WILSON SONSINI | FINTECH AND FINANCIAL SERVICES

AI in PAYMENTS PLAYBOOK

Payments
Playbook Series

In the highly competitive payments space, where **safety and efficiency tools** are table stakes, financial institutions are increasingly employing artificial intelligence (AI) solutions.

Key areas for AI solutions in payments

While financial institutions have long used AI solutions, their deployment is accelerating and evolving in response to **technology shifts** in payments operations and **data-rich transactions**, as well as growing **cybersecurity threats and fraud risks**. Key areas of expanding AI use include:

Fighting fraud

Enhancing security procedures and improving fraud monitoring, detection, and prevention in real time

As part of a solution for combating fraud, Generative AI (GenAI) could be used to create synthetic data based on real data to train fraud models, analyze data in fraud investigations, and create training programs. GenAI is a category of AI models capable of generating content in response to a user's input prompts and based on training data embodied in the AI model.

RegTech

Optimizing monitoring for money laundering and sanctions screening, and automating transaction reporting (e.g., filing suspicious activity reports)

Risk assessment

Leveraging payments activity data for predictive analysis, such as to expedite funds availability to customers

Payments industry trends

As more payment platforms and banks start to adopt a particular type of AI solution, peer financial institutions may find that it is time for them to consider it as well.

> As AI solutions mature, financial institutions will be increasingly mindful of what their peers are doing, so that they do not find themselves falling behind when the industry starts to shift.

FINTECH AND
FINANCIAL SERVICES

An innovator in the payments space without an AI strategy is now the exception, not the norm.

Many financial institutions are looking to third-party service providers for AI solutions, rather than developing and training models internally. At the same time, managing risks in line with **financial regulatory requirements and supervisory guidance** will be key, as well as addressing **privacy concerns**.

This **Playbook for AI in Payments** sets out a blueprint for service providers to strategically optimize the AI solutions they offer to financial institutions and help build a safer, more efficient payments ecosystem.

Financial institutions may also find this playbook helpful as they transition beyond exploring AI solutions to deployment.

Defining your offering	Addressing explainability and model risk	Mapping data dependencies	Maintaining and risk-managing it

DEFINING YOUR OFFERING

It is critical to ensure your financial institution customers **understand the nature and scope of your AI solution**, how it will be used, and its limitations. This includes:

- Strategically framing the use case for your AI solution to position it as the right tool for the job, given your customer base's risk tolerance and strategic goals
  - Distinguish between AI solutions that are more complex, automatically trigger a financial institution's decisions, or are applied in critical use cases, on the one hand, from those that are easier to validate, narrower in scope (e.g., output for a user to consider), or used to automate repetitive tasks, on the other
  - Your framing of your AI solution's use case will impact the rigor and sophistication of how a financial institution will apply its risk management practices. If their use of your AI solution is less prevalent and has less impact on their financial condition, operations, or compliance, then a less sophisticated approach to risk management may be appropriate
- Addressing how your AI solution fits in your customer's broader operations and existing controls (e.g., the customer's layered security control framework and practices for access and authentication for AI solutions that fight fraud)
- Clearly specifying in your customer agreements the IP ownership and use rights for each component of your AI solution (i.e., the AI tool itself, training datasets, instruction materials, data inputs and outputs, and future iterations of the AI solution)—and, if you are using the customer's form agreements, being vigilant that the IP ownership provisions are aligned with your understanding of the arrangement

ADDRESSING **EXPLAINABILITY AND MODEL RISK**

Financial institution customers will not only evaluate AI solutions from the perspective of their technical capabilities but also analyze the solution from a **financial regulatory and supervisory perspective**, particularly with respect to explainability and transparency. Anticipate concerns by:

- Being transparent as to the extent of your ability to explain your AI solution's overall functioning, the framework for how it arrives at an individual outcome in a given situation, and compensating controls to ensure your solution is robust and will not become erratic (e.g., testing, performance monitoring, algorithmic auditing, outcome analysis, benchmarking, and frequent retraining)
- Building in features that allow users to see the reasoning behind the AI solution's actions or outputs (e.g., output annotation and confidence scoring)

Bear in mind that how you define your AI solution's use case will impact the level and type of explainability expected from financial institutions (e.g., opacity will be more acceptable for AI solutions that assist an individual user in making decisions on internal risk management than those that automatically trigger a financial institution's decisions to decline to offer a consumer credit). Not all features and controls described above may be necessary.

MAPPING THE **DATA DEPENDENCIES**

Establishing clear expectations around what data from your financial institution customer is used and how it is used is essential. This includes:

- Ensuring your customer agreements clearly specify the data that will be provided by customers to use the AI solution (particularly if any personal information will be used) and how you will use that data (whether it is to improve your existing AI solution, versus building a new product or generating insights or other outputs)
- Accurately disclosing your data collection, use, and disclosure practices in a privacy policy and complying with applicable privacy laws
- Ensuring good data hygiene for the data used to train the models (e.g., establishing robust controls on the provenance, accuracy, and reliability of the training dataset, as well as legal permission for its use)

Note that larger financial institutions tend to prefer deploying AI solutions in their own environment and limiting the sharing of data, rather than relying on a fully managed and hosted service. In considering your longer-term business strategy, a more flexible approach with multiple commercial models to accommodate different types of deployment of your AI solution may allow you to more dynamically grow and quickly expand your customer base.

MAINTAINING AND **RISK-MANAGING IT**

As reliance by financial institution customers on your AI solution grows, mitigants and controls for vulnerabilities become increasingly critical. Prepare for vetting and oversight from financial institutions based on their **vendor risk management** processes, with emphasis on **AI-specific factors**. This includes:

- Anticipating inquiries from financial institutions commensurate with the level of risk and criticality of their use of your AI solution, including with respect to:
  - the integration of your AI solution into their operations and its ability to function as expected
  - your compliance with applicable laws and regulations and adherence to the financial institution customer's relevant policies
  - your reliance on other vendors for data or models in connection with your AI solution
- Having in place risk assessment processes for biases and unintended drift in your AI solution (e.g., conducting periodic audits and vetting training datasets)
- Monitoring regulatory change (e.g., extraterritorial reach of new laws such as the EU AI Act) and evaluating your AI solution in the context of greater scrutiny by the federal financial regulatory agencies over the risks of AI

HOW WE CAN **HELP**

FINTECH AND
FINANCIAL SERVICES

Wilson Sonsini's Fintech and Financial Services attorneys are market leaders in creatively and collaboratively partnering with clients at the forefront of payments innovation.

Leveraging our **unparalleled legacy of representing AI companies** of all stages, we have deep experience in emerging payments technologies, with a view to:

- minimizing regulatory risks
- incorporating industry best practices
- strategically protecting our clients' interests

Contact

Jess Cheng
Partner
New York
jcheng@wsgr.com

WILSON
SONSINI