Infosys topaz | Infosys cobalt

VIEW POINT

HOW AI COPILOTS ARE RESHAPING THE BANKING INDUSTRY

Infosys
Navigate your next

Summary

Overview of AI Copilots

AI Copilot is an advanced AI assistant designed to support various tasks and enhance productivity. It can provide real-time insights, automate routine processes, and offer intelligent recommendations. With capabilities like natural language understanding and adaptive learning, AI Copilot helps users make informed decisions, streamline workflows, and improve overall efficiency. Whether it's for business, education, or personal use, AI Copilot is a versatile tool that adapts to your needs and simplifies complex tasks. Integrating AI Copilot with the fraud protection module of Microsoft Dynamics 365 in the banking industry offers a powerful combination to enhance security and efficiency.

AI Copilot in Banking

Real-Time Analysis

AI Copilot can analyze a vast amount of transaction data in real time, identifying suspicious activities and flagging them for further investigation. This helps in preventing fraudulent transactions before they are completed.

Behavioral Analysis

AI Copilot monitors customer behavior across various channels (online banking, mobile apps, etc.) to detect anomalies. For instance, sudden changes in spending patterns can be flagged as potential fraud.

Predictive Analytics

By leveraging predictive analytics, AI Copilot can forecast potential fraud scenarios based on historical data and emerging patterns. This proactive approach helps banks stay ahead of fraudsters.

Enhanced Customer Experience

By reducing false positives, AI Copilot ensures that legitimate transactions are not incorrectly flagged, improving the overall customer experience.

User Case: **Fraud Detection Assistance** Using AI

User Case	Industry	Description
Fraud Detection Assistance	**BFSI**	**Purpose:** A lot of fraudulent transactions happen, leading to a lot of financial losses to the banks and financial institutions. **Global Financial Losses:** In 2024, the Federal Trade Commission (FTC) reported that consumers lost over **$12.5 billion** to fraud, marking a **25% increase** from the previous year. The FTC received fraud reports from **2.6 million consumers**, with the most commonly reported scams being imposter scams and online shopping issues. Specifically, imposter scams account for nearly **$2.7 billion** in losses. **Reference:** New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024 | Federal Trade Commission

Challenges and Pain Points

Increasing Sophistication of Financial Fraud

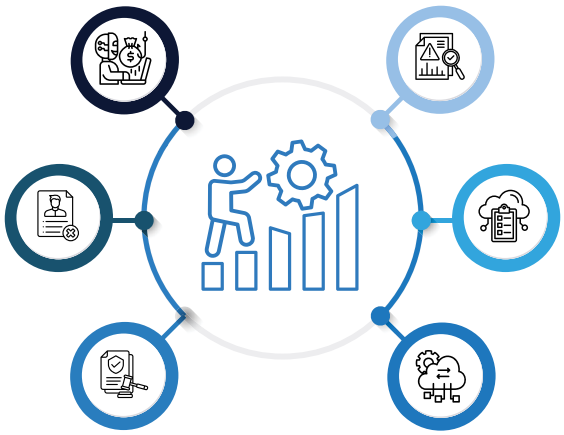
Fraudsters are becoming more sophisticated, leveraging advanced technologies like AI-generated deepfakes and synthetic identities to outsmart traditional security measures. This makes it increasingly difficult for banks to detect and prevent fraudulent activities, leading to significant financial losses and reputational damage.

Manual Effort in Fraud Investigations

Fraud investigations often involve labor-intensive manual processes, such as reviewing transaction histories and verifying customer information. This not only increases operational costs but also slows down the response time, allowing some fraudulent activities to go undetected.

High False-Positive Rates Causing Customer Dissatisfaction

False positives occur when legitimate transactions are incorrectly flagged as fraudulent. This not only frustrates customers but also erodes their trust in the financial institution. High false-positive rates can lead to lost sales, increased operational costs, and a negative impact on customer experience.



Real-Time Transaction Monitoring and AML Compliance

Real-time transaction monitoring is crucial for detecting suspicious activities as they happen. However, implementing effective real-time monitoring systems that comply with AML regulations is complex and resource intensive. Financial institutions must balance the need for thorough scrutiny with the efficiency of transaction processing.

Compliance and Regulatory Pressures

Banks operate in a highly regulated environment and must comply with numerous regulations related to anti-money laundering (AML), counter-terrorist financing (CTF), and consumer protection. Keeping up with evolving regulatory requirements is challenging and requires significant resources, both in terms of time and money.

API Security

APIs are essential for modern banking operations, enabling seamless integration and data exchange between systems. However, they also present significant security challenges. Ensuring robust API security is critical to protect sensitive financial data from cyberattacks and unauthorized access.

How AI Copilots Along with Microsoft Dynamics 365 Fraud Protection Can Address Banking Challenges

Real-Time Fraud Alerts with Reasoning

AI Copilot can significantly enhance real-time fraud detection by providing instant alerts with detailed reasoning. This involves using advanced AI algorithms to analyze transaction patterns and flag suspicious activities. The system can explain why a transaction is considered risky, helping fraud analysts make informed decisions quickly. This reduces the time taken to respond to potential fraud and minimizes the impact on customers.

Automated Case Triaging Based on Risk Scores

The Microsoft Dynamics 365 Fraud Detection Module can automate the triaging of fraud cases by assigning risk scores to transactions. This allows the system to prioritize cases based on their risk level, ensuring that high-risk cases are addressed promptly. Automated triaging reduces the manual effort required and ensures that resources are focused on the most critical threats.

Reference: Microsoft Learn – Account Protection Overview

Conversational AI for Fraud Analysts

AI Copilot can act as a conversational assistant for fraud analysts, simplifying complex tasks through natural language interaction. Analysts can query the system for detailed transaction data, request explanations for alerts, and even set up new rules or patterns for fraud detection. This enhances the efficiency of fraud investigations and allows analysts to focus on more strategic tasks.

Adaptive Learning for Fraud Pattern Updates

Adaptive learning capabilities enable the system to continuously update its fraud detection models based on new data. This means that as fraud patterns evolve, the system can learn and adapt in real time, improving its accuracy and reducing false positives. This dynamic approach ensures that the fraud detection system remains effective against emerging threats.

Reference: Microsoft Learn – Service FAQ

Azure API Management and Zero Trust Security

Integrating Azure API Management with a Zero Trust security model ensures that all API interactions are secure and verified. This involves implementing strict access controls, continuous monitoring, and encryption to protect sensitive data. Zero Trust principles assume that every request could be a potential threat, so they verify each request explicitly, minimizing the risk of unauthorized access.

Reference: Microsoft Learn – Compliance Overview

We can leverage the Microsoft Dynamics 365 Fraud Protection Module which includes the following:

Purchase Protection

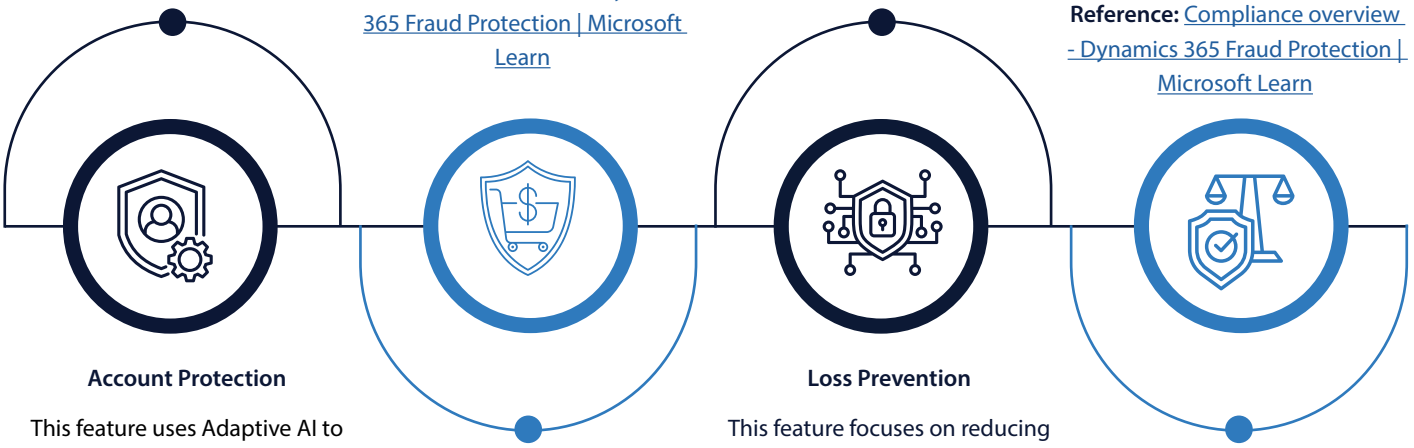
This helps identify and prevent fraudulent transactions in real-time, using AI models that analyze transaction data for anomalies.

Reference: Service FAQ - Dynamics 365 Fraud Protection | Microsoft Learn

Compliance and Security

Microsoft Dynamics 365 Fraud Protection is designed with compliance, privacy, security, and confidentiality in mind. It helps businesses comply with data protection laws and manage data subject requests.

Reference: Compliance overview - Dynamics 365 Fraud Protection | Microsoft Learn



Account Protection

This feature uses Adaptive AI to learn and adapt to patterns of legitimate and fraudulent account activities. It includes fingerprinting to detect returning devices and bot protection to defend against synthetic accounts.

Reference: How account protection works - Dynamics 365 Fraud Protection | Microsoft Learn

Loss Prevention

This feature focuses on reducing fraud-related losses by identifying patterns of fraudulent behavior and taking proactive measures to prevent them.

Reference: Service FAQ - Dynamics 365 Fraud Protection | Microsoft Learn

These solutions collectively enhance the ability of financial institutions to detect, prevent, and respond to fraud more effectively.

Benefits of Using Microsoft Dynamics 365 and AI Copilot in Banking

Copilot could integrate with a bank's fraud detection system to provide real-time suggestions or insights on transactions that look suspicious. If a banker types a query about a particular transaction, Copilot could provide immediate context about why it might be flagged or why further investigation may be warranted.

Enhanced Fraud Detection

The integration of AI Copilot with Microsoft Dynamics 365 Fraud Protection enables banks to detect and prevent fraud more effectively by leveraging advanced AI models and real-time data analysis.

Improved Operational Efficiency

Automating fraud detection processes reduces the need for manual intervention, allowing bank staff to focus on more complex tasks.

Better Customer Trust

By providing a secure banking environment and reducing the incidence of fraud, banks can enhance customer trust and loyalty.

AML (Anti Money Laundering)

A user deposits Rs 10000 every 15 minutes into a different account. AI detects suspicious money laundering behavior and freezes the transaction for further review and compliance.

Azure API Management and Zero Trust Security

A hacker attempts brute-force login attacks on API endpoints. The system auto-detects abnormal API traffic and blocks access.

By combining AI Copilot with Microsoft Dynamics 365's fraud detection capabilities, banks can create a robust defense against fraud, enhancing both security and customer trust.

References

1) Account protection overview - Dynamics 365 Fraud Protection | Microsoft Learn

2) How account protection works - Dynamics 365 Fraud Protection | Microsoft Learn

3) Service FAQ - Dynamics 365 Fraud Protection | Microsoft Learn

4) Compliance overview - Dynamics 365 Fraud Protection | Microsoft Learn

5) New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024 | Federal Trade Commission

About the Author

Devendra Kumar Dubey

Senior Associate Consultant- Microsoft Dynamics, Infosys

Devendra brings over 7 years of diverse industry experience spanning IT, Semiconductor and Renewable Energy. He has successfully led initiatives focused on cross-functional collaboration, improving operational efficiency and transforming business processes. Devendra is recognized for his ability to navigate complex challenges with clarity, lead teams effectively and drive business-aligned outcomes. His achievements include the Best Leader Award at Samsung and the RISE INSTA Award at Infosys, reflecting his impact and dedication. With a management degree that has further sharpened his strategic and analytical capabilities, he aims to deliver long-term value by bridging technology and business and contributing meaningfully to enterprise growth.