Payments opposing requirements: Security and Consumer Satisfaction

Fraud is prevalent in every aspect of our lives, especially when it comes to when we pay for things. It is a consistent battle for technology to keep advancing, but recently we have seen enormous strides in fraud prevention with the use of high-performance analytics, machine learning and artificial intelligence. We spoke to Dave Excell, Founder at Featurespace, and our own Bruce Diesel, Global Head of Product for Vynamic® Payments, about how fraud management plays a significant role in defining the payment experience.

Dave Excell
Founder, Featurespace

Bruce Diesel
Global Head of Product
Vynamic® Payments, Diebold Nixdorf

Open data exchange through APIs fulfils customer demands for more choice and seamless user experience, enabling fintechs, third-party service providers and neobanks to greatly expand and offer tailored products. With consumers adopting digital banking as a more convenient way to manage finances, criminals are seeing this as a perfect opportunity to engage in criminal activities to hide illicit transactions within the enormous transaction volumes occurring globally every day. Access through a single portal or app also expands the perimeter for criminals to infiltrate the weakest link to exploit the whole payment ecosystem and for incorrect or fraudulent data to be shared. Legacy banking fraud detection systems are not enough to effectively manage fraud risks in this new environment. Fraud detection and prevention systems will need to employ artificial intelligence (AI), most notably machine learning to assist with large amounts of transactions. This will help cut down on false-positive errors and allow flagging fraudulent activity in real-time across all banking channels, whether digital or not.	**HOW IS INCREASED DATA SHARING WITHIN BANKS AND FINANCIAL INSTITUTIONS AFFECTING THE PAYMENTS SPACE?**	Open banking has had two significant effects: it has created more payment access points for consumers, and it has reduced the time to authorize payments. Many markets are bringing instant payments to their consumers. Both benefits are creating more challenges for fraud management systems – more attack surface area, and less time to respond, at greater volume. Legacy rule-based fraud management systems are no longer fit for this purpose, with both false negatives and false positives being detrimental to FI's. AI and machine learning are now the most appropriate techniques to handle the velocity and volume of modern transaction processing. However, AI and ML are not simple techniques, and the skill of the organization implementing these tools is a critical success factor. Choose wisely!
FIs that utilize data and indicators across multiple frameworks to understand when a customer's spending behavior is out of character is key to fighting fraud. This will enable FIs to alert customers, improve awareness and to effectively trigger in-session risked based warning messages when a victim is at risk of being scammed. Furthermore, by consistently labeling and categorizing confirmed scam cases, fraud teams will be able to deliver robust, targeted strategies to resolve distinct types of scams.	**BETTER CONTROLS AND NEW REGULATIONS HAVE BEEN DESIGNED TO IMPROVE AUTHENTICATION, YET SCAMS ARE SKYROCKETING. HOW CAN FIS IDENTIFY AND PROTECT AGAINST THIS WHEN CONSUMERS SELF-TRANSACT?**	Unfortunately, as security and fraud detection become more hi-tech, scams often prosper from low-tech strategies. Consumer education is critical but cannot be fear-based as this will be detrimental to overall acceptance. Recognizing changes in behavior, and alerting consumers to potential scams will empower consumers to take the right actions, but again, false positives are also detrimental as they affect consumer confidence.
It is important to remember that most transactions on any one day are not fraud attempts but legitimate customer actions. However, sometimes genuine activity can sometimes appear suspicious. To detect bad actors, some organisations often create undue friction through security step-ups to ensure they are legit. Leveraging machine learning technology to create a holistic customer view is key to accurately identifying anomalous behavior indicative of fraud or financial crime. It's only when genuine customer behavior is understood that bad actors can be spotted in real-time without causing unnecessary friction.	**WHERE IS THE BALANCE BETWEEN CUSTOMER EXPERIENCE AND CUSTOMER PROTECTION?**	The balance is the point at which the protection is visible to the consumer but does not add friction to the experience. Visibility provides the consumer with confidence that they are protected while friction increases frustration, especially as electronic transactions become smaller and more frequent. Unfortunately, this is unique to each consumer, so the ultimate destination is where we have individual behavior patterns and preferences. This requires a combination of automation (AI and ML) and engagement, i.e., enabling consumers to give feedback on their experience.
Innovative technologies have the potential to make anti-money laundering (AML) and fraud prevention faster, cheaper, and more effective. The substantial increase in availability and granularity of data, and new infrastructure, such as cloud and app interfaces, allow large data sets to be collected, stored, and analyzed more efficiently. Real-time machine learning technology with clear model explainability and reason codes enhance risk management capabilities. The efficiency and accuracy gains, arising from automation of previously manual processes facilitate the generation of new insights for improved decision making and compliance with risk teams able to invest their time better analyzing the results and collaborating the findings.	**WHAT IMPLICATION DO NEW TECHNICS HAVE ON COMPLIANCE AND REGULATORY MANDATES?**	Regulatory compliance seeks to limit access to personal information, which is contrary to the requirements of systems that collect data to be able to analyze behavior patterns. Since AI models are mathematically one-way, they cannot be used to derive personal data about consumers. However, consumers don't know this, and often suspect personal data can be leaked from such systems. Regulations can set the consumer's mind at ease. Another important aspect is in the space of liability. Financial decisions are made based on the outcomes of these tools. When the model parameters used to evaluate risk change rapidly, where does the liability reside when those decisions lead to loss.
High performing, more accurate and adaptive fraud and financial crime analytics allow issuers, acquirers, and networks to optimize their own risk profile confidence, onboard a wider range of customers to be more inclusive, and to offer competitive pricing while protecting margins. Best-in-class detection enables them to productize their investments and package them into value-added services. Partnering with best-in-class partners for fraud and financial crime prevention gets new players back to focusing on their business model while having the value of enhanced protection and analytics.	**HOW CAN FIs USE THEIR FRAUD STRATEGY AS A KEY DIFFERENTIATOR?**	FI's focus on trust and convenience. Fraud systems contribute to both issues. Visibility of fraud management leads to improved trust, while reducing false positives and being unintrusive improves convenience. FI's fraud strategy therefore needs to strike that balance between being more visible while being less intrusive. By integrating leading-edge fraud tools so that they operate seamlessly within the payments' ecosystem, such as the combination of Vynamic Payments with Featurespace, a solution can be provided that is easy to maintain, visible to consumers, and frictionless.

KEY TAKE AWAY:

Fraud management is a critical part of the payments' ecosystem. When determining how to properly protect consumers throughout the payment's experience, FIs need to think about their customer base's level of acceptance as well as its implication on regulation and compliance. As technology advances, consumers expect less friction and greater security, yet it's a delicate balance between the two. Utilizing data and machine learning to know the consumer and accurately reduce fraud is key to building trust and to building a distinctive differentiator. To learn more about Fraud Prevention, listen to this podcast with David, Bruce and Marco Salazar, analyst from the Mercator Advisory Group.