281[114]	Requires impact assessments if a company used "covered algorithms"	Proposed
	Massachusetts Information Privacy and Security Act (MIPSA) SD1971[115] & HD3263 (2023)[116]	Requires issuance of a privacy notice to collect personal data and defines additional data privacy rights and requirements for "large data holders"	Proposed
	H1873, An Act Preventing A Dystopian Work Environment (2023)[117]	Requires that workers are provided with notice before the employer uses an Automated Decision System and review of data accuracy	Proposed
	SB31, An Act drafted with the help of ChatGPT to regulate generative artificial intelligence models like ChatGPT (2023)	Looks to introduce operating standards for companies operating large-scale language models, including data protection, informed consent, and regular risk assessments.	Proposed

	Legislation	Description	Status of Legislation
Montana	SB384, An act establishing the Consumer Data Privacy Act (2023)[118]	Regulates the collection and processing of personal data, profiling and automated decision-making.	Enacted
New Hampshire	SB 255 relative to the expectation of privacy (2023)[119]	Relates to profiling and automated decision-making and data protection, allowing consumers to opt-out of having their personal data processed and required a data protection impact assessment	Proposed
New Jersey	S1402 Prohibits certain discrimination by automated decision systems (2022)[120]	Prohibits discrimination by an automated decision system (ADS) in the provision of financial, insurance or health services	Proposed
New York	Local Law 144 A Local Law to amend the administrative code of the city of New York, in relation to automated employment decision tools (2021)[121]	Introduced reporting obligations and notification on the use of automated employment decision tools (AEDTs) and requires audits to identify bias of AI-tools used for employment decisions.	Enacted
Oregon	SB619, relating to protections for the personal data of consumers (2023)[122]	Relates to profiling and automated decision-making and data protection, allowing consumers to opt-out of having their personal data processed and required a data risk assessment	Proposed
Pennsylvania	HB49[123] HB708[124]	Would require the creation of an AI business registry. Relates to profiling and automated processing and data protection, allowing consumers to opt-out and requires a data protection assessment.	Proposed Proposed
Rhode Island	HB62236 Rhode Island Data Transparency And Privacy Protection Act (2023)[125]	Relates to profiling and automated processing and data protection, allowing consumers to opt-out and requires a data protection assessment.in connection to profiling	Proposed
South Carolina	SB404[126]	Will prohibit operators on internet-based applications from using "automated decision systems" to place content on social media platforms for users under eighteen	Proposed
Tennessee	SB73[127] HB1181[128] The Tennessee Information Protection Act	Relates to profiling and automated processing and data protection, allowing consumers to opt-out and requires a data protection assessment in connection to profiling	Enacted
Texas	HB1844 Texas Data Privacy and Security Act[129] HB2060 (2023)[130]	Relates to profiling and automated decision-making, allowing consumers to opt-out, and requires data protection assessment for high-risk profiling activities Will look to create an advisory council for AI	Enacted Proposed
Vermont	H1114 (2023)[131]	Will limit the use of automated decision systems (ADSs) to monitor employees and make employment-related decisions.	Proposed
Vermont	Virginia Consumer Data Protection Act (VCDPA) (2023)	Relates to profiling and automated decision-making, allowing consumers to opt-out, and requires data protection impact assessment for high-risk profiling activities.	Proposed

About Resistant AI

Founded in 2019, Resistant AI uses AI and machine learning to provide identity forensic solutions that protect automated financial services from fraud and manipulation, including customer onboarding, AML and existing fraud detection systems. The Resistant AI founding team has a deep background in machine learning, artificial intelligence and computer security with more than 15 years of experience applying AI in the computer security domain. Backed by GV (formerly Google Ventures), Index Ventures, Credo Ventures, Seedcamp, Notion, and several angel investors specializing in financial technology and security, Resistant AI is headquartered in Prague with offices in London and New York.

Visit resistant.ai to learn more.

About ComplyAdvantage

ComplyAdvantage is the financial industry's leading source of AI-driven financial crime risk data and detection technology. ComplyAdvantage's mission is to neutralize the risk of money laundering, terrorist financing, corruption, and other financial crime. More than 500 enterprises in 75 countries rely on ComplyAdvantage to understand the risk of who they're doing business with through the world's only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day. ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj-Napoca and is backed by Ontario Teachers', Index Ventures and Balderton Capital. Learn more at:

complyadvantage.com

Get in Touch

EMEA
London

+44 20 7834 0252

AMER
New York

+1 (646) 844 0841

APAC
Singapore

+65 6304 3069

References

[1] https://www.wsj.com/articles/i-cloned-myself-with-ai-she-fooled-my-bank-and-my-family-356bd1a3
[2] How AI could transform the future of crime | UK News | Sky News
[3] ai_crime_policy_0.pdf (ucl.ac.uk)
[4] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf
[5] AI Regulation Is Coming To The U.S., Albeit Slowly (forbes.com)
[6] AML and AI: How AI is Changing the AML Landscape | ComplyAdvantage
[7] PUBL283.PS (congress.gov)
[8] https://www.precedenceresearch.com/artificial-intelligence-market#:~:text=The%20global%20artificial%20intelligence%20(AI,USD%20167.30%20 billion%20in%202022.
[9] Artificial Intelligence - Global | Statista Market Forecast
[10] Acceleration through adversity (sas.com)
[11] Acceleration through adversity (sas.com)
[12] The state of AI adoption in AML | SymphonyAI Sensa-NetReveal
[13] The state of AI adoption in AML | SymphonyAI Sensa-NetReveal
[14] Google Cloud Launches AI-Powered Anti Money Laundering Product for Financial Institutions (prnewswire.com)
[15] BILLS-116hr6395enr.pdf (congress.gov)
[16] OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT (fatf-gafi.org)
[17] OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT (fatf-gafi.org)
[18] FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI | The White House
[19] A.I. Regulation Is in Its 'Early Days' - The New York Times (nytimes.com)
[20] Ensuring-Safe-Secure-and-Trustworthy-AI.pdf (whitehouse.gov)
[21] FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI | The White House
[22] Ensuring-Safe-Secure-and-Trustworthy-AI.pdf (whitehouse.gov)
[23] Blueprint for an AI Bill of Rights | OSTP | The White House
[24] Blueprint for an AI Bill of Rights | OSTP | The White House
[25] FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI | The White House
[26] National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf (whitehouse.gov)
[27] A.I. Regulation Is in Its 'Early Days' - The New York Times (nytimes.com)
[28] National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf (whitehouse.gov)
[29] national-ai-commission-act-one-pager.pdf (house.gov)
[30] national-ai-commission-act-one-pager.pdf (house.gov)
[31] PUBL283.PS (congress.gov)
[32] PUBL283.PS (congress.gov)
[33] PUBL283.PS (congress.gov)
[34] PUBL283.PS (congress.gov)
[35] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
[36] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
[37] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
[38] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
[39] Keep your AI claims in check | Federal Trade Commission (ftc.gov)
[40] Aiming for truth, fairness, and equity in your company's use of AI | Federal Trade Commission (ftc.gov)
[41] Aiming for truth, fairness, and equity in your company's use of AI | Federal Trade Commission (ftc.gov)
[42] Aiming for truth, fairness, and equity in your company's use of AI | Federal Trade Commission (ftc.gov)
[43] Using Artificial Intelligence and Algorithms | Federal Trade Commission (ftc.gov)
[44] Using Artificial Intelligence and Algorithms | Federal Trade Commission (ftc.gov)
[45] Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues (FTC Report) | Federal Trade Commission
[46] FTC Hearing #7: The Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence, and Predictive Analytics | Federal Trade Commission
[47] SR 11-7 attachment: Supervisory Guidance on Model Risk Management (federalreserve.gov)
[48] Model Risk Management, Comptroller's Handbook (treas.gov)
[49] The United States' Approach to AI Regulation: Key Considerations for Companies – Publications (morganlewis.com)
[50] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001
[51] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
[52] https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF
[53] https://leg.colorado.gov/bills/sb21-169
[54] https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf
[55] US state-by-state AI legislation snapshot | Bryan Cave Leighton Paisner (bclplaw.com)
[56] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68
[57] https://iga.in.gov/legislative/2023/bills/senate/5#document-b95da0f8
[58] https://mgaleg.maryland.gov/2023RS/bills/hb/hb1202F.pdf
[59] https://laws.leg.mt.gov/legprd/LAW0210W$BSIV.ActionQuery?P_BILL_NO1=384&P_BLTP_BILL_TYP_CD=SB&Z_ACTION=Find&P_SESS=20231
[60] https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9
[61] https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB0073
[62] https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB0073
[63] https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB1844
[64] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB331&search_keywords=artificial+intelligence
[65] C G A - Connecticut General Assembly
[66] https://lims.dccouncil.gov/Legislation/B25-0114

[67] https://legislation.politicopro.com/bill/ME_23R_HP_1270?activeTabs=bill-text
[68] https://malegislature.gov/Bills/193/SD745
[69] https://malegislature.gov/Bills/193/HD2281
[70] https://malegislature.gov/Bills/193/SD1971
[71] https://malegislature.gov/Bills/193/HD3263
[72] https://malegislature.gov/Bills/193/H1873
[73] https://www.gencourt.state.nh.us/bill_status/billinfo.aspx?id=865&inflect=1
[74] https://www.njleg.state.nj.us/bill-search/2022/S1402
[75] https://olis.oregonlegislature.gov/liz/2023R1/Measures/Overview/SB619
[76] https://www.legis.state.pa.us/cfdocs/billInfo/billInfo.cfm?sYear=2023&sInd=0&body=S&type=R&bn=49
[77] https://www.legis.state.pa.us/CFDOCS/billInfo/billInfo.cfm?syear=2023&sInd=0&body=H&type=B&bn=708
[78] https://legiscan.com/RI/text/H6236/2023
[79] https://www.scstatehouse.gov/sess125_2023-2024/bills/404.htm
[80] https://capitol.texas.gov/tlodocs/88R/billtext/html/HB02060I.htm
[81] https://legislature.vermont.gov/bill/status/2024/H.114
[82] Digital Transformation of AML/CFT (fatf-gafi.org)
[83] https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf
[84] https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf
[85] https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf
[86] Sanctions Compliance Guidance for Instant Payment Systems (treasury.gov)
[87] Sanctions Compliance Guidance for Instant Payment Systems (treasury.gov)
[88] download (treasury.gov)
[89] eCFR :: Appendix A to Part 501, Title 31 -- Economic Sanctions Enforcement Guidelines.
[90] https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/
[91] FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI | The White House
[92] SUGGESTED ACTIONS TO SUPPORT THE USE OF NEW TECHNOLOGIES FOR AML/CFT
[93] Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov)
[94] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
[95] PUBL283.PS (congress.gov)
[96] SR 11-7 attachment: Supervisory Guidance on Model Risk Management (federalreserve.gov)
[97] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
[98] https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
[99] SUGGESTED ACTIONS TO SUPPORT THE USE OF NEW TECHNOLOGIES FOR AML/CFT
[100] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001
[101] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
[102] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB331&search_keywords=artificial+intelligence
[103] https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF
[104] C G A - Connecticut General Assembly
[105] https://leg.colorado.gov/bills/sb21-169
[106] https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf
[107] US state-by-state AI legislation snapshot | Bryan Cave Leighton Paisner (bclplaw.com)
[108] https://lims.dccouncil.gov/Legislation/B25-0114
[109] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68
[110] https://iga.in.gov/legislative/2023/bills/senate/5#document-b95da0f8
[111] https://legislation.politicopro.com/bill/ME_23R_HP_1270?activeTabs=bill-text
[112] https://mgaleg.maryland.gov/2023RS/bills/hb/hb1202F.pdf
[113] https://malegislature.gov/Bills/193/SD745
[114] https://malegislature.gov/Bills/193/HD2281
[115] https://malegislature.gov/Bills/193/SD1971
[116] https://malegislature.gov/Bills/193/HD3263
[117] https://malegislature.gov/Bills/193/H1873
[118] https://laws.leg.mt.gov/legprd/LAW0210W$BSIV.ActionQuery?P_BILL_NO1=384&P_BLTP_BILL_TYP_CD=SB&Z_ACTION=Find&P_SESS=20231
[119] https://www.gencourt.state.nh.us/bill_status/billinfo.aspx?id=865&inflect=1
[120] https://www.njleg.state.nj.us/bill-search/2022/S1402
[121] https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9
[122] https://olis.oregonlegislature.gov/liz/2023R1/Measures/Overview/SB619
[123] https://www.legis.state.pa.us/cfdocs/billInfo/billInfo.cfm?sYear=2023&sInd=0&body=S&type=R&bn=49
[124] https://www.legis.state.pa.us/CFDOCS/billInfo/billInfo.cfm?syear=2023&sInd=0&body=H&type=B&bn=708
[125] https://legiscan.com/RI/text/H6236/2023
[126] https://www.scstatehouse.gov/sess125_2023-2024/bills/404.html
[127] https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB0073
[128] https://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB0073
[129] https://capitol.texas.gov/BillLookup/History.aspx?LegSess=88R&Bill=HB1844
[130] https://capitol.texas.gov/tlodocs/88R/billtext/html/HB02060I.htm
[131] https://legislature.vermont.gov/bill/status/2024/H.114

COMPLY ADVANTAGE®

RESISTANT.AI

Disclaimer: This is for general information only. The information presented does not constitute legal advice. ComplyAdvantage accepts no responsibility for any information contained herein and disclaims and excludes any liability in respect of the contents or for action taken based on this information.