2020 | WHITEPAPER

wibmo

Why Real-Time Fraud Detection is the Pillar of Digital Payments Globally

TRIDENT FRM™

www.wibmo.com

Digital fraud is an ever-present and rising concern in a world of digital payments and online transacting. The customer, today, is at the heart of ecommerce. Everything about the digital space is designed with the customer in mind. Products, services, transaction devices, payment methods and processes, etc., are all designed to give the end user the best possible digital experience.

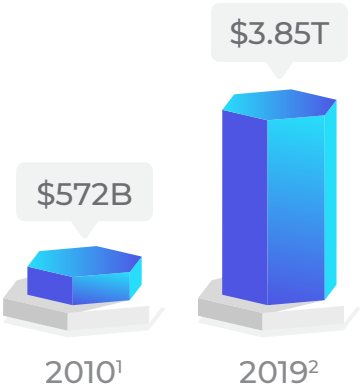
Over time, customer behavior has drastically evolved and seems to be in a state of constant change. Customer loyalties now lie with brands that offer the best experience in terms of convenience, speed, and security. But, as end users explore the myriad benefits of global ecommerce, digital fraud is keeping pace as well. The vast number of user devices, transaction channels, and payment methods create more avenues for malpractice, making digital payments hard to defend. This makes fraud detection and prevention a core requirement for every issuer. Balancing optimal security against modern fraudulent practices with seamless online purchasing journey is a challenge issuers face in this on-the-go generation.

This is where risk engines make all the difference. They help brace this challenge and overcome it. They literally are the pillars on which digital payments are made today. This white paper deep dives into the modern-day risk of fraud and the risk engines that help fight it. It talks about:

- The proportional growth of digital transactions and fraud
- What drives digital fraud?
- Inefficient fraud detection solutions
- Characteristics of a strong fraud mitigation solution

The Proportional Growth of Digital Transactions and Fraud

The trend over the past two decades show that fraud rates have increased along with the increase in the number of online transactions. The value of online purchases has boomed over the years.
In 2010, the value of online sales globally was $572 billion[1].
In 2019, the total value of global ecommerce was almost $3.85 trillion[2].

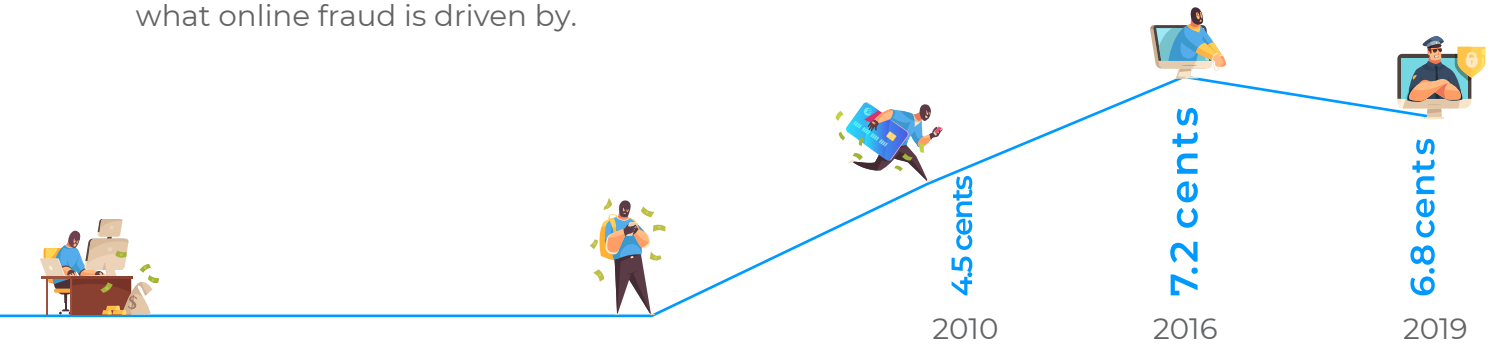


The boom in digital transactions can be attributed to two factors:

- Consumers moving from a hard cash to digital platform as more and more products and services are made available online.
- The feasibility of using multiple devices such as mobiles for on-the-go purchasing.

As of 2019, about 65% of millennials have used a mobile phone to make online purchases[4]. They prefer the convenience enjoyed by going digital. As customer behavior and transacting preferences changed, so did fraud. It is estimated that by the end of 2020, more than a million transactions will happen online every minute. Although, this number may seem a bit out of reach given the current pandemic that has crippled global economy.

At the same time, the value of fraud per $100 of card sales was 4.5 cents in 2010. At the beginning of 2019, this amount was 6.8 cents[3]. Although data shows that online fraud is on a slow decline after it peaked to 7.2 cents in 2016, it is a definite problem that issuers are trying to solve, one that cannot be entirely weeded out.
To understand this, one should first look at what online fraud is driven by.

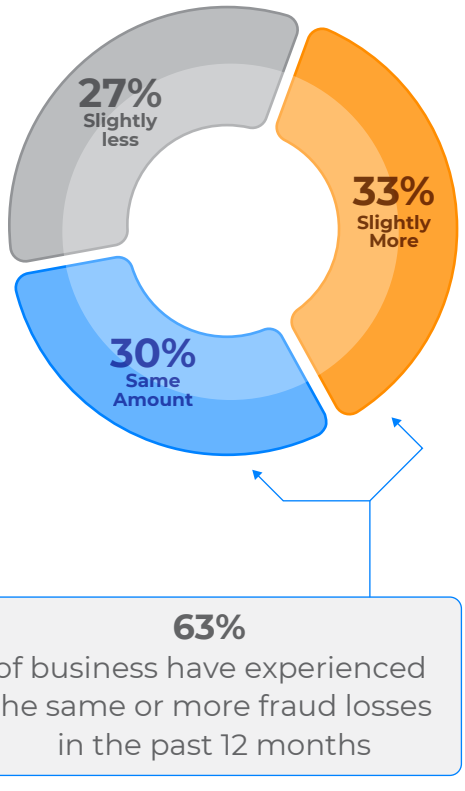


What Drives Digital Fraud?

All through history, fraud has been a part of the payments industry. But this was significantly less due to restrictions in worldwide connectivity, legal requirements, and government regulations for participants. Now that various new payment methods and systems have come into play, global regulations have also changed. Customer behavior and payments patterns now determine how digital payments need to continuously evolve.

As newer digital platforms emerge, it becomes easier for fraudsters to hijack transactions since there are various touch points in the transaction journey. According to Forrester, as of 2019, 55% of merchants surveyed said that payment fraud was the top concern they were dealing with. As the number of payments being made digitally on-the-go rises every year, it becomes critical to detect and prevent fraud in real-time.

In 2018, 63% of businesses reported experiencing the same level or more of fraud losses during a twelve-month period when compared to the previous twelve months. 27% of consumers said they abandoned a digital transaction because there was no form of visible security[5].
Fraud prevention has taken centre stage as fraudsters find new ways of hiding and hijacking online transactions. For example, in Europe's adoption of the PDS2 (Payment Services Directive 2) initiatives, handling fraud in real-time has been given 85% criticality when complying with SCA (Strong Customer Authentication) requirements[6].



Modern online payments depend on the exchange of customer data between the transacting parties. Now how hard would it be for fraudsters to hack into the process and steal this data? The democratization of data poses the potential danger of information leaking out.

As fraudsters become more and more adept at making their illicit activities look genuine, the fraud landscape is constantly evolving. The use of sophisticated tools makes it a lot easier for a transaction to be beset by fraud today. The usage of mobile phones, wearables, digital wallets, and more to make online purchases makes the system highly vulnerable.
As ecommerce transactions started booming around the start of the century, many solutions were deployed to try and prevent this from happening. But their efforts seemingly had little effect.

Why Traditional Fraud Detection Efforts Failed

Inability to handle huge transaction volumes: The number of digital purchases made per day was and is staggering, often in the hundreds of thousands. Many solutions were not able to handle them and detect fraud in real-time due to the sheer volume of transactions. Scaling up the framework was a challenge many service providers faced.
Not able to utilize a variety of data properly: Today's fraud detection solutions need as much customer data as possible to provide accurate detections. Not being able to draw on and analyze multiple data sources at the same time led to sub-optimal decisions being made.
Not being able to distinguish accurately: A risk engine is supposed to distinguish between a genuine transaction and a fraudulent one with a high degree of accuracy. Many fraud detection solutions were not able to do this, leading to heavy business losses and bad customer experiences.
Inability to support multiple devices: Traditional risk analysis solutions were not able to provide necessary for mobile transactions. As customers started using mobiles more, fraudsters started targeting them since the mobile security protocols were not robust enough.

These limitations and inefficiencies are what led to the development of modern-day risk engines, updated and upgraded to handle fraud at the most complex levels.

Characteristics of Modern-Day Fraud and Risk Analysis Engines

Present-day solutions are built to support digital transactions on any device, anywhere in the world. They offer real-time risk analysis to enable business decisions to be made in an instant. They incorporate optimum-level security but do not compromise on customer experience.
Customer-based analysis: The customer is the central focus of each payment. Every transaction is analyzed on the basis of customer data gathered from multiple sources and channels. The engine has thorough visibility of the entire transaction process. Customer behavior is studied in-depth to help distinguish it from fraud patterns.
The power of analytics: Data analytics is the backbone of the risk engine today. At lightning speed, it calculates the measure of risk involved in a transaction with near-perfect accuracy. This helps the engine decide whether to approve or reject a payment in real-time.
Decisions based on risk appetite: The solution can be customized according to the risk appetite of the issuer. This helps in making the right business decisions according to the issuer's risk priorities and tolerance.
Seamless customer experience: The solution is designed to help offer a smooth, frictionless experience to every customer making digital payments. With minimal customer interaction, valid payments are approved, and transactions are completed in seconds.

Our Solution: TRIDENT FRM™ – Multi-Channel Data-Based Fraud Detection and Prevention In Real Time

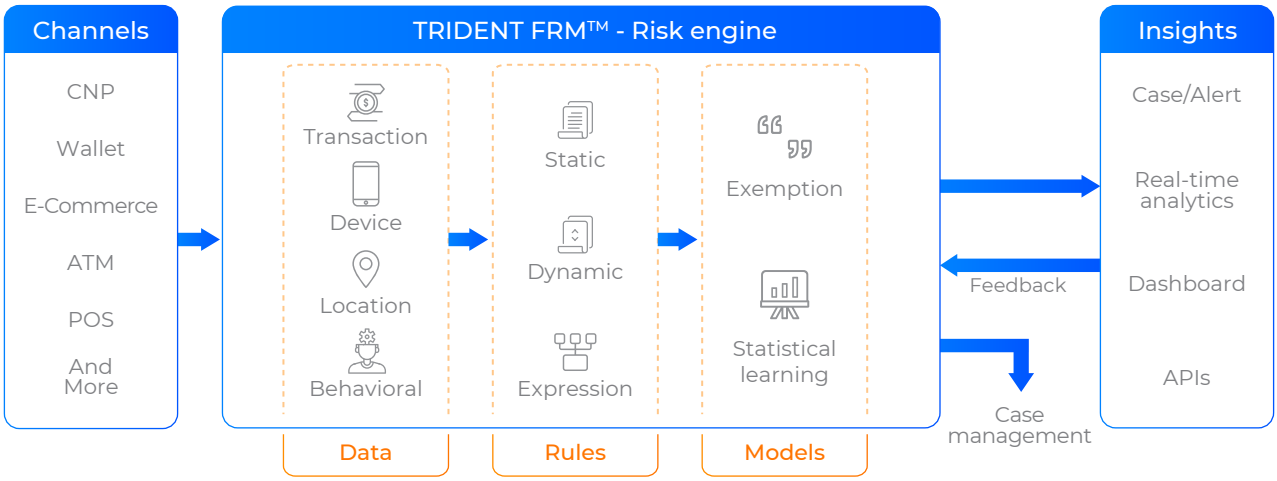
TRIDENT FRM™ is Wibmo's comprehensive risk assessment and fraud detection and prevention engine that identifies fraud in real time. It functions based on the customer data it receives from multiple channels and devices. When a customer makes a digital transaction, the risk engine evaluates it against every possible data point and assigns it a risk score. This makes it possible to offer optimal security irrespective of the device being used in the transaction.

TRIDENT FRM™ is a self-learning system. As fraud patterns and customer behaviors evolve, it studies, learns, and adapts itself to offer accurate risk scores. Based on the assigned score, the transaction is either recommended for approval, rejection, or further authentication via stepped-up options. The engine enables issuers to offer optimized transaction security to customers while ensuring an enhanced payment experience through minimal interaction.

Key Features of TRIDENT FRM™

- Comprehensive risk assessment based on multiple data sources – internal and external
- Real-time risk score generation
- Pre-defined rules to enable instant transaction scoring for both payment and non-payment transactions
- Risk-profile-based recommendation engine to minimize manual intervention
- Rich back-end graphical UI to configure dynamic rules
- Holistic view of the consumer built from diverse data points
- Feedback model from transaction and fraud patterns

How TRIDENT FRMTM Works



Conclusion

As transaction volumes are set to grow in double digits year on year, and as customers expect to transact from anywhere using multiple devices, the threat of increased online fraud becomes more real. Customers want speed and convenience with more security than ever before, especially since they determine the growth of global ecommerce. It is evident that customer loyalties lie with brands that given them the most optimized services and experiences. Hence, it becomes absolutely imperative for issuers to be integrated with robust fraud detection and prevention risk engines.

TRIDENT FRM™ empowers issuers to stay ahead of fraudsters, effectively defending digital payments in real-time and helping reduce the losses that arise out of such malpractices. It is designed to help customers have a seamless and frictionless experience, which is critical in today's world.

Wibmo, with over two decades of experience in the digital payments industry, partners with multiple global banks, offering Risk Engine for Fraud and Risk Management, ACS, 3DS, and other payment solutions.

To know more about how you can help your customers combat digital fraud, please visit **https://www.wibmo.co/trident-frm/** or send an email to **sales@wibmo.com**

Sources:

[1] Red Stag Fulfilment – The 2010s: A Decade of ECommerce Growth

[2] Statista – eCommerce (worldwide)

[3] Statista – Fraud losses per 100 U.S. dollars of total card sales worldwide from 2010 to 2027

[4] Ikjao – How Millennials Are Reshaping The Digital Payments Landscape

[5] Experian – The 2018 Global Fraud and Identity Report

[6] Capgemeni Financial Services Analysis, 2019