UNISYS | Securing Your Tomorrow®

How AI and Machine Learning are Securing Financial Institutions

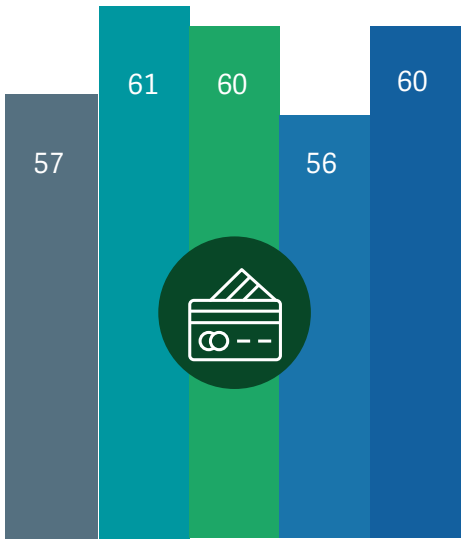
By Jorge Andrés Gómez

49% of respondents do not trust their bank to alert them of suspicious activity.

2021 is unique in that we've lived a full year in "the new normal," and with that came significant changes. Cloud computing helped function as a catalyst for digital banking transformation, as more people needed to work and bank from home. At the same time, as more of our lives, transactions and ways of connecting moved online, the security of all these interactions has become increasingly important. It's safe to say the financial services industry has entered the era of the AI digital marathon.

The Unisys Security Index™ surveyed 11,000 people across 11 countries on a wide range of issues including personal, financial, national and internet security concerns.

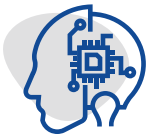
Of the eight areas of concern measured, the 2021 results show that bankcard fraud ranks number two, up four points when compared to 2020 results. More concerning is that 49% of respondents do not trust their financial institution to alert them of suspicious activity on their account.



Of the 8 security concerns, bankcard fraud ranks #2

Artificial Intelligence (AI)

What is AI? Artificial intelligence (AI) is the overall science of using computers or machines to solve problems that are usually done by humans with our natural intelligence. Machine learning is a subfield of artificial intelligence. At the most basic level, machine learning recognizes patterns in data, and helps describe the process that generates data used to predict future behavior. Machine learning uses algorithms that iteratively learn from data, allowing computers to find insights without being programmed to do so.



AI helps improve efficiency, enable growth, manage risk, and most importantly makes a world of difference for customer experiences.

The financial services industry has long been technology-dependent and data-intensive, and data-enabled AI technology can drive innovation further and faster than we ever imagined. AI helps improve efficiency, enable growth, manage risk, and most importantly makes a world of difference for customer experiences. Once expensive, AI systems are now becoming more the norm, with cost and barriers to adoption falling. What we see are financial institutions making targeting investments in cloud, big data, and data applications such as microservices, eliminating the capital investment needed to develop, deploy, and scale AI solutions. One of the ways in which financial institutions have embraced AI in their customer service operations is via chat bots and conversational banking.

Care to Chat?

Remember when internet banking was considered cutting edge? Then we had mobile banking when smartphones took over the world. Now, it's all about conversational banking, enabled by AI. Simply put, conversational banking is communication between a financial institution and its customers via text, voice, or visual interface. It's important as it adds an extra personal touch to customer relationships. Financial institutions are tasked with improving customer experiences. To do so, they have to understand the true needs of their customers. This is where advanced analytics and machine learning can help, crunching the data and allowing humans to perform higher value tasks. From account opening, authentication, and cancellation of credit and debit cards, chatbots can perform the "boring" tasks once performed by humans.

Conversational banking isn't the only area where AI and machine learning are making huge strides. Today, we see machine learning as a key component of many financial institutions' fraud prevention efforts.

Machine Learning Is a Critical Fraud Prevention Tool

Surprisingly, machine learning adoption to combat fraud is not uniform across financial institutions. As consumers, we tend to assume our financial institution—no matter what size—has the latest fraud prevention technology. Among major financial institutions in the U.S. with more than $100 billion in assets, more than 72% are using machine learning systems to combat bankcard and credit card fraud. But what about smaller institutions with $10 million or $100 million in assets? It turns out that only 6% of those institutions in the U.S. have adopted machine learning systems to combat fraud, according to PYMTS.com research.[1] Now, we see why nearly half of survey respondents do not trust their financial institution to alert them to suspicious activity.

Many of these smaller financial institutions need a trusted partner to help them adopt machine learning technology and enable real-time monitoring. This will also drive cost savings, as it's much cheaper to prevent a fraudulent transaction up front compared to investigating a potential fraudulent transaction after the fact.

When we look at the most prevalent types of fraud, credit card fraud tops the list. This type of fraud is also one of the most preventable. For example, to detect credit card fraud, financial institutions train their machine learning systems to look for patterns of common suspicious behavior based on vast amounts of data.

[1] Fraud Prevention At Banks With AI And ML | PYMNTS.com

Surprisingly, machine learning adoption to combat fraud is not uniform across financial institutions.

Jorge Andrés Gómez
Jorge Andrés Gómez is the Industry Director for Financial Services at Unisys.

He can be reached at Jorge.gomez@co.unisys.com or connect with him at LinkedIn.

The key word here is data. Financial institutions require vast amounts of fraud data to train machine learning systems. This data includes meaningful features of the credit card user's transactions, including date, amount, product category, provider, and user behavioral patterns. This data then goes through a trained machine learning model that finds patterns and rules to classify whether a transaction is legitimate or fraudulent. However, this is based on known types of fraud. What about new types of fraud that bad actors haven't designed yet?

To combat this, some financial institutions are creating synthetic data on uncommon fraud patterns to train their machine learning systems. This is essential to moving from a reactive to a proactive approach for fraud detection. Synthetic data can augment a financial institution's existing data set of fraud behaviors to improve its overall fraud detection machine learning models.

Why Do People Not Trust Their Financial Institutions?

According to PYMNTS.com, "Human analyst teams not only have a hard time detecting fraud as it happens – 45% of financial institutions say investigations take too long to complete."[2] These investigations unfortunately have high false-positive rates of up to 90%, where legitimate transactions are identified as being fraudulent. The end result is frustrated customers, and worst-case scenario, customer abandonment.

Conclusion

Financial institutions that move from a reactive to a proactive approach for fraud detection will be better positioned to build trust with their customers and stay a step ahead of rapidly evolving and increasingly complex cyber threats. To do that, financial institutions must embrace technologies like AI and machine learning to drive better customer experiences and combat fraud in a systemic manner. Doing so will increase employee productivity and strengthen consumer trust, which leads to greater loyalty and happier customers.

2. Fraud Prevention At Banks With AI And ML | PYMNTS.com

To learn more about financial services, visit www.unisys.com/industries/financial-services

For more information visit www.unisys.com