



Stirring Up the Artificial Intelligence Pot

January 31st, 2024 | and [Trisha J. Cacciola](#)

On October 30, 2023, President Joe Biden signed an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. This Executive Order sweeps across many categories of products and programs, with its purpose generally being to protect consumers and employees from privacy, discrimination, and other potential harms presented by the widespread and ever-increasing use of artificial intelligence.

What is artificial intelligence? The term “artificial intelligence” or “AI” is defined in the National Artificial Intelligence Initiative 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 perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.”

In more basic terms, AI is the proverbial “black box” that takes data from a variety of sources as inputs and uses complex algorithms to produce an accurate prediction or result on an automated and expedited basis.

The Executive Order names the U.S. Department of Commerce’s National Institute of Standards and Technology as the agency charged with the development of guidelines and best practices for “developing and deploying safe, secure, and trustworthy AI systems.” The Secretary of Homeland Security will be charged with establishing an AI Safety and Security Board and applying standards to critical infrastructure sectors to ensure that best practices are followed before companies implement AI processes. In addition, the Department of Labor must establish guidance for the use of AI to track worker behavior. Also, the Department of Health and Human Services, along with the Department of Agriculture, will be required to use its authority to regulate how AI impacts government benefit programs. Further, executive agencies, such as the Department of Justice, are charged with preventing the use of AI to harm individuals through, for example, discrimination or infringement of privacy rights.

What is the result of these and other mandates under the Executive Order? Well, one thing is certain. This level of guidance and oversight will absolutely translate into companies being required to do much more testing and disclosure than in the past.

For purposes of this article, we will focus on the Executive Order’s call to action to protect consumers from algorithmic discrimination. This mandate dovetails nicely with earlier guidance on AI from the Federal Trade Commission and recent guidance from the Consumer Financial Protection Bureau. Let’s start with the FTC.

Back in 2020, the FTC issued business guidance on the use of AI and algorithms that stated what should be obvious to creditors under the Equal Credit Opportunity Act and Regulation B:

Some might say that it's too difficult to explain the multitude of factors that might affect algorithmic decision-making. But, in the credit-granting world, companies are required to disclose to the consumer the principal reasons why they were denied credit, and it's not good enough simply to say, "your score was too low" or "you don't meet our criteria." You need to be specific (e.g., "you've been delinquent on your credit obligations" or "you have an insufficient number of credit references"). This means that you must know *what* data is used in your model and *how* that data is used to arrive at a decision. And you must be able to explain that to the consumer. If you are using AI to make decisions about consumers in any context, consider how you would explain your decision to your customer if asked.

Then, in May 2022, the CFPB published its Consumer Financial Protection Circular 2022-03 guidance focused on compliance with the ECOA requirement to provide consumers with a statement of the principal reasons that resulted in adverse action, no matter how complicated the credit system may be. The CFPB emphasized that using AI does not eliminate that responsibility, stating: "Whether a creditor is using a sophisticated machine learning algorithm or more conventional methods to evaluate an application, the legal requirement is the same: Creditors must be able to provide applicants against whom adverse action is taken with an accurate statement of reasons."

This pronouncement is perfectly consistent with the ECOA and Reg. B; thus, it did not introduce any new spin on the law. Specific reasons for decline are required under the ECOA and have been since its inception. Despite this clarity, the CFPB felt compelled to recently reiterate this guidance. On September 19, 2023, the CFPB issued Consumer Financial Protection Circular 2023-03 that expressly addresses the legal compliance requirements imposed by the ECOA and Reg. B. The circular emphasizes that creditors need to comply with adverse action notice requirements even when making decisions using complex algorithms. In response to a question from a creditor about being in compliance with its adverse action responsibility simply by using the reasons that appear in the sample adverse action forms in Reg. B's appendix, the CFPB indicated that "creditors may not rely on the checklist of reasons provided in the sample forms (currently codified in Regulation B) to satisfy their obligations under ECOA if those reasons do not specifically and accurately indicate the principal reason(s) for the adverse action. Nor, as a general matter, may creditors rely on overly broad or vague reasons to the extent that they obscure the specific and accurate reasons relied upon."

Thus, we see again and again the notion that complicated technology is not accepted as a defense to a failure to comply with the requirement to give a specific and accurate statement of reasons for an adverse action. Checking a box with a reason that is wrong or inaccurate, even if the reason selected is one of those printed in an ECOA/Reg. B model form, will not suffice to satisfy the notification requirements under the ECOA and Reg. B. A creditor must be clear about why the customer was actually declined under the model or algorithm that caused the denial.

So, where does that leave us? Well, it is abundantly clear that transparency is critical. Companies cannot wrap themselves in a shroud of mystery, using AI complexity as a shield against compliance with the law, whether under the ECOA, Reg. B, privacy requirements, in the workplace, or in any other manner with consumers and workers. The Executive Order appears to provide regulatory agencies, including the DOJ, with more support for enforcing these concepts.

Specifically in the credit-decisioning space, creditors using AI in the credit application process (which is the vast majority in this automated, model-driven environment) need to be cognizant of the fact that they must understand the reasons for the decline that results from the use of their AI-driven credit-decisioning models and algorithms. Therefore, the application process must incorporate a way to provide the applicant with written reasons that help the applicant understand with a degree of clarity what the applicant needs to “fix” before applying to that creditor again. So, a creditor should not rely on its tried and true “judgmental” reasons if those are no longer accurate or employ the use of overly broad statements to cover a multitude of real reasons that the creditor perhaps cannot easily communicate without some thought and attention to the phrasing.

A word to the wise: it would be worthwhile to tee up your adverse action process for a compliance review in the near future, especially if it has not been examined in a while. 