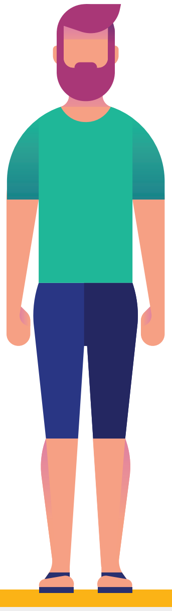
Transforming Payment Security Through Artificial Intelligence

VISA

Table of Contents



Executive Summary

In a sector as dynamic as payments, the power and reach of Artificial Intelligence (AI) is vast. It will power the security foundation necessary to deliver the frictionless, secure payment experiences that consumers have come to expect. This paper will provide an overview of how AI is set to transform the payment security landscape and how Visa leverages AI to build capabilities that enable its partners to improve decision making, enhance risk management, and move beyond the tradeoff between ensuring payment security and providing a seamless experience.

Meet Avery

Follow Avery's journey to see how his day-to-day experiences are impacted and shaped by AI.

Artificial Intelligence: An Introduction

Over the past few decades, technological innovation has focused on greater automation and connectivity, resulting in the realization of significant societal and economic benefits. The next transformation in technology, driven by Artificial Intelligence (AI), promises unprecedented gains as it enables consumers to conduct a wide variety of day-to-day activities in easier and more efficient ways.

The prospective impact of AI on financial services broadly and payments specifically will be no less dramatic. With AI, payments can move beyond the transaction and become increasingly automated, interactive and personalized, embedded across everyday experiences and across all channels and devices. However, this evolution in payments can only be realized by security frameworks that advance and evolve as security threats do.

Artificial Intelligence: Definition and Use Cases

AI is the theory and development of computer systems to perform tasks that normally require human intelligence. AI makes it possible for machines to learn from experience, adjust to new inputs and perform human-like tasks. AI manifests itself into three main business applications: **machine learning, natural language processing** and **image recognition.**

Machine Learning

Machine learning allows machines to learn iteratively from data to perform a specific task, without being explicitly programmed to do so. Deep learning is a particular class of machine learning based on artificial neural networks, a computational approach inspired by the human brain's use of synaptic connections to solve problems.

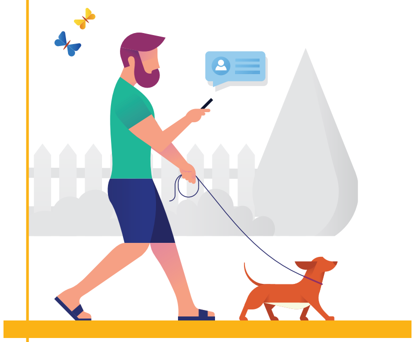
Machine learning has provided a new way for banks to evaluate, approve, and manage credit applications. With machine learning, banks can leverage non-traditional data points like telecom and utility bill payment history to approve credit-worthy individuals who may not have a traditional credit history. This use case has the potential to impact the 1.7 billion people who are financially underserved by offering them access to formal credit networks.[1]

At home, Avery goes onto an online marketplace to order a book and sees other options under a section titled "customers who bought this item also bought" and adds a suggested book to his cart. Avery then goes onto his streaming service, and his homepage has a "recommended for you" section that aligns with Avery's typical taste in shows.

Natural Language Processing

Natural language processing (NLP) refers to a machine recognizing spoken words, digesting those words by converting them into text, inputting the text into a search mechanism and, lastly, returning results to the initial command. Virtual digital assistants are the most common application of this use case. In fact, the number of virtual digital assistant users is expected to grow to more than 1 billion users by 2025. Beyond popular digital assistants like Amazon's Alexa, banks globally are offering chatbots to their consumers to digitize the customer service experience and to differentiate themselves to digital-first customers. SEB Group, a bank in Sweden, launched a chatbot named Aida that helps bank customers with a variety of card-related issues and account questions. In addition to the ease of use for consumers, chatbots are expected to save businesses more than $8 billion per year by 2022.[2]

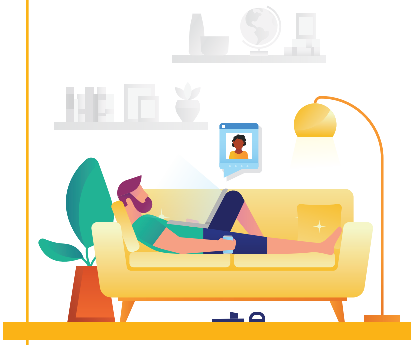
The applications of natural language processing extend far beyond chatbots. For example, NLP can also be used to extract information from applications, helping streamline the often cumbersome onboarding process where 25% of customers abandon their applications due to problems stemming from Know-Your-Customer (KYC) friction and shorten the time for onboarding. Additionally, NLP can automatically classify documents making it easier for financial professionals to verify they have all the required details needed to comply with KYC regulations.



Avery notices a transaction on his debit card statement that he doesn't recognize. With ease, Avery reaches out to the chatbot in his mobile banking app. Within 30 minutes, Avery's problem was solved. Avery was incentivized to reach out to customer service because his bank offered him an accessible, secure, and time-saving option.

Image Recognition

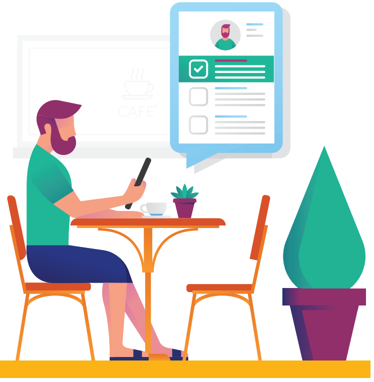
Image recognition uses AI to identify places, people, logos, objects, and buildings. Amazon Go, an automated retail experience, is an example of the technology. In Amazon Go stores, customers can take items out of the store without waiting to check out because the store deploys image recognition to detect when products are taken or returned to shelves and keeps track of them in a customer's virtual cart. From a financial services perspective, issuers are increasingly leveraging facial recognition for mobile-log in, significantly reducing the time it takes for their users to access their accounts and complete their banking activities.



Avery logs on to his social media account and uploads a photo album. When Avery tags his friends in the photos, the social media service has provided him with recommended people to tag. Today, computer vision can recognize people with 98% accuracy, which is at par with humans' performance, creating a speedy and accurate tagging process for users like Avery.[3]

Visa's Deployment of Artificial Intelligence for Payment Security

Visa's AI-driven solutions aim to create a more secure and safe payments ecosystem. As Scott Boding, Vice President at Visa and AI expert, states, "We are trying to use AI as a way to seize and automate a lot of the heavy lifting in fraud detection — a time-consuming task that many clients are doing manually today. We are trying to use AI to increase efficiencies for our clients."[4]



Delivering a Secure, Frictionless Experience

Account Onboarding

As cyber attacks increase in scope, criminals are exploiting consumer data elements to perpetrate synthetic identity fraud, combining real and fake information to create a new identity that is used to open new accounts and make fraudulent purchases and loans. In a Forrester Consulting study commissioned by Visa, 39% of surveyed firms globally experienced new account fraud (e.g., using stolen identifying information to open a fraudulent account) in the past two years, and 32% of surveyed firms globally experienced synthetic identity fraud in the same period.

Aiming to solve the pain points associated with the onboarding process for customers, Visa developed Visa Advanced Identity Solution (VAIS), which leverages machine learning to analyze fraud migration patterns across issuers and irregular use of identity elements during the application process. VAIS generates a risk score that issuers can then use to inform their decision on the applicant. It leverages Issuers' Clearinghouse Service data, which gathers applications across all issuers that have been approved or declined for a particular consumer, the velocity of the consumer's applications, and other relevant data elements. It then incorporates this data and uses pattern recognition and machine intelligence to create dynamic consumer persona-based profiles, enabling application verification to be performed in real-time and at scale.

Avery would like to apply for a credit card with a new issuer, First Digital. It is his first interaction with the issuer and presents First Digital with an opportunity to deliver a seamless application and onboarding process to gain Avery's business. By running traditional and non-traditional data through its machine learning model, First Digital was able to develop a tailored view of Avery's creditworthiness and approved his application in an efficient manner.

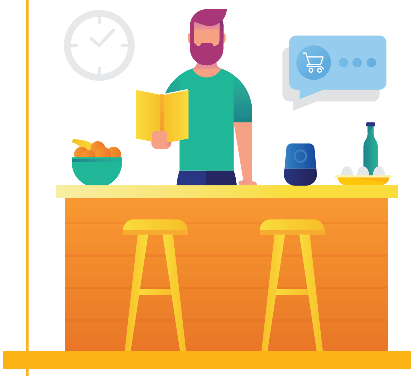
When Avery applied for a credit card, he experienced a quick and relatively painless process that was enabled by First Digital's deployment of AI to streamline the important security process known as Know-Your-Customer (KYC) to verify his identity and assess any potential risks associated with his application.

Authentication

As consumer interactions migrate to digital channels, authenticating consumers digitally using traditional forms of identity is challenging, especially as consumers' expectations for frictionless experiences are concurrently increasing. In a Forrester Consulting study commissioned by Visa, 34% of global respondents stated that complicated end user authentication is a key challenge they face with managing payment security. Firms have to simplify the authentication process for their consumers as well as invest in the right tools that enable them to assess accurately that the user is who they say they are. This is especially key given the increasing complexity of fraud: in the same Forrester study, 32% of firms globally experienced account takeover fraud in the previous two years.

In an effort to provide seamless yet secure authentication, firms are implementing various authentication methods such as biometrics. Visa Biometrics is a solution that provides multi-factor and out-of-band authentication, allowing consumers to authenticate themselves in a secure and seamless manner through face, fingerprint, and voice while reducing the friction associated with PINs and passwords. Additionally, this biometric solution applies cutting-edge machine learning to validate the biometric matching and identify "spoof attacks", layering an extra level of security on for the customer.

Additional data elements such as biometrics can be used to assess user identity more accurately without introducing unnecessary friction into the process. Visa Consumer Authentication Service (VCAS) leverages data points, like account profiles and geo-location, to support an issuer's authentication strategy and score each authentication request. VCAS uses risk-based authentication that enables issuers to quickly and dynamically assess the risk of a transaction, apply rule criteria based on data modeling, and determine if they have a high confidence level to authenticate their cardholder passively in the background, or if they need to engage the cardholder more actively. On the other side of the transaction, merchants can use Cardinal Consumer Authentication to engage in sophisticated, AI-powered anomaly monitoring and detection. The greater data exchanged between merchants and issuers optimizes risk decisions over time, resulting in reduced friction for the consumer. Visa is using AI to create secure authentication solutions that enable our partners to navigate successfully the evolving payments landscape.



Avery goes to the kitchen to prepare his dinner and he realizes he failed to pick up key ingredients, so he utilizes his voice assistant to order groceries. Over time, the voice assistant has learned Avery's voice, recognizes the voice as Avery's, and is able to authenticate his identity using his voice biometric.

Authorization

A significant obstacle firms face is the generation of false positives when trying to identify fraudulent transactions, meaning that oftentimes they are unable to separate the legitimate transactions from the illicit ones. This is especially relevant in the digital channel, where risk management is as much about enabling good sales as it is about avoiding fraud. In 2018, $278 billion in card-not-present transactions were declined globally, representing a 27% year-over-year growth.[5] AI can analyze large amounts of transaction data, helping to identify sophisticated criminal activity more accurately and ultimately allowing firms to minimize their false positives and approve more transactions that are legitimate.

Using the power of AI, Visa has created sophisticated tools to ensure cardholders are protected from fraud, merchants can submit their orders confidently, and issuers can approve the legitimate transactions while declining illegitimate ones. Issuers can take advantage of Visa Advanced Authorization (VAA), which evaluates VisaNet authorizations in real time, helping issuers promptly identify and respond to emerging fraud patterns and trends. Using sophisticated risk detection technologies, VAA evaluates 100% of Visa card authorizations that flow through its network. As transactions are processed, VAA assigns a risk score, and with VAA, issuers can stop potential fraud losses before the transaction goes through. Today, VAA is used by more than 8,000 issuers in 129 countries and in 2018 alone prevented an estimated $25 billion in fraud.[6]

Complementing the work of VAA is Visa Strategy Manager, a service that applies algorithms to a client's historical data and identifies correlations between pockets of fraud that might otherwise go undetected. These algorithms are then fed into Visa Risk Manager, which is the intelligent decisioning solution powered by VisaNet that allows banks to decline only the highest-risk transactions while optimizing approval rates at the point of purchase.

To enable and empower merchants in this space, Visa provides CyberSource Decision Manager (CyberSource DM). CyberSource DM has more than 260 anomaly detectors and 15 region- channel- and industry-specific risk models, each optimized to identify fraud in different scenarios. Meanwhile, machine learning is ingrained in its fraud-fighting capabilities as part of the patented approach called real-time fusion modeling. Real-time fusion modeling leverages the proven effectiveness of conventional static models with the more agile data analysis capabilities of today's most advanced self-learning models to help businesses more effectively and efficiently manage and detect fraud.

With these offerings, issuers and merchants can be confident an extra layer of protection is added when their cardholders and consumers are transacting.

Considering the ease by which Avery was able to place the order, he would be frustrated if his issuer were to decline the transaction. On the other hand, if his issuer were to authorize a fraudulent transaction, Avery would have to contact the issuer and dispute the charge – a frustrating experience. Fortunately, Avery's issuer uses sophisticated algorithms to score the riskiness of the transaction and, determining the risk level to be relatively low, approves the payment.

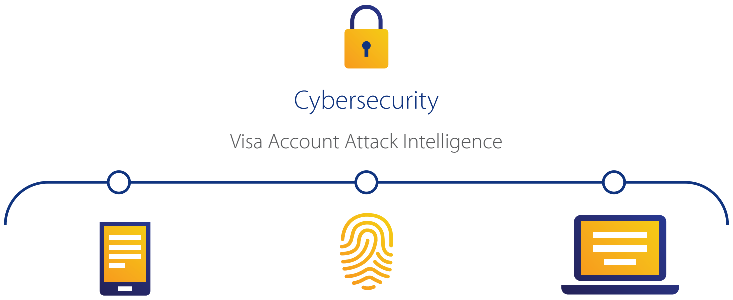
Protecting the Ecosystem Through Cybersecurity Services

Our hyper-connective world is creating new ways to exploit consumers' information and data. In 2018, the cybercrime business was estimated at $600 billion,[7] and the average cost of a data breach is nearly $1.2 million.[8] In 2018 alone, there were 2.7 billion records exposed globally.[9] Given the magnitude of this problem, cybersecurity is top of mind for both consumers and businesses.

AI can be used to help solve this pervasive problem. As attacks continuously evolve, it is crucial that companies also adapt and develop a fluid and dynamic approach to detecting and stopping these attacks. Visa recognizes the importance of evolving its strategy and has created solutions that serve to protect both consumers and companies beyond the transaction. For example, Visa Account Attack Intelligence, an AI-driven solution, applies deep learning to Visa's vast number of processed transactions through VisaNet to identify issuers and merchants as well as BINs that are being used by cyber criminals for guessing PANs, expiration dates and CVV2 codes through account testing. The machine learning technology detects sophisticated enumeration patterns, eliminates false positives, and alerts affected financial institutions and merchants before fraudulent transactions begin. Visa is committed to protecting the integrity of the payments ecosystem and safeguarding cardholder information — and this solution allows Visa to successfully achieve that goal.

Visa recognizes the importance of evolving its strategy and has created solutions that serve to protect both consumers and companies beyond the transaction.

Visa is innovating and leveraging AI to secure transactions throughout the lifecycle



Cybersecurity

Visa Account Attack Intelligence

	Onboarding	Authentication	Transaction Security
Issuer	Visa Advanced Identity Solution	Visa Consumer Authentication Service	Visa Advanced Authorization Visa Strategy Manager
Merchant		Cardinal Consumer Authentication	CyberSource Decision Manager
Both		Visa Biometrics	

Innovative Fraudsters and Artificial Intelligence

Fraudsters are continually innovating their methodologies and attack vectors and are likely to use AI to advance beyond just simple hacking techniques. With AI, fraudsters can streamline social engineering tactics and optimize cybersecurity evasion. Moreover, with advancements in AI technology, fraudsters can easily (and cheaply) conduct attacks, both parallel and distributed. They just need access to readily available servers and basic coding skills.

In the case of social engineering, fraudsters are creating what appear to be legitimate videos, audio files, and emails designed to trick individuals into compromising actions. As a result, the consumer may click on an illegitimate link allowing the fraudster to either capture the consumer's personal information or gain access into an otherwise private corporate IT system on a greater scale than what happens currently; this is a rampant problem, and 1 in 3 companies worldwide has been affected by social engineering.[10]

Fraudsters can also leverage AI and combine it with existing malware techniques to create a new, challenging strain of malware. As soon as the target is identified either via facial recognition, geolocation, or voice recognition, the malicious action is released; however, prior to the attack, the malware will go unnoticed.

To combat these potential challenges, it is critical to continue sharing intelligence across the ecosystem and collaborating on strategies that provide industry-level solutions.

To combat these potential challenges, it is critical to continue sharing intelligence across the ecosystem and collaborating on strategies that provide industry-level solutions.

A Look Forward

The impact of artificial intelligence on consumers' lives is transformative. AI today looks entirely different from its inception 50 years ago, and AI will look vastly different 50 years from now. Regardless of these changes, the need for security and trust between consumers, merchants and financial institutions will remain a constant. While most of the AI research and applications focus on pattern recognition and sound recognition, there is less work around transactional (i.e., time series) data when it comes to deep learning. Visa combines a significant stock of payment data with unparalleled technical expertise to advance industry-leading research in deep learning for transactional data applications. This has resulted in several patents for solutions that not only leverage deep learning at massive scale but also do it in sub-milliseconds. Visa will continue to develop and deploy powerful applications of AI to reinforce this foundation of security and lead the way in deep learning for payments.

Visa will continue to develop and deploy powerful applications of AI to reinforce this foundation of security and lead the way in deep learning for payments.

About the Authors

Michael Jabbara is a senior director in Visa's Global Risk organization and leads strategic initiatives in its Global Risk Strategic Initiatives, Execution & Operations function. He can be reached at yjabbara@visa.com.

Sofia Katsaggelos is a business development analyst in Visa's Merchant Sales & Acquiring organization. She can be reached at sokatsag@visa.com.

Acknowledgments

The authors would like to thank their many Visa colleagues whose insights and expertise are reflected here, and in particular Carolina Barcenas, Melyssa Barrett, David Capezza, Ann Ewing, David Henstock, Aruna Joshi, Andrew Naumann, Penny Lane, Tara Lavelle, Shane Malloy, John Zhan, and Anna Wintle.

Terms of Reference

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and are intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.

These materials and best practice recommendations are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory or other advice. Recommended marketing materials should be independently evaluated in light of your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of the marketing materials, best practice recommendations, or other information, including errors of any kind, contained in this document. This document is intended for illustrative purposes only. It contains depictions of a product currently in the process of deployment, and should be understood as a representation of the potential features of the fully-deployed product. The final version of this product may not contain all of the features described in this presentation.

[1] Forbes, 1.7 Billion Adults Worldwide Do Not Have Access To A Bank Account, June 2018

[2] Financial Brand, Meet 11 of the Most Interesting Chatbots in Banking, March 2018

[3] Fortune, Facebook's new algorithm can recognize you even if your face is hidden, June 2015

[4] PYMNTS.com, Visa CyberSource: AI's Role Is To Predict — Not to Know, May 2019

[5] Excludes insufficient funds and issuer/switch inoperative declines. eCommerce purchases for the year ending in CY18. YoY growth based on CY18 vs. CY17. Sales based on VisaNet authorization data. Fraud based on issuer reported TC40 (including transactions which were not processed on VisaNet.)

[6] PYMNTS.com, 'Visa Advanced Authorization Blocks $25 Billion In Fraud', June 2019

[7] BusinessWire, New Global Cybersecurity Report Reveals Cybercrime Takes Almost $600 Billion Toll on Global Economy, February 2018

[8] Kaspersky Lab, What is the Cost of a Data Breach, May 2018

[9] BloomBlog, 2018: The Year of the Data Breach, December 2018

[10] T-Systems, Social Engineering, 2019

VISA