A REFERENCE GUIDE

A-Z of Fraud Prevention Innovations

Making the world a safer place to transact, together

FEATURE SPACE

OUTSMART RISK

TSYS

A Global Payments Company

Introduction

As fast as your organization can innovate, criminal networks are inventing new ways to scam, trick and defraud your customers. In an increasingly digital world, banks, fintechs, merchants, and payment providers need scalable, intelligent solutions and services that outsmart risk.

TSYS and Featurespace combine our expertise and capabilities to bring you the complete A to Z of fraud trends, and the innovations in anti-fraud technology that you'll need to beat these threats.

APIs

APIs drive the potential for seamless, secure data sharing to enrich fraud scoring and model data sets. Our vision is for issuers to feed their enriched processing data and external data as inputs or outputs using APIs to gain a deeper intelligence on identity threats or risky behaviors.

Financial institutions are increasingly looking to best-in-breed partners to support them not only with issuing and processing services, but also fraud services, driven by a desire to access the best possible fraud prevention technologies without lengthy implementation projects in-house. Fraud is moving and scaling faster than individual financial institutions can keep up, and they need help now. Accessing the insights from machine learning be simplified with APIs, which make connectivity to fraud services quick and seamless as well as facilitate the enrichment of fraud scoring with other non-monetary data such as customer information.

Using APIs, TSYS can quickly onboard financial institutions and payment processors to **Foresight Score** to begin protecting their end customers' transactions in as little as a few weeks with parallel scoring environments rapidly live.

B Behavioral Analytics

Featurespace invented Adaptive Behavioral Analytics because we know that the only predictable thing about people is their changing habits.

The challenge in payments fraud is not spotting fraud, it's understanding individual customer behaviors and how those evolve over time. None of us act, think or spend the same way for our entire lives. Machine learning can aid in accurately identifying genuine customer behavior. But traditionally machine learning systems remain static, as the learning process is complex and typically requires human oversight. Over time static models degrade in performance, as the previously learnt patterns and trends do not align to the current behavior being processed by the system. Machine learning models can produce superior results to a rules-based system, however if the models remain static, they still suffer from performance degradation over time. Featurespace developed 'self-learning' machine learning algorithms, adaptive behavioral analytics, that continue to evolve and adapt to consumer and fraud trends. Unlike traditional rules-based decision making, machine learning models do not degrade over time, as they can "self-learn" from experience. This enables businesses to make more accurate fraud and risk decisions at speed and scale, with minimal manual intervention to update the fraud management system.

Using Adaptive Behavioral Analytics, Featurespace's machine learning models automatically evolve over time, continuing to learn and adapt to new patterns and trends to ensure optimal performance. **Discover more**.

Cloud

It's no longer a question of 'if' cloud, but 'how soon' for fraud systems in financial crime prevention. Moving to the cloud will bring efficiencies for issuers: to implement fraud strategies faster; to decrease time spent on rule maintenance with Predefined Features; and to increase efficiency across functions with plug-and-play configurations for easier integrations.

New fintech competitors are born in the cloud, and it is clear how this new environment is leveling the playing field in financial services. Even small neobanks and new entrants can purchase trusted, world-class solutions thanks to the scalability of platforms which can grow with them.

Payment processing and transaction monitoring platforms are moving to the cloud, like many of the services we use in our everyday life. The advantages in terms of speed, agility and innovation are unparalleled. It's not about replicating legacy services and thought processes, but about planning for a whole new paradigm. But moving processing platforms to the cloud has implications for the business as orchestration between different platforms can pose data and security challenges. However, by approaching this orchestration challenge with a new cloud-native mindset, financial institutions may find new synergies between historically disparate systems. But be warned, fraud innovations such as machine learning in the cloud demand precise orchestration capabilities to ingest data inputs from across a financial institution's complete environment.

Featurespace is rearchitecting for the cloud to take advantage of the latest technologies and stay at the forefront of innovation. **Read more about how to overcome legacy technology constraints in financial services**.

D

Deep Learning

Criminals have the darknet, but we have deep learning to outsmart them. Truly the next generation of Machine Learning, transformative Automated Deep Behavioral Networks from Featurespace, built on Recurrent Neural Network-based architecture, improves fraud detection across the board.

Until now, the use of Deep Learning technology in detecting and preventing fraud in card and payments had not been optimized into a software product to operationalize the protection of companies and their customers. Featurespace's latest innovation, Automated Deep Behavioral Networks (ADBN), is fast-tracking Featurespace's data science exploration based on Recurrent Neural Networks to create smart memory and enable automated feature discovery for fraud detection.

To build effective machine learning models* for fraud prevention, data scientists require deep domain expertise to identify and select appropriate data features – a step that is laborious but vital. Detecting fraud before the victim's money leaves their account requires contextual understanding of time to predict behavior accurately. However, most transactions are intermittent, making contextual understanding of time an equally critical element that creates an overall behavioral profile. ADBN introduces memory cells with native understanding of the significance of time in transaction flows, further improving upon the market-leading performance of Featurespace's Adaptive Behavioral Analytics.

ADBN prevents 73% of fraud while still approving 99.5% of transactions. Its Recurrent Neural Network based architecture works by processing time series data to deliver further improved rates of fraud detection, with up to 38% uplift in model performance. One customer using ADBN improved its fraud benchmark performance by 10 basis points, equivalent to catching 38% more fraud.

*TSYS can help you take advantage of Featurespace's machine learning innovations through TSYS Foresight Score. Speak to your customer success representative to learn more.

Expertise

Technology is only as good as the expertise embedded within it. The most important driver of our ecosystem: TSYS and Featurespace's consultants and technologists. They are imperative to keeping the Foresight Score model growing. They are ones who you consult with to analyze score performance, who analyze model health after monthly model retrains, and govern the model.

Financial institutions are well versed in complex technologies that failed to deliver return on investment. That's why it is so important to choose a technology partner whose expertise they can trust to ensure they achieve their goals.

In fraud prevention, that expertise needs to span the **data science insights** that underpin the platform as well as the strong understanding of the trends, regulation and innovations that impact the market. Partners should bring a team of Subject Matter Experts (SMEs) who can add strategic input to how technology is implemented and deliver on value projections.

Featurespace's award-winning **ARIC™ Risk Hub** includes the research and expertise of its team of data scientists whose models outperform industry benchmarks and do not degrade overtime. Their experience in implementations, processing platforms, integrated data and model explainability and governance is critical in ensuring that the technology that underpins TSYS Foresight Score and TSYS Smart Secure is best-in-class.

Foresight Score

A scoring model with adaptability and stability scaled through machine learning is more important than ever in the fight against fraud. Issuers rely on **Foresight Score** powered by the machine learning ARIC Risk Hub from Featurespace. Because of the speed at which it learns cardholder genuine behavior, it can spot very subtle differences and deem them anomalies. Detecting new and unknown fraud types helps stop fraud in its tracks.

The pandemic emphasized that machine learning for fraud prevention needs to constantly learn and adapt to ensure an accurate scoring model. Transaction and spending patterns changed overnight, and issuers needed to remain confident that fraud scores from their partners could adapt at this pace. In one single month from March 1st to April 1st (2020), total card not present (CNP) transaction volume was 81% higher*. And the total value of those transactions increased 77%. Consumers began subscribing to new delivery services with recurring subscription payments, and even made more impulsive large value purchases such as spin bikes and gym equipment. Legitimate spending habits changed, and fraudsters adapted too.

Advanced machine learning is needed to detect anomalies in cardholder spending patterns with this speed and accuracy. It allows models to spot subtle variances from expected human behavior, allowing it to predict both new and unknown fraud types and elusive changes and existing prototypes. This allows for more dynamic risk and fraud management. Featurespace's invention, Adaptive Behavioral Analytics, along with supervised machine learning, underpin TSYS Foresight Score, and this innovative combination was able to pinpoint rapid changes in good behavior and adapt models to keep pace. Foresight Score leverages the Featurespace machine learning principles of focusing on understanding genuine behavior in order to more accurately identify fraud. This approach builds behavioral profiles based on normal behavior for entities like an individual card, a merchant, a merchant type, or the location of the transaction. And when these entities are built and matured and new transactions come in to compare against those entities, the model is extremely efficient at adapting and identifying anomalies. The model is less concerned about what a cardholder did a week, a month, or a year ago, and prioritizes the cardholder's current activity. Profiles adapt to new behaviors within hours, resulting in fewer false positives and ensuring the digital economy keeps flowing.

TSYS Foresight Score in partnership with Featurespace continually self-learns based on ever-changing data endpoints. The result is that Foresight Score has been shown to achieve up to 15% increase in overall fraud detection and up to a 34% decrease in transactional false positive rates. **Learn more about adaptive fraud prevention in this report**.

Governance

Model governance is the next challenge for financial institutions. Machine learning cannot be a black box. TSYS and Featurespace ensure responsible and appropriate controls and management are in place.

Model governance centers around two processes – an audit of the model before deployment, and the monitoring of the model once it is deployed.

Featurespace has a strict model governance process which focuses on four main questions:

1. Is the model as performant as possible?
2. Can the model's decisions be understood?
3. Is the model as fair as possible?
4. Is the model stable in production?

Our Model Governance Framework was developed with the input of our customers and regulators. The underpinnings of this framework capture Featurespace's Machine Learning Equality Policy and our commitment to producing solutions that enable fair access to financial services products, removing prejudice from behavioral profiling while identifying as much suspicious activity as possible.

While frameworks for off-the-shelf machine learning models for AML transaction monitoring can be standardized across implementations, Featurespace's approach to model governance is more tailored. This means that the model governance varies across each deployment, ensuring that models are validated and tested against each customer's specific data. The result is not only a model best suited to our customers' use case but a governance framework that truly takes our customer's requirements into account while our adaptive models ensure performance is maintained and our explanations ensure investigators have insight as to why a transaction is suspicious.

Featurespace constantly exceeds the expectations of our customers with our models showing "more explainability and transparency than any other platform on the market." **Read the Aite-Novarica report**.

H Hacks

Data breaches compromise your customers' data. Hacks call for an extra line of defense in the fight against fraud. Real-time machine learning must be deployed alongside multi-factor authentication to protect customers in a world where hacks and leaks have made Personal Identifiable Information (PII) easily accessible to criminal networks. Financial institutions are peppered daily by attempts to use stolen information, much of which is available on the dark web in marketplaces that sell pilfered personal data at relatively little cost. Personal details exposed in these incidents are compromised for years.

Fraudsters understand how fraud prevention rules work and how to get around them. For example, hackers know that financial institutions will be on high alert after a well-publicized attack or breach. They know that stolen information will be worth even more in the future, when any red alert subsides.

Overcoming the challenge posed by savvy criminals with vast amounts of compromised data, who also have an intricate understanding of lender operations, is extremely difficult. It requires identifying fraudulent events from genuine ones. Thankfully, AI-driven fraud solutions can recognize an individual's unique behaviors in situational context, protecting customers in a world where these types of attacks will only become increasingly prevalent.

Rules-based approaches are insufficient in managing the aftermath of a data breach or hack. Real-time machine learning which adapts to profile and understand individual consumer behavior over time is essential in combating stolen information and the dark net. Featurespace and TSYS' Foresight Score model quickly analyzes the entire payment journey and accurately predicts individual behavior in real time, understanding risk even as underlying behaviors change. With this self-learning technology, anomalies in customer behavior are rapidly understood, evaluated and acted upon to stop fraud and financial crime. Suspicious transactions are flagged immediately for the bank's fraud prevention teams to act on resolve.

ISO 20022

New industry standards for processing data are enabling more enriched data and unlocking the value of disparate data. This, combined with interpersonalization of data - using both financial and non-financial customer data, is allowing better identification of the cardholder and more effective realization of the relationship between the genuine cardholder and single legitimate transactions, enhancing the customer experience.

Traditional transaction data standards, such as ISO 8583 for card transactions, were limited in the data they could support. This posed challenges for fraud prevention, and necessitated layering in other third party data sources to augment decisions with non-monetary information such as device ID or biometrics. But fraudsters were quick to adapt to these new data sources and began to develop approaches such as SIM swap fraud, or manipulation and impersonation scams to circumvent Two Factor Authentication (2FA) on devices.

ISO 20022 is the new de facto data standard for instant payments, and there is even discussion about how some card schemes and networks might modernize to this new format. ISO 20022 supports richer and more structured data, which can be leveraged in the fight against fraud. With more available data in the transaction itself, fraud prevention can focus on the transaction signals rather than third-party data sources. But analyzing a greater volume and variety of data without impeding the transaction flow requires real-time machine learning.

Featurespace's machine learning and platform have been architected to support real-time transaction monitoring and high volume, low latency event processing. For partners like TSYS, this delivers an average response time of 30 milliseconds, and 3,800 transactions per second (TPS) in real-time processing across multi-tenancy deployments. **Learn more about Featurespace's fraud prevention capabilities for issuers and processors**.

J

Jurisdictions

Globalization makes customer habits and criminal networks international. Compliance with global jurisdictions is essential of course, but more important is to leverage the benefits of a global community of fraud fighters. Macro trends data should be combined into jurisdiction-relevant models to create solid industry defenses.

Global payments are becoming ever more seamless and speedier, with interoperability and international payment acceptance supporting cross-border trade even for small businesses and individual sellers. But as money moves more freely, fraudsters spot an opportunity. Preventing international and 'imported' fraud is essential in a modern ecommerce environment.

Rules-based approaches need to be adaptive at a minimum. But, to really prevent imported fraud from other jurisdictions impacting your customers, either as sellers or buyers, merchants need the benefits of machine learning. But that machine learning must be dynamic and real-time.

Instead of continually retraining models, which takes too much time to keep pace with the fraudsters, cutting edge Adaptive Behavioral Analytics from Featurespace prevent model degradation with self-learning analytics to ensure TSYS Foresight Score is a step ahead. **Learn more about award-winning Adaptive Behavioral Analytics**.

K

Kubernetes

Cloud modernization should overcome the legacy technology silos and restrictions of the past. Faster deployments, upgrades and innovations are crucial in the fight against fraud, and adopting a Software as a Service (SaaS) strategy for cloud adoption can help achieve this. Kubernetes is the key in this need for speed, without increasing risk around technology changes.

There is one key innovation that has made the journey to SaaS possible for financial institutions: Kubernetes. Kubernetes for container orchestration is the technology that creates ease of change and upgrade, for both the FI and the vendor. Change configuration can now be done in the application layer rather than the infrastructure. App-state configuration becomes as easy as adding a seat for a new user.

Kubernetes begins delivering value for financial institutions before they even go-live with SaaS solutions. Traditional on-premise deployments, or products that have been lifted and shifted to the cloud without architectural change, required time-consuming configurations for financial institutions to begin processing. But with containerized workloads made possible in the orchestration environment that Kubernetes can facilitate, interfaces can be tailored precisely to a financial institution's needs, and that configuration can be done at the application layer.

Kubernetes not only delivers on the benefits of SaaS for financial institutions, but they actually create the transformation path. Kubernetes can improve on-premise systems right now, and also facilitate a move to SaaS or own-cloud deployments later on.

In modernizing solutions for the marketplace, TSYS, as a large-volume issuing processor, has certain scale requirements. Working together to bring new Foresight Score models to market, Featurespace has modernized its solutions' cloud environment, rearchitecting to handle the increased processing scale and better support customers in this digital transformation. Learn more about getting in shape for SaaS transformation in financial services **in this article**.

Laundering

Every dollar scammed or defrauded, ultimately has to be washed into the financial system. Tackling fraud means preventing money laundering and funding criminal networks. Featurespace's mission is to make the world a safer place to transact, and that means tackling the fraud and money laundering that drives human trafficking and child exploitation.

Real-time or same-day processing in fraud systems (which tend to operate faster) has been known to be very successful at identifying money mule activity for vulnerable populations, and hence stopping customers from becoming an unwitting accomplice to money laundering. But for many Anti- Money Laundering (AML) teams their data is still processed in batch, rather than real-time. This inhibits AML practitioners' ability to action insights from their fraud teams into their own strategies. There is a growing realization that for certain crimes like terrorist financing, human trafficking or modern slavery, a timely reporting and speedy intervention by relevant authorities can literally save lives.

There are considerable challenges for real-time transaction monitoring in AML, a payment request alone contains insufficient information for financial crime monitoring. To produce a significant risk decision the transaction monitoring needs to be able to look at the whole customer profile to identify any anomalous pattern. For fraud those lookback periods are typically a lot shorter, whereas AML transaction monitoring is all about historical pattern analysis. Evaluating all of that customer intelligence whilst providing a risk evaluation within milliseconds is a technological challenge.

Learn about the Artificial Intelligence innovations for AML that are improving the collaboration between fraud and AML professionals to make the world a safer place to transact. **Read the AI Innovation in AML white paper**.

Machine Learning

Machine learning is the new standard in the fight against fraud, but it must be adaptive to match the speed of change from criminal networks. Featurespace is founded from data science, and we're constantly innovating in machine learning to bring the benefits to payments fraud and financial crime.

When it comes to fraud prevention for issuers and processors, historical concerns around machine learning centered on its ability to match the scale required for transactions per second (TPS). Particularly as digital payment volumes have grown exponentially.

Since 2017, TSYS has processed billions of transactions protected by Foresight Score and powered by Featurespace. **Total volumes exceeded 5 billion transactions in 2021**. Current TPS volumes peak around 1,200 and are expected to almost double in the near future. TSYS protects over 25 million transactions per day with Foresight Score. This is one of the largest scaled machine learning applications in the suite of products at Global Payments.

The data science team at TSYS estimates that in just three months, the transactional equivalent of 0.6% of the US annual Gross Domestic Product (GDP) was processed through Foresight Score training, to generate dozens of custom models. If the Foresight application were a country, it would be the 59th largest country by GDP in the world, placing it just behind Algeria and just ahead of Kuwait. The data associated with Foresight Score is vast. It is the very definition of Big Data machine learning.

"Experience in implementations, processing platforms, integrated data, data science, and model governance is critical and cannot be accomplished with AI and machine learning alone. Issuers look to purchase a solution they can rely on, and they trust TSYS and Featurespace experts who have a track record in successfully deploying and maintaining the advanced adaptive machine learning model."

Read more about IDC's evaluation of TSYS and Featurespace's highly scalable, adaptive machine learning.

N Nuances

Being able to recognize nuances between genuine customer interactions and anomalous activity, in real-time, is only possible through the very best machine learning* and AI-powered technology.

Growing transaction volumes and fraud attempts mean that being accurate in understanding genuine behavior and minimizing false positive flags is crucial to operational efficiency and customer experience. To achieve this, requires highly nuanced machine learning models that can understand what genuine customer behavior looks like, even if it varies over time.

Gaining a nuanced view of risk means the use of predictive behavioral analytics driven by machine learning to scale in line with the volume of transactions and variety of data sources, to make real-time decisions. Featurespace's transformative Automated Deep Behavioral Networks (ADBN) architecture for real-time fraud prevention automatically identifies key features in the data without human input. This provides years' worth of feature extraction in a few weeks, resulting in more accurate anomaly detection and reduced false positives. This new deep learning approach offers exceptional risk detection as well as reduced false positive ratios. Consumers face reduced friction with fewer escalated verifications needed. At the same time, scams, account takeover, card and payment fraud attacks are identified before the victim's money has left their account.

Neural networks are the foundation of machine learning for fraud prevention, and ADBN's Recurrent Neural Network-based architecture improves fraud detection across the board, especially high value – low volume and low value – high volume attacks. **Learn more about ADBN, the next generation of machine learning from Featurespace**.

*TSYS can help you take advantage of Featurespace's machine learning innovations through TSYS Foresight Score. Speak to your customer success representative to learn more.

Orchestration

Solutions with strong orchestration and translation capabilities will be essential, as new, disparate data systems have to be connected into existing legacy products. To access, combine and make better decisions with new data demands strong and real-time orchestration across both payments and non-payments systems.

Many organizations are investigating a combined or holistic fraud and AML approach (FRAML), bringing fraud and AML data into a single place to enhance the value that both teams get from technology investments. But this requires an excellent orchestration layer. Looking at the entire customer journey as a whole allows a financial institution to protect the customer holistically, as opposed to just looking at a single channel each time a questionable transaction is raised.

As Gartner states in its '2020 Market Guide for Online Fraud Detection': "Online fraud detection is expanding beyond traditional use cases, and market overlap with identity proofing and authentication is growing. Security and Risk Management leaders focused on fraud should select vendors based on desired business outcomes and recognize that orchestration has become a critical requirement."

An integrated approach to fighting fraud and money laundering can improve risk management outcomes. Learn more about orchestration technologies, in the article, **"FRAML Payments Guide: How To Deploy A Holistic Risk Hub"**.

P Parallel Scoring

Enabling customers to harness the power of "What If" and explore possible changes in fraud strategy through parallel scoring is a differentiator. TSYS and Featurespace are providing fraud strategists with certainty in decision-making by granting a level of reporting that's invaluable - being able to see the exact performance of the incumbent model versions against the future version at given intervals during model upgrades.

Machine learning must be well understood by the teams deploying it for fraud prevention. They must be confident in the self-learning capabilities of models and the results they deliver for detection and prevention. Parallel scoring and the benchmarking reports it facilitates is one way to build trust. In this way fraud strategists can compare the exact performance of incumbent models against the future versions at different intervals during an upgrade process. Reports should be delivered to them in a timely manner throughout the upgrade process, knowing the thresholds for certain activity between the incumbent version and the future version, adapting fraud strategy accordingly. As well as multiple parallel scoring reports, specific model governance documentation at different intervals and at different levels of detail during the migration process should be available. Reports should include breakdowns at different thresholds, such as spend types or transaction types.

Fraud teams should look for solutions that provide the highest level of parallel scoring and reporting to support their strategies. TSYS and Featurespace regularly use parallel scoring analysis to maintain the stellar performance of Foresight Score as well as to innovate. **Learn more about Foresight Score's performance**.

QR codes

The pandemic spawned new customer behaviors, including strong QR code adoption. Protecting these new payment experiences is crucial as they are often the attack point of focus for fraudsters. Adaptive, real time machine learning is the only way to effectively fight new fraud typologies, and surface previously unknown threats.

QR codes have been commonplace in Asia for some time for payments, but elsewhere in the world they emerged as a response to contact-free experience requirements during the pandemic, often as an integrated menu, ordering and payment experience.

Throughout the buyer's journey, businesses are using QR codes in innovative ways to drive additional sales and improve the customer experience. For example, social media influencers who use video and streaming platforms to demonstrate products are displaying QR codes so viewers can purchase the product with a click. Brands are incorporating QR codes into their non-digital marketing materials, such as print ads and TV commercials, so consumers can easily make a purchase. Finally, retailers are using QR codes on labels to provide discounts, encouraging consumers to make a more immediate purchase.

But new embedded payments experiences create opportunities for new scams: fake QR codes, in-person manipulation scams with AR codes, or embedding malware in a code. Some of these threats can be mitigated with customer education, namely teaching people never to scan a code they don't trust. Additionally, fraud and financial crime solutions need to be ready to protect transactions initiated by dynamic or one-time QR codes. These codes facilitate hybrid ecommerce experiences between online and mobile transactions and help to overcome some of the potential friction in the customer experience in 3DS or Strong Customer Authentication transactions flows.

Adapting to both new payment initiation types and new customer behaviors, as well as spotting new scams requires dynamic and adaptive machine learning. **Learn more about preventing scams with machine learning**.

R Real-time

Traditional machine learning was built from static batch data, but solving for payments fraud requires adaptive, real-time decisions. Real-time decision making across multiple vectors and channels is the only way to protect payments in an increasingly digital world. Featurespace brings real time machine learning to payment fraud prevention, wherever they are on their data science journey, with adaptive supervised, and unsupervised models.

Transactions and digital experiences require real-time responses, even if the underlying payment doesn't clear or settle in real-time. Therefore, fraud prevention solutions must also operate in real-time, making accurate decisions across complex data sets to identify anomalous behavior. Degradation of fixed-data snapshots means that legacy consortium-based models can be as much as a year or more behind the fraud innovation curve. In-fraud prevention models must be flexible, self-learning, real-time solutions that depend on machine learning to continually train and optimize datasets to better identify changing fraud trends and suspicious activities. The solution should be proactive and continuous by nature — rather than being reactive or driven by data from months or even years past — and therefore able to quickly and accurately identify subtle changes in customer behavior. This helps you differentiate between genuine spending and fraud, even when specific behaviors might be considered "unusual" by other models.

Traditional machine learning doesn't operate in real-time, so to achieve this for fraud prevention in payments necessitates several innovations in relation to feature stores, and training and retraining neural networks.

To accelerate model training Featurespace has optimized its neural network architecture and training strategy, accelerating this by a factor of 10 without increasing the number of Graphic Processing Units (GPUs). In this way we can answer many more questions about designing the best possible fraud detection models.

Featurespace's training approach creates deep neural networks that can work with and adapt to transactional data in the real world. We can retrain our models to account for concept drift, so that our models understand not just what fraud means broadly but what it means today. At the same time, our retrains are lightweight enough that they are practical in production. We can retrain without damaging or destroying our historical state, while allowing the stateful information to be updated by the latest events.

Learn more about Featurespace's inventions in real-time machine learning from our data scientists in their insights series, "The Technologists".

Stability

A model with the ability to swiftly adapt to changing underlying transactional behaviors has become ever so more important as evidenced by the rapid swings in payments behavior in the COVID-19 pandemic. Built with adaptability and scale in mind, TSYS Foresight Score with its monthly model retrains continues to protect millions of people from fraud and financial crime.

Without the ability to continuously recognize baseline behavior and adapt to changes, fraud detection platforms become less effective and less efficient, leaving financial institutions in a precarious situation at a critical time. The abruptness and speed with which spending behaviors shifted during the pandemic turned a spotlight on the significance of self-learning technologies and how their intrinsic adaptability works to quickly analyze the entire payment journey, and accurately distinguish fraudulent activity from the behaviors of genuine customers.

The importance of a constant cadence of model upgrades based on response to industry changes and business needs cannot be underestimated. A high performing model reduces operational burden on the fraud analyst team. Foresight Score and its models have been proven to reduce net fraud by 70% and gross fraud by more than 50%.

Foresight Score is the gold standard for model adaptability, providing stability in fraud prevention operations even through rapid swings in consumer behavior. **Read the report, "Ongoing Adaptability in Unpredictable Times"**.

Tokenization

Tokenization is now the de facto standard for data protection and fraud prevention in the industry. Preventing access to the actual card number and enabling instant reissue of just the token ensures our clients are operationally efficient and cardholders have peace of mind.

Card Not Present (CNP) transactions are increasing, both as ecommerce payments as well as contactless or mobile transactions. Because of the nature of CNP fraud, banks and merchants often must act as the customer's backstop. It's their verification procedures that stop unauthorized card payments. Ways to improve those verification procedures, include multi-factor authentication, biometric scans, and digital tokenization. Using tokens instead of sharing PAN or account numbers that can be fraudulently misused if accessed, can improve security and reduce fraud. Verified, secure payment processors will encrypt payment data, tokenize payment data and have several methods of customer authentication processes in place to verify the legitimacy of payments.

PCI compliance is commonplace across the payment ecosystem. PCI tokenization replaces the PAN at one specific point in the transaction flow and renders the data meaningful only to the token provider and the merchant.

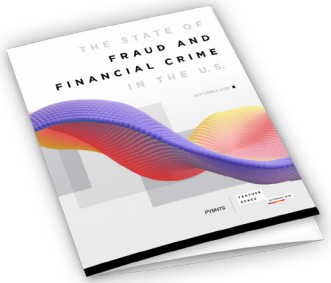
PCI tokenization compliance is embedded into Featurespace and TSYS' platforms to protect CNP transactions.
Learn more about TSYS Tokenization for Issuers.

Unbanked

Driving financial inclusion is important and the unbanked often have to rely on more risky payment alternatives to transact their business. Protecting both alternative and emerging payment types is just as important and is only made possible through the application of intelligent machine learning models.

Around the world, new Peer to Peer (P2P) payments have taken off as a way to bring the previously unbanked (those without access to a bank account or digital payment instrument) into the modern, digital economy. But it's not just developing markets where traditional banking services have left large sections of the population out of digital payments. In the U.K. one of the major drivers of faster payments was providing reliable, predictable payment services for the unbanked: those for whom the existing payment options didn't meet their needs. Direct debits and debit cards were not optimal for those on a tight budget when the date and time of funds clearance was unpredictable.

In the U.S. these same challenges have seen P2P apps like Venmo take off in the previously underbanked sector. But where there is payment innovation, there is innovation from fraudsters. Protecting the most financially vulnerable is crucial when they begin to move into the digital economy. It is no longer 'cheaper' to live your life in cash, and many utility, government and private sector services now require digital payments.



Fraud against these new payment services adopted by the previously unbanked or underbanked concentrated on the weakest link in the chain: the customer. Fraudsters are capitalizing on the unfamiliarity of users with banking, payments and fraud controls to execute manipulation, impersonation and coercion scams. **Authorized payments fraud is on the rise in the U.S., representing more than 50% of all fraudulent transactions in the last 12 months, and requires targeted prevention strategies**.

With accurate and fair machine learning models, financial institutions can be confident that they are providing financial access to more customers, who otherwise may have been excluded – with the confidence that if fraud or financial crime takes place it can still be prevented or identified. **Read more from Dave Excell, Founder of Featurespace, and his mission of 'Tech for Good'**.

V Virtual Cards

Instant is the new normal for today's businesses. Virtual cards fulfill the need for immediate convenience. The move to digital payments is now for companies with master accounts to protect. Fraud prevention is built-in with virtual cards, as payments are made with no account numbers revealed.

Businesses around the world have recognized the need to transition from paper-based processes and payments to a seamless, digital connection of all the steps in the cash cycle, from procurement to reconciliation. Virtual payment instruments can be instantly issued, accelerating the shift from paper to digital without the need to wait for plastic in the post.

Virtual cards, a digital credit card with a randomly generated 16-digit number designed for one-time use and only authorized for a specific dollar amount, can help organizations better manage cash flow and employee spend. It can, as well, minimize overall risk on transactions made by employees that may be subject to fraud. Virtual cards are single use. Even if fraudsters successfully infiltrate one transaction, they can't spend with the virtual card beyond that one-time use.

In the consumer space, digital wallets are on the rise:

- An estimated 4.4 billion global consumers will shop with a digital wallet by 2023, accounting for 52% of ecommerce payments globally.
- 1.6 billion global consumers will pay by digital wallets at the point of sale (POS) in 2023, accounting for 30% of POS payments.

*Global Payments 2022 Commerce and Payment Trends Report

Virtual cards can be instantly issued into digital wallets, particularly in cases of confirmed Account Takeover (ATO) or lost cards that could be misused, to block the compromised card and ensure customers can continue to transact safely.

Virtual cards are an essential tool in the customer experience and fraud prevention strategy. **Read more about virtual cards and other trends shaping the future of commerce in: Global Payments "2022 Commerce and Payment Trends Report"**.

W-2 phishing/BEC

Scammers target businesses too. Business Email Compromise fraud is a huge risk in an increasingly digital and remote workplace. Protecting business customers from scams necessitates adaptive behavioral profiling combined with other controls to protect employers and employees. Featurespace's Adaptive Behavioral Analytics continuously profiles genuine behavior to better spot when payers act out of character, stopping scams in their tracks.

Fraudsters are collaborative on the darknet, sharing their 'best practice' scams and increasingly targeting these against individuals, both in their personal and professional lives. Focusing on individuals in their work environment: phishing techniques, one type of social engineering that exploit both human error and email communications in organizations to gain sensitive financial data or log-in credentials. A W-2 phishing attack by email or messaging service, or Business Email Compromise (BEC) scam, impersonates senior management at the organization and applies time pressure to manipulate more junior employees into either making transactions, sending sensitive information that allows the criminals to commit financial fraud themselves through ATO, or to sell the sensitive data on the black market to other criminal organizations for that purpose.

The scam transactions or stolen data can be made or used instantly, usually before cyber security and risk teams have identified the breach, so fraud prevention systems at the financial institutions serving these organizations must be able to identify transactional behavior that is unusual for the organization and stop both authorized and unauthorized payments fraud from occurring.

Featurespace's deep learning invention, Automated Deep Behavioral Networks (ADBN) power the ARIC Risk Hub so that it can help businesses spot account takeovers, man-in-the-middle attacks, APP fraud and all of the other payment scams initiated through social engineering. **Read more about ADBN and preventing payment fraud**.

X-border

Scams know no borders, so fraud prevention teams must be globally savvy to stay ahead of international criminal networks. Working with a global partner like Featurespace, banks and financial institutions gained the benefit of global experience combined with local details. This expertise is built into Featurespace machine learning models, to ensure your business is prepared as new fraud threats arrive in your markets.

Consumers have never had more choice, with global ecommerce platforms making goods and services accessible to international audiences. The proliferation of cross-border purchasing and transactions poses challenges for financial institutions. Protecting customers requires local expertise in fraud trends and scam techniques, combined with a global network to understand how these trends migrate to new markets.

Even for financial institutions operating in a single home market, the reality is their customers now transact across borders and, as such, are vulnerable to global fraud trends. Fraud prevention machine learning models should be tailored to local markets based on in-person expertise, but with self-learning capabilities to adapt as global trends infiltrate local markets.

Featurespace and TSYS partner to ensure the local details on payment and fraud trends are integrated into our award-winning models, that continuously self-learn to ensure financial institutions in any market continue to outsmart risk. **Learn more about how adaptive modeling meets fraud head-on: "IDC Vendor Spotlight Report".**

Young People

Understanding genuine customer behavior means understanding each generation through the use of personas, be it Gen Y or Gen Z. Giving our clients the means to apply customer journeys and experiences tailored and valued by each generation will help them turn their young cardholders into customers for life.

New generations of customers bring new preferences and habits that must also be protected. Younger shoppers appreciate the flexibility of BNPL, with 44% of Gen Z and 37% of millennials expected to make a BNPL payment in 2022, compared to 23% of Gen X and 9.4% of baby boomers.

In addition, many younger shoppers may not have the income or credit history required to leverage credit cards, as 30% of millennials say they live paycheck to paycheck, compared to 15% of older shoppers. These consumers appreciate the simplicity and predictability of BNPL. BNPL allows these shoppers to be more strategic about their spending to avoid debt. *Global Payments 2022 Commerce and Payment Trends Report

But a variety of fraud types are emerging from the growth of buy now pay later (BNPL). For most BNPL providers, customers need to create accounts, which opens the door to account takeover fraud. Further, there is a type of return fraud that's common in BNPL, usually after the first payment installment gets billed to the customer's account, and buyer's remorse sets in.

Both those serving Gen Z customers and BNPL providers need fraud prevention solutions that can combat ATO and first party fraud, by truly understanding the genuine behavior of their customers to quickly identify when fraudsters or they themselves act out of character.

Learn more about rising fraud trends and how to combat them with a holistic approach in ARIC Risk Hub: "What is ecommerce Fraud".

Z

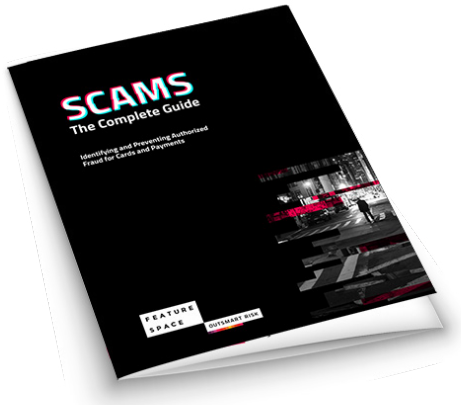
Zombie Bots

A zombie bot is a malicious bot that makes it possible for hackers to remotely control devices. Zombie bots are a key ingredient in creating a botnet and driving large-scale cyberattacks, a growing challenge for fraud prevention teams.

Often created through social engineering or phishing attacks, they can be used to enable data breaches at financial institutions. And there is a trend of zombie armies being used to create fraudulent applications for credit, insurance, buy-now-pay-later schemes, and merchant accounts on a massive scale. The economy of scale that zombies create for cyber criminals, means even more scalable solutions are needed for fraud prevention to combat the next level of threats.

And scalable solutions must be able to understand the difference between a zombie, a human, and bad actors. Genuine credit applicants or business transactions must be accurately differentiated from human fraudsters, and bot scams. It is not an acceptable customer experience to generate high numbers of false positives that impede genuine customers from making genuine transactions, but neither can fraudsters and zombies slip through the net. Balancing fraud prevention with customer experience is the biggest challenge for today's financial institutions.

Featurespace's machine learning can ingest and generate real time decisions across large and varied data sets and is specifically designed to understand genuine customer behavior to more accurately identify bad actors and bots without increasing false positive ratios. Learn more about combating phishing attacks in **Scams: The Complete Guide**.



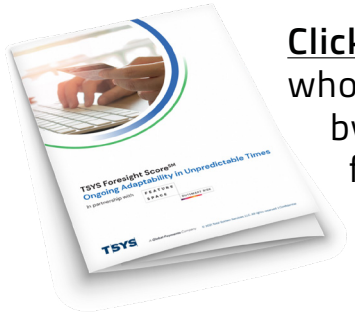
Combating fast-evolving fraud threats requires partners who bring innovations, expertise, scale and agility to the fight. Together, Featurespace and TSYS are working to make the world a safer place to transact for our customers and yours.

FEATURE SPACE

OUTSMART RISK

TSYS

A Global Payments Company



Click here to learn how TSYS customers who used the TSYS Foresight, powered by Featurespace, score saw a net fraud reduction of 70%, even during the pandemic.

For more insights on how TSYS and Featurespace can protect your customers, visit TSYS.com.

FEATURE SPACE

OUTSMART RISK

TSYS

A Global Payments Company