affirmative™

TECHNOLOGIES

The Powers and Pitfalls of AI: How to Leverage Analytics Responsibly to Manage ACH Risk

Payments Risk Management

Measure

Monitor

Manage

Meet the Speaker

With over twenty-four years experience in payments risk management, Aaron has been at the forefront on innovation in the field.

Aaron is currently the President and CEO of Affirmative Technologies. In this role, Aaron leads efforts to leverage payment data to help clients make smarter risk decisions.

Before joining Affirmative, he spent eight years working with ValidSystems in partnership with Fiserv, utilizing consortium data to accelerate funds availability on mobile deposits for both consumers and small businesses.

Prior to that, Aaron spent twelve years at FIS in risk operations and managing product lines under two of the nation's largest specialty consumer reporting agencies.

A recognized innovator in the field, Aaron has two inventor patents leveraging consortium data to model risk behavior in Payments to accelerate funds availability.

Who is Affirmative Technologies?

- Privately held company based in the Tampa, FL area. 26-year history focused exclusively on electronic transaction processing and risk management.
- Primarily operate as a Third-Party Service Provider (TPSP) supporting a wide variety of organizations from Nacha Top 50 originators to community banks, credit unions, payments companies and FinTech's.
  - Support programs with a combined 750,000+ originators
  - Support over 600 million ACH transactions annually
- Subject Matter Expertise. Employees average over a decade+ in risk management across our leadership team.
- Forefront of industry risk management initiatives consistently nominated to serve on industry risk and advisory committees and the recipient of multiple industry awards.

affirmative™
TECHNOLOGIES

How may of you have been solicited by a vendor who says something like this?

“Leverage the power of AI to make your life _____?”

Agenda

affirmative™ TECHNOLOGIES

- Test our Knowledge– Artificial Intelligence
- Near Term Industry Drivers shaping Risk Management in Payments
- How Models are Developed and Regulatory Considerations of AI
- Practical Examples on how to Leverage the Power of AI in your Risk Program
- Test our Knowledge– Artificial Intelligence
- Connect with Us

Test our Knowledge – AI

Primer on Artificial Intelligence (AI)

Instructions

- Five multiple choice questions to test your knowledge
- No cheating……..put your phones down
- Pay attention and you may just go back to your organization more informed
- We have Prizes!

Test our Knowledge– AI

- **Question 1.** How many primary forms of Artificial Intelligence are there?

A) Less than 3

B) Between 3-5

C) Between 6-9

D) More than 10

affirmative™ TECHNOLOGIES

Test our Knowledge– AI

- **Question 1.** How many primary forms of Artificial Intelligence are there?

A) Less than 3

B) Between 3-5

C) Between 6-9

D) More than 10

affirmative™ TECHNOLOGIES

Common Forms of Artificial Intelligence

Primary Form	Definition	Examples
Narrow (AI)	AI that is designed and trained for a specific task	Voice Assistants, Netflix Recommendations, ChatBots
Machine Learning (ML)	AI that involves training algorithms to learn from and make decisions or predictions based on data.	Supervised and Unsupervised
Deep Learning	A subset of ML that uses neural networks with many layers (deep neural networks) to model complex patterns in large amounts of data.	FICO Falcon Credit Card Fraud
Natural Language Processing (NLP)	AI focused on the interaction between computers and humans using natural language.	Google Translate, Conversational AI
Generative AI	AI focused on generating new content such as text, images, music, or code.	Text Generators: GPT (like ChatGPT). Image Generators: DALL-E, Stable Diffusion.

Test our Knowledge– AI

- **Question 2.** When were the earliest forms of Artificial Intelligence (AI) developed?

A) 1940s

B) 1950s

C) 1970s

D) 1990s

affirmative™ TECHNOLOGIES

Test our Knowledge– AI

- **Question 2.** When were the earliest forms of Artificial Intelligence (AI) developed?

A) 1940s

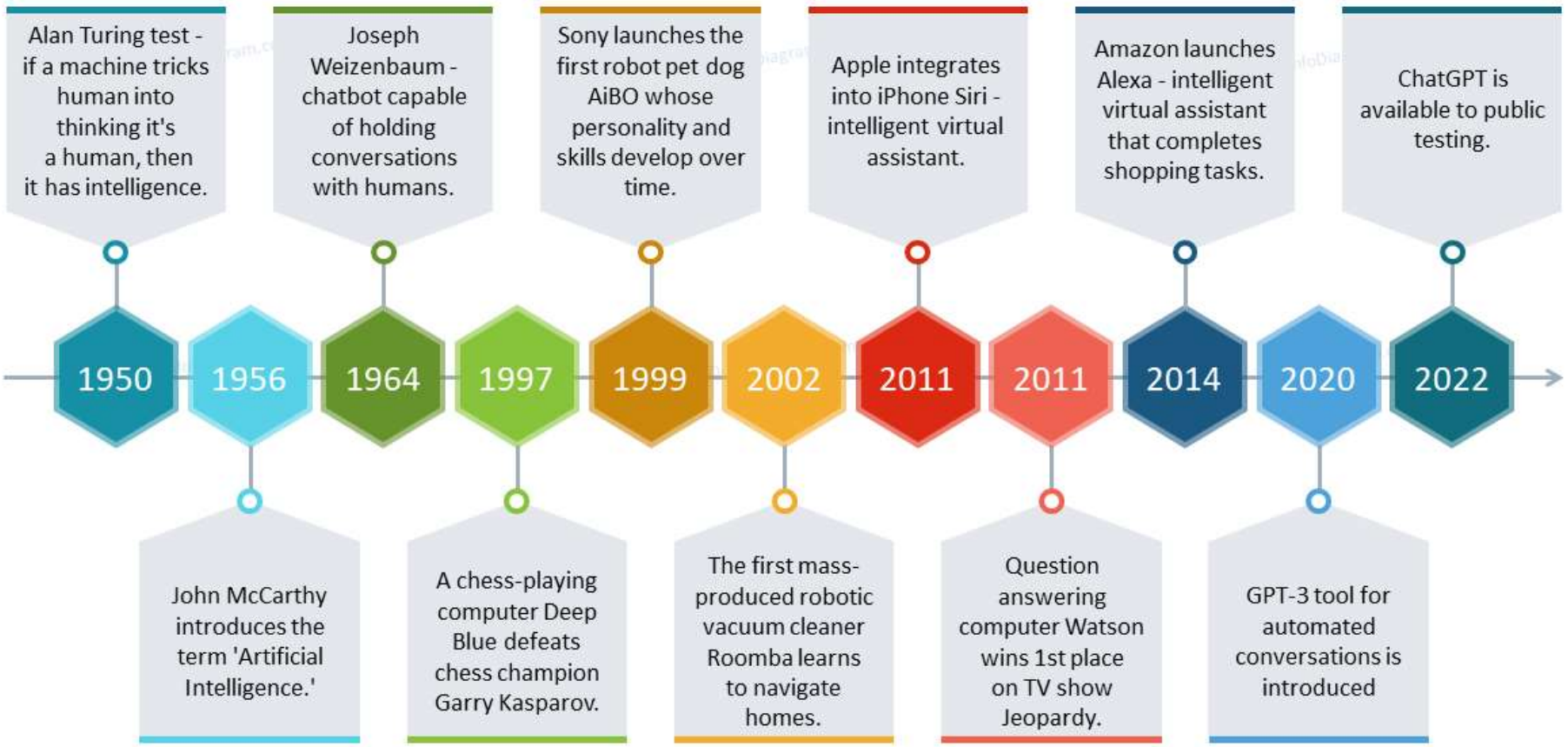
B) 1950s

C) 1970s

D) 1990s

affirmative™ TECHNOLOGIES

Artificial Intelligence Development History Timeline



Source: InfoDiagam.com

Test our Knowledge– AI

- **Question 3.** Which of the following statements best describes the relationship between Artificial Intelligence (AI) and Machine Learning (ML)?

A) Machine Learning is a broader concept that includes all aspects of Artificial Intelligence.

B) Artificial Intelligence is a subset of Machine Learning, which focuses on creating intelligent systems.

C) Machine Learning is a subset of Artificial Intelligence, which involves systems that can learn from data.

D) Artificial Intelligence and Machine Learning are two separate fields with no overlap.

affirmative™
TECHNOLOGIES

Test our Knowledge– AI

- **Question 3.** Which of the following statements best describes the relationship between Artificial Intelligence (AI) and Machine Learning (ML)?

A) Machine Learning is a broader concept that includes all aspects of Artificial Intelligence.

B) Artificial Intelligence is a subset of Machine Learning, which focuses on creating intelligent systems.

C) Machine Learning is a subset of Artificial Intelligence, which involves systems that can learn from data.

D) Artificial Intelligence and Machine Learning are two separate fields with no overlap.

affirmative™
TECHNOLOGIES

Test our Knowledge– AI

- **Question 4.** What form of AI is Chat GPT?

A)Narrow AI

B) Machine Learning (ML)

C) Deep Learning

D) Natural Language Processing (NLP)

E) Generative AI

affirmative™
TECHNOLOGIES

Test our Knowledge– AI

- **Question 4.** What form of AI is Chat GPT?

A)Narrow AI

B) Machine Learning (ML)

C) Deep Learning

D) Natural Language Processing (NLP)

E) Generative AI

affirmative™ TECHNOLOGIES

Test our Knowledge– AI

- **Question 5.** What form of AI is FICO's Falcon credit card transaction monitoring system?

A) Narrow AI

B) Machine Learning (ML)

C) Deep Learning

D) Natural Language Processing (NLP)

E) Generative AI

affirmative™ TECHNOLOGIES

Test our Knowledge– AI

- **Question 5.** What form of AI is FICO's Falcon credit card transaction monitoring system?

A) Narrow AI

B) Machine Learning (ML)

C) Deep Learning

D) Natural Language Processing (NLP)

E) Generative AI

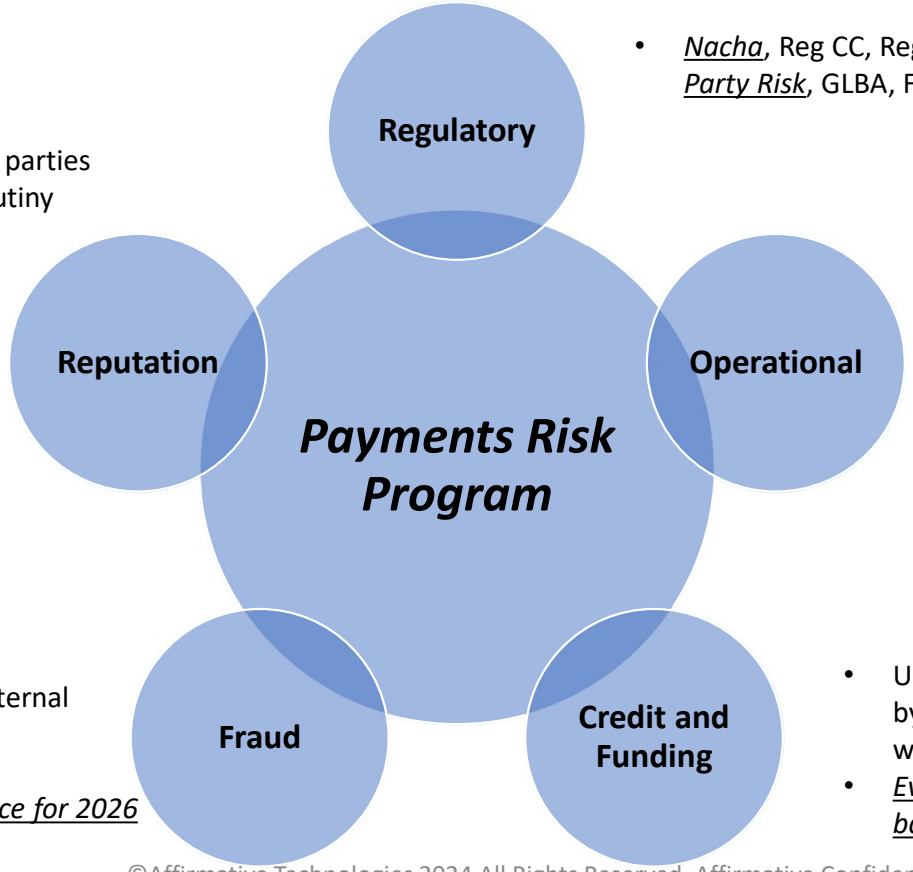
affirmative™ TECHNOLOGIES

Did we learn something?

Risk Programs. What should we be paying attention to?

Near Term Industry Drivers shaping Risk Management in Payments

Dimensions of Payments Risk Management



- *Nacha*, Reg CC, Reg E, OCC, Eccho, *Third Party Risk*, GLBA, FCRA, *Data Privacy*……

- Are you doing business with third parties that could cause unnecessary scrutiny and/or reputational harm to your organization?

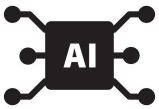
- People vs. Resilient Internal Processes
- *Processing Business Resiliency for all Third Parties Involved*

- Both Friendly/Victimization and External Threats
- Proliferation of AI use by criminals
- *Nacha Rule Changes and Compliance for 2026*

- Underwriting, setting and enforcement of limits by payment type at various frequencies (daily, weekly, monthly)
- *Evaluating Funds Availability against collected balance across **ALL** payment types*

Near Term Industry Drivers of Risk Management in Payments

Evolution and Proliferation of AI



- Be conscious of staying within the guardrails of existing regulatory and legal guidance. To leverage typically means you are training confidential data sets using a cloud-based "Black Box"
- Don't forget the Bad Guys will use it too. Keep an eye out for more sophisticated fraud attacks.

All Participants. How do you protect consumer privacy and the confidential nature of your business, GLBA and FCRA Dynamics, Disparate Impact and other very well defined legal and regulatory considerations?

Financial Institutions. OCC SR-11-7. Model Risk Governance. Expect this to adopted beyond OCC regulated banks.

Continued Enforcement of Interagency Third-Party Risk

- Financial intuitions MUST perform closer scrutiny on ALL Third Parties they do business with.
  - This includes more than just Processing Risk. Credit/Liquidity, Reputational, Information Security
- Expect more stringent audits with upcoming Audit Cycles

affirmative™ TECHNOLOGIES

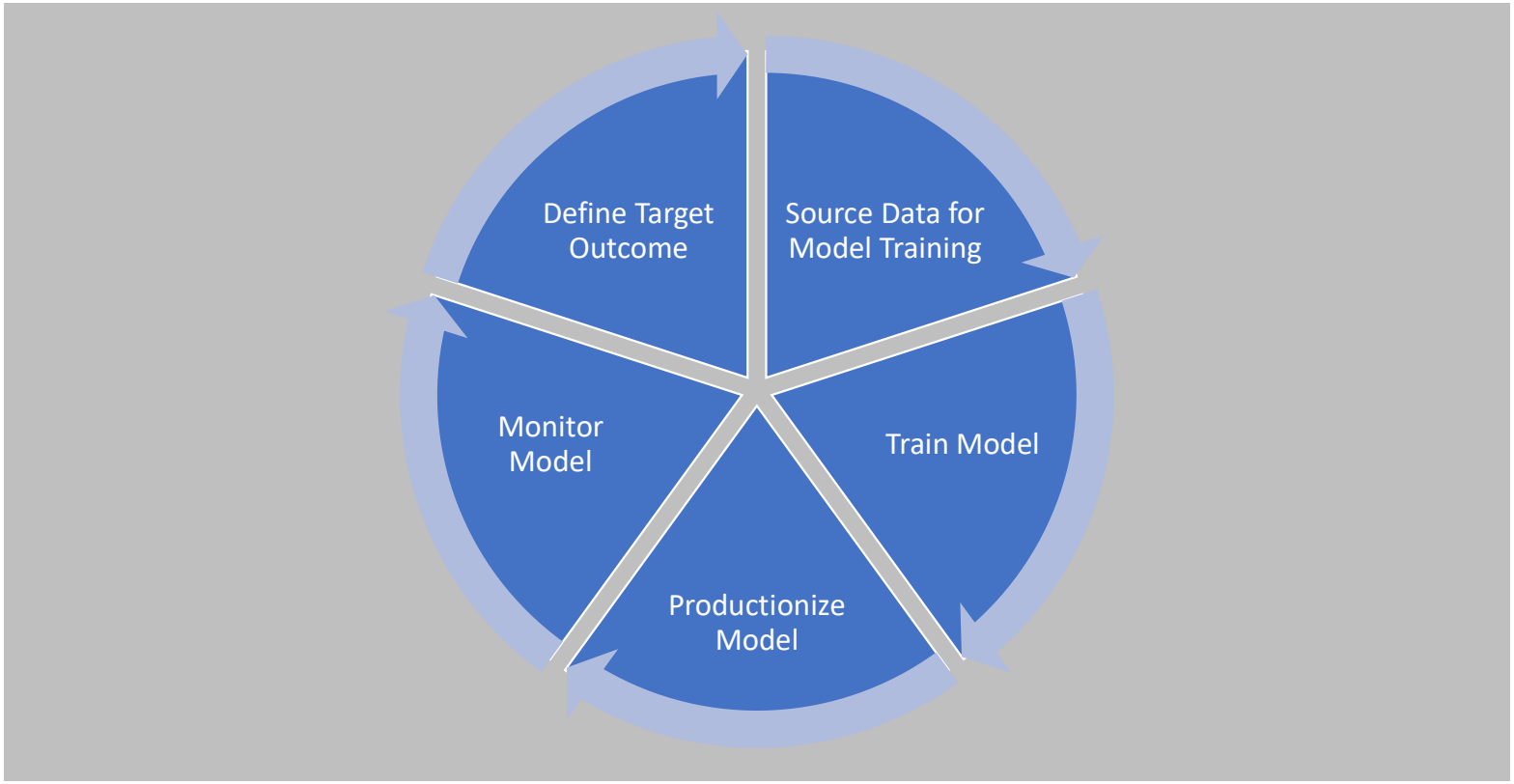
Nacha Mandated Fraud Prevention for ALL

- Rule Change effective 2026 to further protect the Safety and Soundness of the ACH Network and applies to ALL network participants

Financial Institutions. Not just getting yourself compliant but how are you going to help support your customer's compliance? Are you going to put the obligation on them? What if they don't know how to monitor?

Other Participants. How are you going to demonstrate compliance to your network sponsor institutions? Where can you find help?

Typical AI Risk Model Lifecycle



affirmative™ TECHNOLOGIES

Common Challenges in Training an AI Model

eWEEK

Whether hosted in your data center, outsourced to a vendor or cloud-based, most AI solutions on the market are a "black box"– you don't have full control.

Existing regulations already exist regarding data privacy, consumer reporting and model governance you must adhere to when leveraging Artificial Intelligence.

Image Credit: www.eweek.com

Regulatory Considerations– GLBA

What is GLBA? The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, is a U.S. law that governs the collection, use, and protection of consumers' personal financial information by financial institutions. The GLBA has several key provisions, including the Financial Privacy Rule, the Safeguards Rule, and the Pretexting Provisions. *Before you start training AI models on your data be mindful of these guardrails.*

Key Considerations:
Seven Key Considerations including: Data Privacy and Consumer Consent, Data Security and Protection (Safeguards Rule), Third-Party Service Provider Management, Data Minimization and Purpose Limitation, Transparency in Automated Decision-Making, Consumer Notification in Case of Data Breaches, and Pretexting Protections

Best Practices:

- *Data Governance:* Establish strong data governance frameworks that ensure AI systems use data in accordance with GLBA requirements, including appropriate data access controls, monitoring, and auditing.
- *Transparency and Explainability:* Use AI models that are interpretable and ensure that consumers are informed about how their data is being used.
- *Regular Security Audits:* Conduct regular security audits and risk assessments of AI systems to ensure they are secure and comply with GLBA data protection requirements.
- *Third-Party Oversight:* Develop robust third-party management protocols to ensure that vendors and service providers comply with GLBA standards when handling consumer data.
- *Bias and Fairness Checks:* Regularly audit AI models for bias and ensure they do not introduce or perpetuate discriminatory practices.

Regulatory Considerations– GLBA

Requirement	Implication	AI Challenge
Data Privacy and Consumer Consent	The GLBA requires financial institutions to disclose their privacy policies to consumers, explaining what information they collect, how they use it, and with whom they share it. Consumers must also be given the opportunity to opt out of certain information sharing.	AI systems, particularly those involving machine learning, often require large datasets, which may include sensitive financial information. This creates challenges around ensuring that data collection, usage, and sharing are transparent and that consumers provide informed consent.
Data Security and Protection (Safeguards Rule)	The GLBA's Safeguards Rule mandates that financial institutions implement security measures to protect the confidentiality and integrity of consumer information.	AI models often require large volumes of data to train and make predictions, which may increase the risk of data breaches or unauthorized access. Additionally, AI systems can be vulnerable to adversarial attacks, data poisoning, and other security threats that compromise consumer data.
Third-Party Service Provider Management	The GLBA requires financial institutions to ensure that third-party service providers (such as vendors or data analytics firms) implement adequate security measures to protect consumer information.	Many financial institutions outsource AI development or use third-party AI tools and platforms. These external providers must also comply with GLBA requirements, which means institutions need to establish robust contractual obligations and monitoring to ensure compliance.
Data Minimization and Purpose Limitation	The GLBA encourages minimizing the collection and retention of personal data and using it only for specific, disclosed purposes.	AI systems often require extensive data for training, which can lead to the collection of more data than is necessary for a specific purpose. Financial institutions must ensure that AI data practices align with the principle of data minimization to avoid non-compliance.
Transparency in Automated Decision-Making	The GLBA does not explicitly address AI or automated decision-making, but it implies a need for transparency in how consumer data is used, especially when it affects consumers' rights or financial opportunities.	AI models, particularly those that are complex or opaque ("black boxes"), can make it difficult to explain to consumers how their data is being used or why specific decisions are made. Financial institutions must ensure that AI-driven decisions are understandable and comply with GLBA's privacy policy disclosure requirements.

Regulatory Considerations– GLBA

Requirement	Implication	AI Challenge
Consumer Notification in Case of Data Breaches	While the GLBA does not have a specific provision for breach notification, the Safeguards Rule implies a need for protecting data and, by extension, requires responses to data breaches.	If an AI system is breached or manipulated (e.g., through data poisoning attacks), it could expose sensitive consumer data or make erroneous decisions. Financial institutions must have protocols in place to detect breaches promptly and respond effectively.
Pretexting Protections	The GLBA prohibits "pretexting" or obtaining personal financial information through false pretenses.	AI systems must be implemented correctly to avoid unintended breaches or misuse of consumer data.

Regulatory Considerations– FCRA (DF)

What is the Fair Credit Reporting Act? The Fair Credit Reporting Act (FCRA) is a U.S. federal law enacted in 1970 to ensure accuracy, fairness, and privacy in the collection and use of consumer credit information. *Data furnishers, such as banks, lenders, credit card companies, and other entities that provide consumer credit information to consumer reporting agencies (CRAs), have specific obligations under the Fair Credit Reporting Act (FCRA).* Supplying consumer information to an AI "black box" raises several implications arise regarding compliance with the FCRA Data Furnisher obligations.

Key Considerations for Data Furnishers:

- Data Accuracy
- Timely Correction of Inaccurate Information
- Fair Treatment of Consumers
- Compliance with Dispute Resolution Requirements
- Data Governance and Security

Best Practices for Data Furnishers:

- *Monitor Data Quality: Establish rigorous data quality control measures to ensure accuracy and completeness.*
- *Regular Audits: Conduct regular audits and evaluations of AI systems to detect and mitigate biases and inaccuracies.*
- *Strengthen Data Security: Implement strong data security protocols to protect consumer information used by AI systems.*
- *Develop Dispute Resolution Procedures: Ensure that AI systems have built-in mechanisms for handling consumer disputes in line with FCRA requirements.*

Regulatory Considerations– FCRA (DF)

Requirement	Implication	AI Challenge
Accuracy of Information Provided to CRAs	The FCRA requires data furnishers to provide accurate and complete information to CRAs and to promptly correct any inaccuracies.	AI systems that analyze or generate credit data may inadvertently produce or propagate errors if they rely on inaccurate, outdated, or biased data. Additionally, AI systems may derive insights or creditworthiness scores that differ from traditional metrics, potentially introducing discrepancies
Timely Correction of Inaccurate Information	Under the FCRA, data furnishers are obligated to investigate and correct any inaccuracies in the information they provide to CRAs within a specific timeframe.	AI systems can make it harder to identify and correct errors if they lack transparency or if there is insufficient human oversight. Data furnishers must ensure that their AI systems can quickly and accurately process disputes and corrections to comply with FCRA deadlines.
Fair Treatment of Consumers	The FCRA requires data furnishers to treat consumers fairly and provide accurate information that does not discriminate or bias against any group.	AI algorithms can inadvertently introduce or amplify biases present in the training data. For instance, if an AI model used by a data furnisher reflects historical biases or is trained on biased data, it may unfairly impact certain consumer groups by reporting biased or discriminatory information.
Compliance with Dispute Resolution Requirements	The FCRA requires data furnishers to have robust procedures to handle disputes filed by consumers about inaccuracies in their credit information.	AI systems must be equipped to handle disputes efficiently and transparently, ensuring that errors in data processing or interpretation are quickly resolved. If AI systems are not properly managed, they could inadvertently ignore or mishandle disputes.
Data Governance and Security	The FCRA mandates that data furnishers ensure the privacy and security of consumer information shared with CRAs	AI systems often require access to large volumes of sensitive consumer data to function effectively. Securing this data against unauthorized access, breaches, or misuse is crucial for compliance with the FCRA. Additionally, the use of AI in data processing may introduce new vulnerabilities, such as exposure to data breaches or cyber-attacks.

Regulatory Considerations– OCC SR 11-7

- **What is the OCC SR 11-7?** OCC SR 11-7, also known as the Supervisory Guidance on Model Risk Management issued by the Office of the Comptroller of the Currency (OCC) and the Federal Reserve in 2011, provides guidelines for managing the risks associated with models used by financial institutions. This guidance emphasizes the need for a strong model governance framework, including robust processes for model development, validation, use, and oversight. *Under SR 11-7, any tool or method that uses quantitative techniques to process inputs and produce estimates, forecasts, or decisions is considered a model*. AI and machine learning models used for risk management, credit scoring, fraud detection, or other purposes fall within this definition.
- **Key Considerations**:
- Ten total key considerations you need to be aware of including: *Model Development, Implementation, and Use, Model Validation, Model Risk Management and Governance Framework, Data Quality and Management, Ongoing Monitoring and Performance Management, Model Inventory and Documentation, Model Risk Aggregation and Reporting and Third-Party Model Risk Management*
- **Best Practices:**
- *Enhance Model Documentation*: Ensure that AI models are thoroughly documented, including their design, data sources, assumptions, and validation methods.
- *Strengthen Model Validation Processes:* Develop new validation techniques suitable for complex AI models, such as sensitivity analysis, adversarial testing, and bias detection.
- *Implement Explainability Tools:* Use tools and frameworks (like SHAP, LIME, or Explainable AI techniques) to enhance the interpretability of AI models.
- *Establish Continuous Monitoring Protocols:* Set up automated monitoring

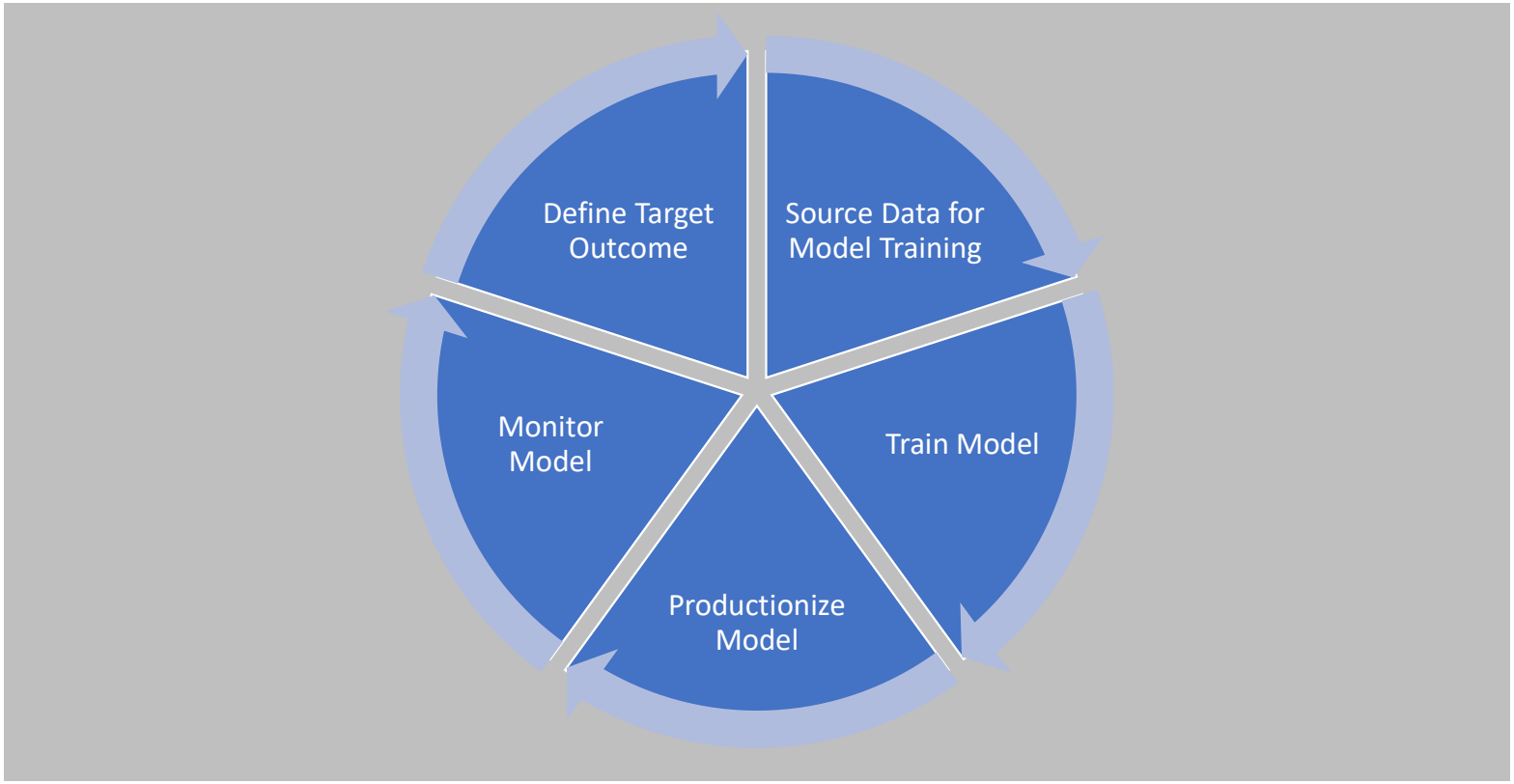
Regulatory Considerations– OCC SR 11-7

Requirement	Implication	AI Challenge
Model Definition and Classification	Under SR 11-7, any tool or method that uses quantitative techniques to process inputs and produce estimates, forecasts, or decisions is considered a model. AI and machine learning models used for risk management, credit scoring, fraud detection, or other purposes fall within this definition.	AI models, particularly those using machine learning, can be more complex and less interpretable than traditional models, making it challenging to define and classify them appropriately. Financial institutions must clearly identify which AI tools qualify as models under SR 11-7 and ensure that they are governed by appropriate policies
Model Development, Implementation, and Use	SR 11-7 requires that models be developed, implemented, and used according to a formal, well-documented process that includes data quality checks, sound development methodologies, and controls to ensure proper use.	AI models often rely on large datasets and complex algorithms that can change dynamically (e.g., self-learning models). Ensuring data quality, model performance, and appropriate use in an AI context can be more challenging than with traditional models. AI models may also require continuous monitoring and recalibration to maintain accuracy and relevance.
Model Validation	SR 11-7 emphasizes the need for independent and comprehensive validation of models before they are implemented and throughout their lifecycle. Validation includes evaluating conceptual soundness, ongoing monitoring, and outcomes analysis.	AI models, particularly those using machine learning techniques, can be difficult to validate due to their complexity, non-linear nature, and lack of transparency ("black box" models). Traditional validation techniques may not be sufficient, and new approaches may be required to evaluate AI models' conceptual soundness, accuracy, and reliability.
Model Risk Management and Governance Framework	SR 11-7 requires institutions to establish a robust governance framework for managing model risk, including clear roles and responsibilities, policies, and procedures for model development, use, and validation.	AI models introduce additional governance challenges, such as managing model complexity, ensuring explainability, and overseeing continuous model updates. Financial institutions must adapt their model governance frameworks to address these challenges, including integrating AI-specific policies and procedures.
Data Quality and Management	SR 11-7 requires that data used for model development and validation be accurate, complete, and representative of the institution's portfolio and operating environment.	AI models often rely on large and diverse datasets, which can introduce risks related to data quality, such as bias, incompleteness, or representativeness. Institutions must ensure that the data used in AI models meets quality standards and that any issues are identified and addressed promptly.

Regulatory Considerations– OCC SR 11-7

Requirement	Implication	AI Challenge
Explainability and Transparency	SR 11-7 requires that models be explainable and that their results be interpretable to users, management, and regulators.	AI models, especially those using deep learning or other complex algorithms, are often seen as "black boxes" with limited interpretability. Financial institutions must ensure that these models are sufficiently transparent to meet regulatory expectations, which may involve developing new techniques for explaining AI-driven decisions.
Ongoing Monitoring and Performance Management	SR 11-7 emphasizes ongoing monitoring of models to ensure they perform as expected over time and under different conditions.	AI models may change over time, especially if they are designed to learn from new data (adaptive models). This creates challenges in monitoring and managing model performance. Institutions must implement continuous monitoring practices to detect performance degradation, bias, or other issues.
Model Inventory and Documentation	SR 11-7 requires institutions to maintain a comprehensive inventory of all models, including documentation of their purpose, design, validation, and use.	The dynamic nature of AI models and the use of external or third-party models can make it difficult to maintain a complete and accurate model inventory. Institutions must ensure that all AI models are documented thoroughly and that their inventories are kept up to date.
Model Risk Aggregation and Reporting	SR 11-7 requires institutions to aggregate model risk across the organization and report it to senior management and the board of directors.	Aggregating risks from diverse AI models can be challenging due to differences in model types, purposes, and risk profiles. Institutions must develop methods to quantify and report AI-related risks in a way that is consistent with their overall model risk management framework.
Third-Party Model Risk Management	SR 11-7 requires institutions to manage risks associated with third-party models, including those developed or maintained by external vendors.	Financial institutions often use third-party AI tools or platforms, which adds complexity to model risk management. Institutions must ensure that these third-party models are validated, documented, and monitored in accordance with their internal policies and SR 11-7 requirements.

Typical AI Risk Model Lifecycle



Did we learn something?

Practical Examples of AI

Leveraging AI to help enhance your Payments Risk Program

AI Use Case: Identify High-Risk Originators

Leveraging AI to help enhance your Payments Risk Program

Overview

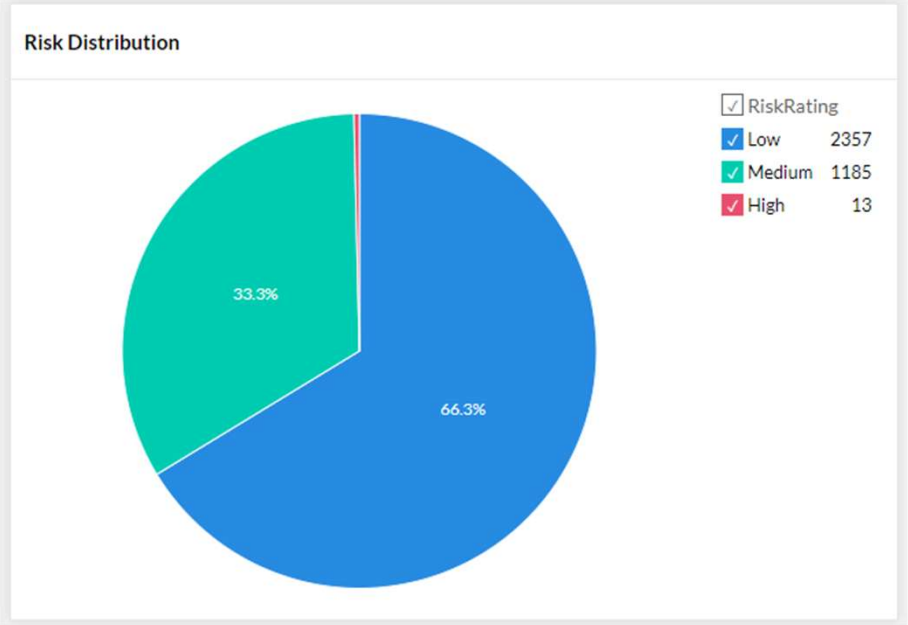
What is ‘Unauthorized (UA) Risk Rating’?

- Empirically derived and statistically sound predictive model, developed with a proprietary database of 750,000+ originators
- Scores the likelihood each originator will submit an unauthorized transaction in the next 90 days. The score is then translated into a risk grade of High, Medium, or Low.
- Identifies originator characteristics and patterns of behavior that will result in unauthorized activity

Use Cases?

- Proactively identify high-risk originators for review and risk management
- Reduce exposure through limit adjustments
- Grow banking relationships with low-risk originators
- Monitor portfolio health: reporting for management, board and regulatory compliance

Actual Customer Risk Distribution (Anonymized)



ATI Summary Attributes

Over 130 summary attributes describe originators and their transaction activity….

Originator Type

OrigName	Originator name
OrigDesc	Originator company description
Nested	Is the originator is under a third party processor
Purpose	Payroll, Transfer, Payment
OrigAge	Number of months with transactions

Origination Activity

OrigV01	Average Monthly Total (Credit + Debit) Origination Count
OrigV01a	Average Monthly Total Origination Amount
OrigV05	Average Monthly Debit Origination Count
OrigV06c	Mode Debit Origination Amount
OrigV13	Percentage of Total transaction count = PPD
OrigV18	Percentage of Total transaction amount = WEB
OrigV31	Count of days originated divided by total number of days
OrigV35	Standard Deviation of all origination transaction amounts

Return Activity

RetV00a	Average Monthly Total (Credit + Debit) Unauthorized Return Count
RetV04	Min Total Return Amount
RetV11	Percentage of Total return transaction count = Telephone
RetV22	Average Monthly Debit Return Count
RetV26	Average Monthly R01 Return Count (NSF)
RetV59	Average Monthly R11 Return Amount (cust advises not w/ terms)
RetV87	Count of days with returns divided by total number of days
RetV88	Count of return transactions in prior month (t – 1)

NOC

NOCV01	Average number of CO1's – incorrect DFI account number
NOCV02	Average number of CO2's – incorrect Routing and Transit Number
NOCV03	Average number of CO3's – incorrect RTN and Account Number
NOCV05	Average number of CO5's – incorrect payment transaction code
NOCV06	Average number of CO6's – incorrect AN & transaction code
NOCV07	Average number of CO7's – incorrect RTN, AN & transaction code

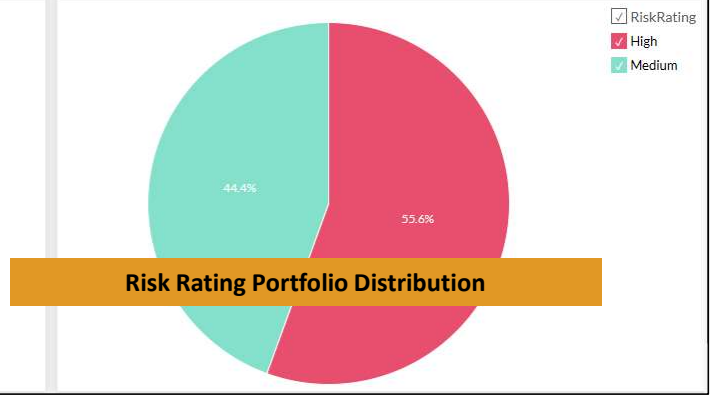
Unauthorized Return Prediction

Originators by Risk Group

	Processor	Originator	CompanyID	RiskRating	Risk Group
1	Northwest	ALIQUAM AUCTOR	26N77	High	7
2		AMET PHARETRA	WRML4GI	High	7
3		RISUS LIBERO	EYNY6W2	High	7
4		VESTIBULUM	GIFXVF	High	7
5	QuickPay	FIRST PAYMENTS	240158556	Medium	4
6		LEAP INDUSTRIES	240158562	Medium	4
7		PAYMENT TECH	240158558	Medium	4
8		TEMPOR REGALIA	240158110	Medium	4
9	TRANXACT	POSUERE INTEGER	7DE6BHZZ	High	7

List by Risk Rating and Risk Group

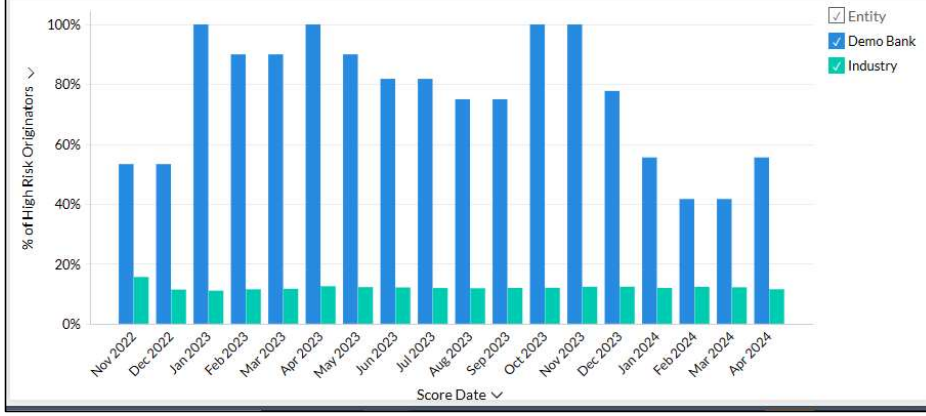
Risk Distribution



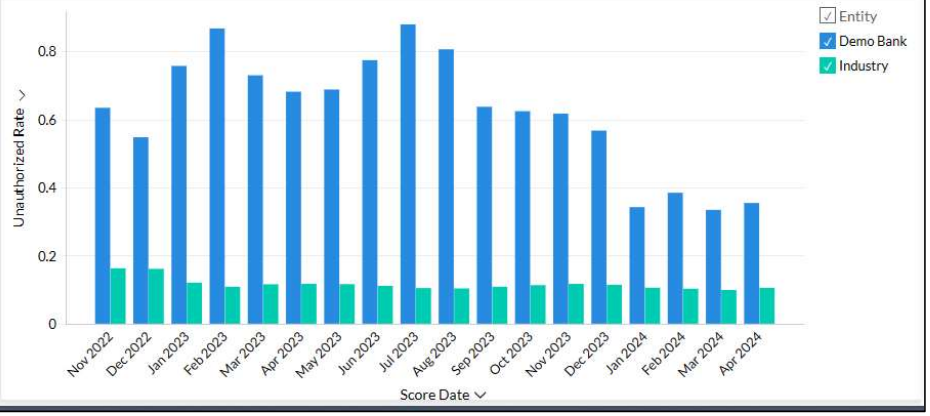
Risk Rating Portfolio Distribution

ATI Network Benchmark Comparison

High Risk Originators vs Network Avg



Unauthorized Rate vs Network Average



AI Use Case: Identifying Abnormal Originator Behavior

Leveraging AI to help enhance your Payments Risk Program

Overview

What is a 'Behavioral Alert'?

- Model that periodically reviews financial institution's originator base for activity consistent with high-risk behavior
- Identifies originator characteristics and patterns of behavior potentially indicating:
  - Nested Third Party Processors
  - Dormancy Risk

Use Cases?

- Proactively identify high-risk originators for review and risk management
- Adjust credit limit exposure amounts
- Monitor portfolio health: reporting for management, board and regulatory compliance

Identified Potential High Risk Behavioral Patterns (July 2024)

- **Company ID XXXXX:** *******. Transactional patterns consistent with a third-party ACH processor.
- **Company ID XXXXXX:** This originator submits batches under 1,309 difference names all appearing to be international (IAT) transfers.
- **Company ID XXXXXX:** ******** Transactional patterns consistent with a third-party ACH processor.
- **Company ID XXXXXXX:** ****** appears to be a FinTech. Transactional patterns consistent with a third-party ACH processor.
- **Company ID XXXXXXX:** ****** appears to process payments between businesses but with infrequent volumes for large dollar amounts. Review credit limits for potential adjustments.

Did we learn something?

Test our Knowledge– AI

- **Question 6.** The next time a vendor comes to you and says “leverage the power of AI……”, what are you going to ask them?

A) What type of AI are you using?

B) What data was used to train the model?

C) Will any of my data be used to train the model? How will my sensitive and confidential data be protected?

D) How will you help me demonstrate compliance for my regulators?

E) All of the above

affirmative™
TECHNOLOGIES

Test our Knowledge– AI

- **Question 6.** The next time a vendor comes to you and says “leverage the power of AI……”, what are you going to ask them?

A) What type of AI are you using?

B) What data was used to train the model?

C) Will any of my data be used to train the model? How will my sensitive and confidential data be protected?

D) How will you help me demonstrate compliance for my regulators?

E) All of the above

affirmative™ TECHNOLOGIES

Connect With Affirmative

Aaron Calipari

President and CEO

acalipari@affirmativeusa.com

https://www.linkedin.com/in/aaroncalipari/

https://www.linkedin.com/in/affirmativeusa/

Download a free copy of our **AI Initiative Questionnaire** to assist your organization in developing clarity with some of these concepts we discussed today for any AI initiative you undertake.