JANUARY 2023

DATA POLICY IMPACTS - FRAUD PREVENTION

CASE EXAMPLES

INSTITUTE OF INTERNATIONAL FINANCE

Foreword

National restrictions on the flow of data continue to proliferate around the globe. We are rapidly reaching an inflection point where data localization requirements and fragmented standards for data and privacy may begin to break the on-demand services and real-time systems that we have come to expect and rely on.

While recent years have revealed some serious problems with privacy, security, monetization and taxation in the digital economy; the policy responses have been rapid, fragmented, and poorly coordinated at the international level. Data localization measures, a lack of coordination of data governance requirements, hastily drafted privacy laws, digital identity efforts without interoperability standards, far-reaching AI regulation, and an overall lack of coordination threaten to choke the future of the digital economy.

This is an increasing problem for broad-based sectors including dynamic startups, small and medium sized enterprises (SMEs) and other high-growth businesses which are driven by global digital infrastructure to support their activities. Restrictive data frameworks have real world costs to the businesses and consumers and the full impact of localization requirements and other restrictions are not always measured and frequently not part of the political debate.

This IIF staff paper is part of a series seeking to identify the broad-based impacts of restrictive data policies. The series began with Data Localization: Costs, Tradeoffs, and Impacts Across the Economy (December 22, 2020) which outlined the ways restrictive data policies had proliferated beyond clear data localization laws as well as how the costs and inefficiencies driven by these policies emanated broadly across the economy. It continued with Strategic Framework for Digital Economic Cooperation - State of Play (October 11, 2021) which highlighted the lack of clear international "rules of the road" for the digital economy, challenges to clear global standards, and the headwinds against initiatives such as the G20 "Data Free Flow With Trust". The next piece, Strategic Framework for Digital Economic Cooperation - A Path for Progress (April 19, 2022) outlined what is at stake for the financial services industry, where opportunities for improved data frameworks are possible, and a modular approach for more international improvements—including trade agreements between likeminded markets and industry driven standards.

This series is continuing with the addition of three case examples sharing tangible impacts and real-world trade-offs in fraud prevention, travel insurance, AML-KYC, compliance, and operations. Exploring the impacts of data policy in these areas comes as the G7 appears poised to revisit the importance of data flows against a backdrop of continued proliferation of restrictive policy. We hope that they will trigger further reflection on the possible costs and potential for better solutions.

Table of Contents

Summary

This case example explores why the free flow of data across borders is important to enable effective and efficient fraud detection and prevention. It also shares the real-world impacts for micro, small and medium enterprises (MSMEs) as an example of the broad-based costs from restrictive data frameworks.

Participants in the economy require safe and secure transaction mechanisms to grow their customer base and revenue. Fraud prevention is an essential component of a robust financial services ecosystem and necessary for a positive customer experience. In 2020, payments fraud loss totalled $28.58bn and is projected to grow to $49.32bn by 2030. To fight this trend and maintain accurate and effective fraud prevention systems, data sets need to be broad – the more data, the more effective the model is at detecting fraud.

Speed also matters. Timely and secure processing of sales transactions relies on payment fraud prevention mechanisms that can keep pace. Inefficient fraud detection mechanisms will not only impede sales if validation checks are delayed or incorrectly blocked but will also result in losses if fraud is not detected and prevented. Studies have found that milliseconds matter as consumers will abandon transactions that are delayed. Micro, small and medium enterprises (MSMEs) are more at risk given their reliance on third parties and payment providers to help them mitigate the risks.

Payment fraud is increasing in sophistication and complexity and occurs across borders. Therefore, cross-border sharing of fraud data is essential to ensure effective and efficient fraud detection. Data restrictions not only limit the effectiveness of fraud detection, but also introduce payment system friction. As the policy world pushes for faster and cheaper payments, ensuring that fraud prevention can keep pace is an important element for success.

I. Background and Introduction

The need for fraud prevention and the value of fraud detection

Over the next 10 years, card industry losses to fraud could collectively amount to ***408.50 billion***

Digitization of commerce, including digital payment mechanisms and online marketplaces, has brought enormous benefits to businesses and consumers; unfortunately, rapid growth in digital commerce has also brought about an increase in the numbers and sophistication of criminal activities. Trust and confidence in the payment ecosystem is vital for business and consumers, therefore effective fraud detection and prevention will remain critical to ensure businesses and consumers are able to transact with confidence. Digital transformation is also part of the solution. Advanced new systems, and data flows to for their operation, can keep pace and prevent fraud.

Visa Advanced Authorization ***prevented $27 billion in fraud during 2022*** *and screened 30% more transactions than in 2020*

Fraud detection is important across all transaction types but a consumer shift toward card-not-present (CNP) transactions has highlighted the issues. Nilson Report, December 2021, illustrated the increase in card-not present (CNP) sales in 2020 owing to Covid-19 and how it contributed to the ongoing trend of merchants incurring steadily higher fraud losses. CNP card sales reached 19% in 2020 of total card sales, up from 15% in 2019. Nilson Report states that merchants continued the practice of manually reviewing questionable CNP sales, particularly as the average value of those purchases grew throughout the year. This added to their expenses. And criminals scored successes in using stolen card credentials to execute CNP sales to gain merchandise they could subsequently sell online.

Making fraud detection systems less efficient impacts all sectors of the economy including MSME's

Digital commerce enables many micro, small and medium enterprises (MSMEs) to reach larger audiences and offer customers greater choice; however, MSMEs likely lack specialized skills and resources to combat the increased exposure to fraudulent activity which digital expansion can bring. Reliance is placed on global payment networks which can deliver the benefit of advance fraud analysis using global data sets, to combat fraudsters, other malicious actors and even sophisticated nation states who do no respect sovereignty or borders.

COVID and the shift on-line may have enabled increased fraud attacks on MSMEs, but it also accelerated digital transformation and deployment of new systems and solutions to help business combat the threat.

*One global network observed a **14%** increase in fraud rates pre vs. during COVID-19 for MSMEs*

Inefficient fraud detection and prevention systems have negative impacts on business:

Negative impacts	Implications and cost of inefficient fraud detection and prevention
Direct financial loss	• Charge back losses resulting from fraudulent transactions. • Additional administration cost. • Increased transaction cost from banks and payment providers, mostly via higher interchange fees.
Customer frustration	• Delays in transaction approvals resulting in customer frustration.
Loss of sales	• Lost sales due to false positive declines. • Lost sales due to customer frustration and abandonment of slow online transactions.

Speed matters

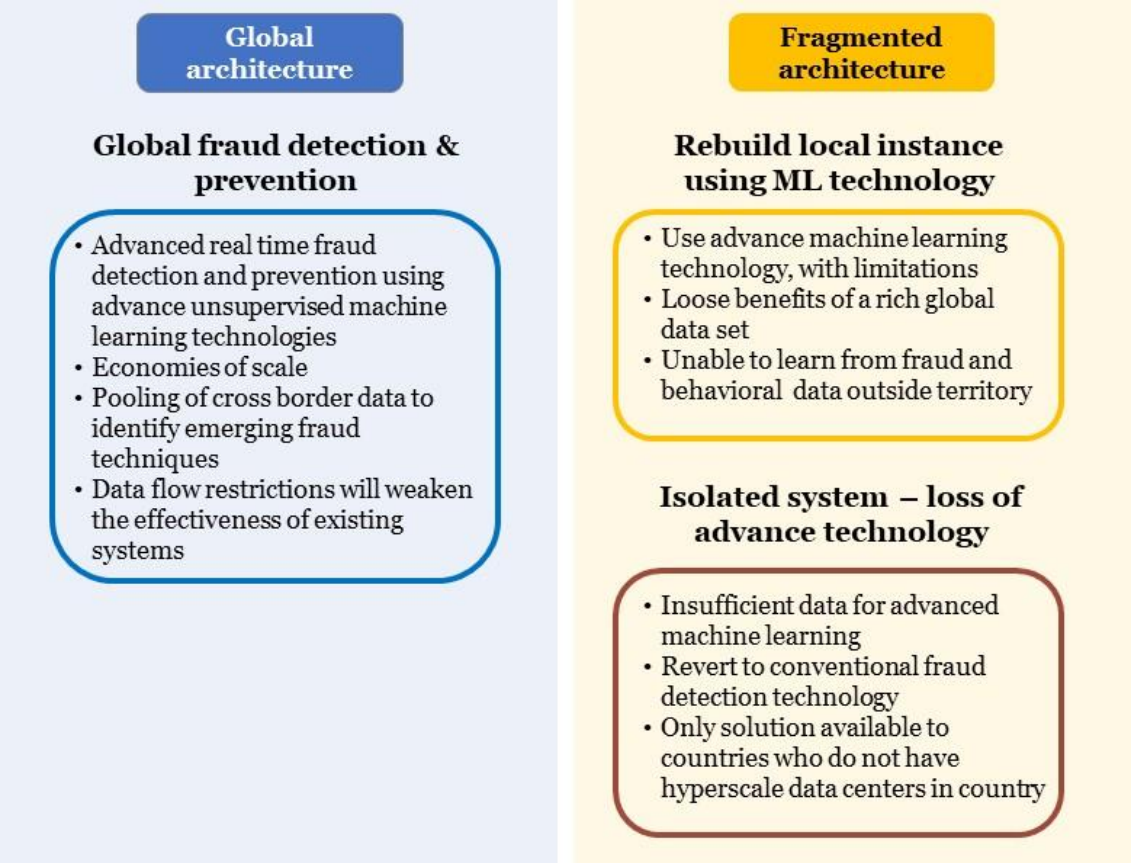
The speed of fraud detection and transaction approval also matters. When fraud data is mandated to stay inside national borders and be separated from global fraud detection data pools, it will result in slowing of fraud detection and transaction approval services, mostly due to additional verification steps. Google, in 2016, found that 53 percent of smartphone users would leave a site that takes longer than three seconds to load, and that time has likely shortened in recent years. A 2020 study by Deloitte Ireland "Milliseconds Make Millions" showed that a mere 0.1s change in mobile page load time can influence every step of the user journey. Consumers are more likely to abandon online sales when transaction approvals are delayed. Therefore, speed of fraud detection and transaction approval is an important factor to prevent abandonment of sales for MSME's.

II. Payment Fraud is a Global Problem

Data fragmentation hampers fraud detection

Fragmentation of the data sets used in existing platforms or imposing restrictions on data flows, could weaken the effectiveness of existing fraud detection and prevention systems. Furthermore, a hard-line data localization approach could require that new localized fraud detection instances be developed with limitations in fraud detection capabilities, or in a worst-case scenario, a territory will have to revert to conventional fraud detection mechanisms which will not be adequate to combat sophisticated fraud.

Global systems vs. fragmented and localized systems



This cross-border challenge was amplified by COVID-19

The Covid-19 pandemic accelerated the adoption of digital commerce with an increase utilisation of credit and debit cards and other electronic payment mechanisms for online purchases. This results in a large increase in Card-not-present (CNP) fraudulent transactions where the customer does not physically present the card to the merchant during the fraudulent transaction. Criminal activities are not confined to conventional borders, for example during 2021 in South Africa, the majority of Card-not-present CNP fraudulent transactions occurred outside the borders of where the cards were issued, as illustrated below. Similar fraud trends exist in other markets.

CNP fraud losses are frequently the responsibility of the merchant and their acquirers, and they were hit hard in 2020 during the COVID-19 pandemic lockdown, as issuers were unprepared for the big increase in CNP transactions. Dollars lost to CNP fraud losses were more than six times higher in 2020 than the prior year.

Cross-border data underpins AI fraud detection

Payment fraud detection and prevention technologies have undergone significant change over the past decade, evolving from conventional fraud detection practices such as black lists, device fingerprints and rules engines, towards much more advanced machine learning based systems. Appendix A details these changes and the benefits.

This shift towards Artificial Intelligence (AI) and Machine Learning (ML) algorithms in fraud detection systems has driven dramatic improvements in fraud prevention. It has also increased the impact of data policy on these solutions. Machine Learning requires historical data to train an AI algorithm. Once deployed, using what it learned from historical data, the algorithm can flag similar suspect credit card transactions as potentially fraudulent. Some payments providers use more advanced forms of Machine Learning, called Neural Networks (also called unsupervised machine learning), which is highly dependent on the quality and number of data points. Refer to Appendix A for more information on the different types of fraud detection systems.

Machine Learning *based fraud detection* ***requires large, high quality data*** *sets*

There is a ***direct correlation*** *between the* ***quality of data*** *and the ability of Machine Learning algorithms to* ***identify fraud***

Both supervised and unsupervised machine learning systems require vast amounts of high-quality data to enable identification and modelling of behavioral patterns to identify fraud.

Cyber-crime and fraud syndicates operate globally and often test a new modus operandi in a particular territory before rolling it our globally. Payment card providers deploy sophisticated Machine Learning algorithms that use global fraud data sets, to screen transactions for potentially fraudulent activities. Sharing fraud data across territories is important to keep pace and enable financial service providers to fight fraud as it moves and evolves quickly.

Quantifying the impact of data fragmentation on fraud losses

While precise forecasts under different scenarios is challenging given the unknowns, it is possible to use proxy data to determine the directional impact of fragmentation and the loss of data sets used in machine learning based fraud detection models. Gerhard Svolba, data scientist at SAS, performed an analysis to quantify the effects of missing values on model accuracy in supervised machine learning models. In his particular case study, he found that with only 10% of missing values, almost 18% of the predictive power of the perfect world model is lost. The models predictive ability progressively worsens as more data is lost, 30% missing values results in a 31,6% loss of predictive power and 50% missing values results in 52,6% loss in predictive power of the model.

A 10% loss in the machine learning data sets could result in additional ***$62 billion*** *losses up to 2030*

A 50% loss in the machine learning data sets could result in additional ***$180*** *billion losses up to 2030*

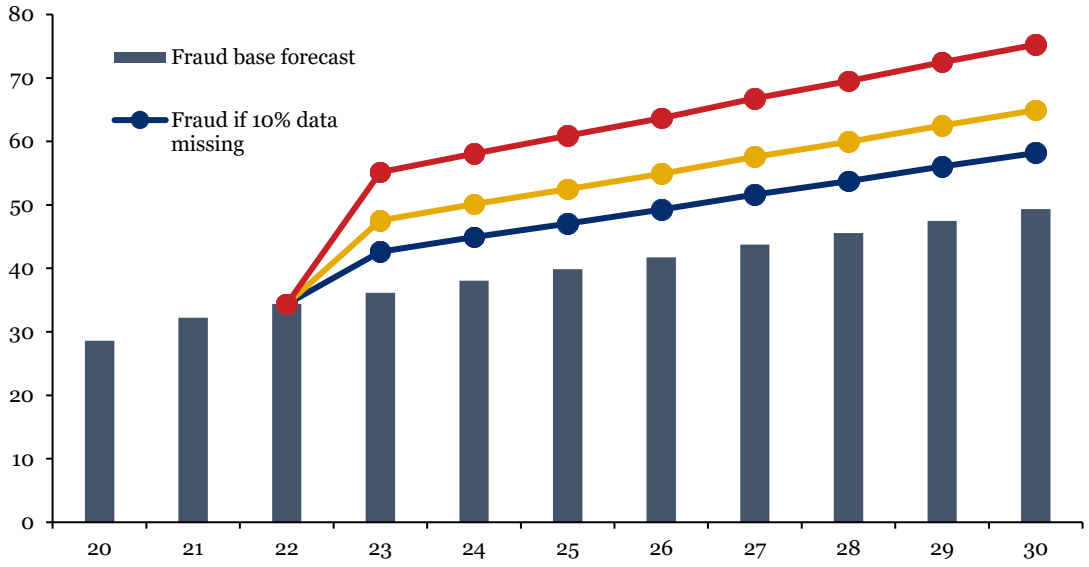
Different circumstances could lead to the loss of data in the machine learning fraud data sets, for example the following plausible scenarios could be considered (illustrated in the graph below):

- A **10% loss** in fraud modelling data could occur when **a few countries** across the globe impose restrictive cross-border data transfer requirements, thereby no longer allowing the transfer of payment card fraud data to contribute to the large data sets of global payment card processors.
- A **30 % loss** in fraud modelling data could occur when large trading blocks are formed and fraud data is **only allowed to be shared within the respective trading blocks**, or between such trading blocks, where trade agreements and equivalence recognition arrangements are in place.
- A **50% loss** in fraud modelling data could occur when **large scale digital fragmentation sets in** across the digital economy, where most countries adopt nationalistic protectionist measured, require in country localized infrastructure, and prohibit the sharing of fraud data across borders.

If we assume a simple approximation overlay on fraud loss forecasts using Svolba's results, a significant increase in fraud losses could potentially be experienced when data flow restrictions result in fragmentation of fraud prevention data sets.

Exhibit 1: Data completeness influences losses

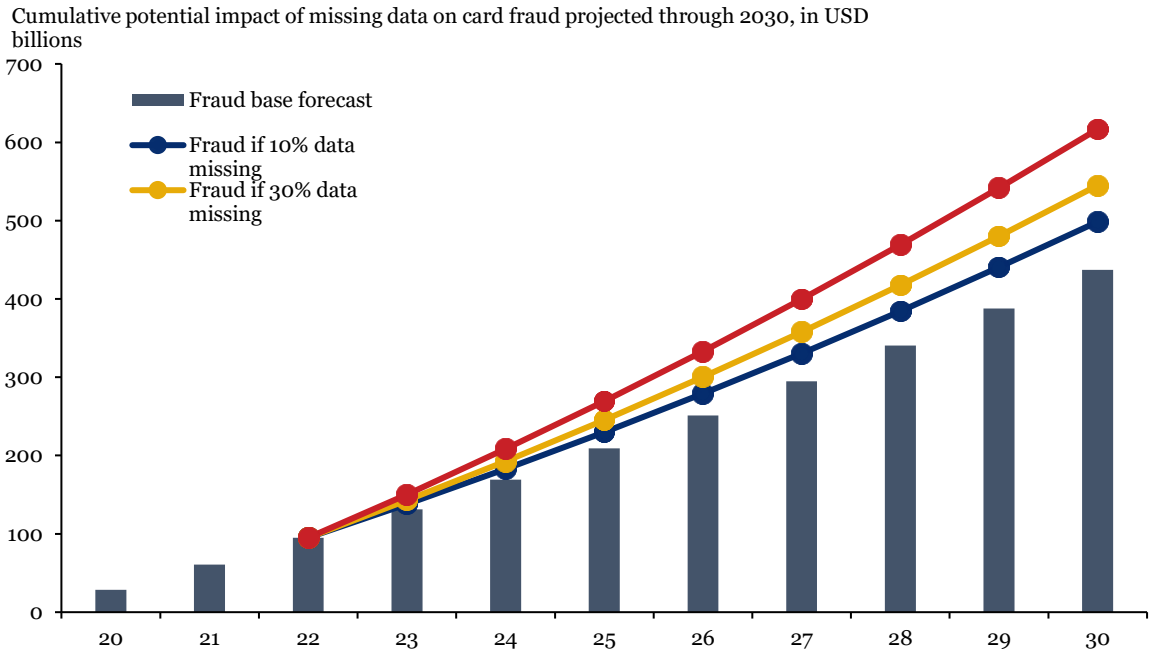
Potential impact of missing data on card fraud projected through 2030, in USD billions



Source: Nilson report, IIF

Once digital fragmentation sets in it will be very difficult to undo. The resulting deterioration in ability to detect and prevent payment fraud and the broad-based impact on the economy could be meaningful. The current geopolitical dynamic is an additional driver and exacerbates trends in digital fragmentation. Under these scenarios, the cumulative effect of fraud losses could reach an additional **$108bn** of fraud up to 2030 if 30% of machine learning fraud data is lost and up to an additional **$180bn** up to 2030 if 50% of machine learning fraud data is lost. The imperative to digital fragmentation policies, such as data localization or prohibition of transfer of fraud data across borders.

Exhibit 2: Cumulative impact of missing data is significant



Source: Nilson report, IIF

III. Conclusion

Fraud is a major problem for all participants in the payment ecosystem, including MSME's, and consumers, and is growing larger with the increase in digital transformation and commerce. Fraudsters are constantly innovating and rapidly adopting new technologies, including the use of Artificial Intelligences, facial recognition, geolocation and voice recognition to enable their malicious actions and identity theft.

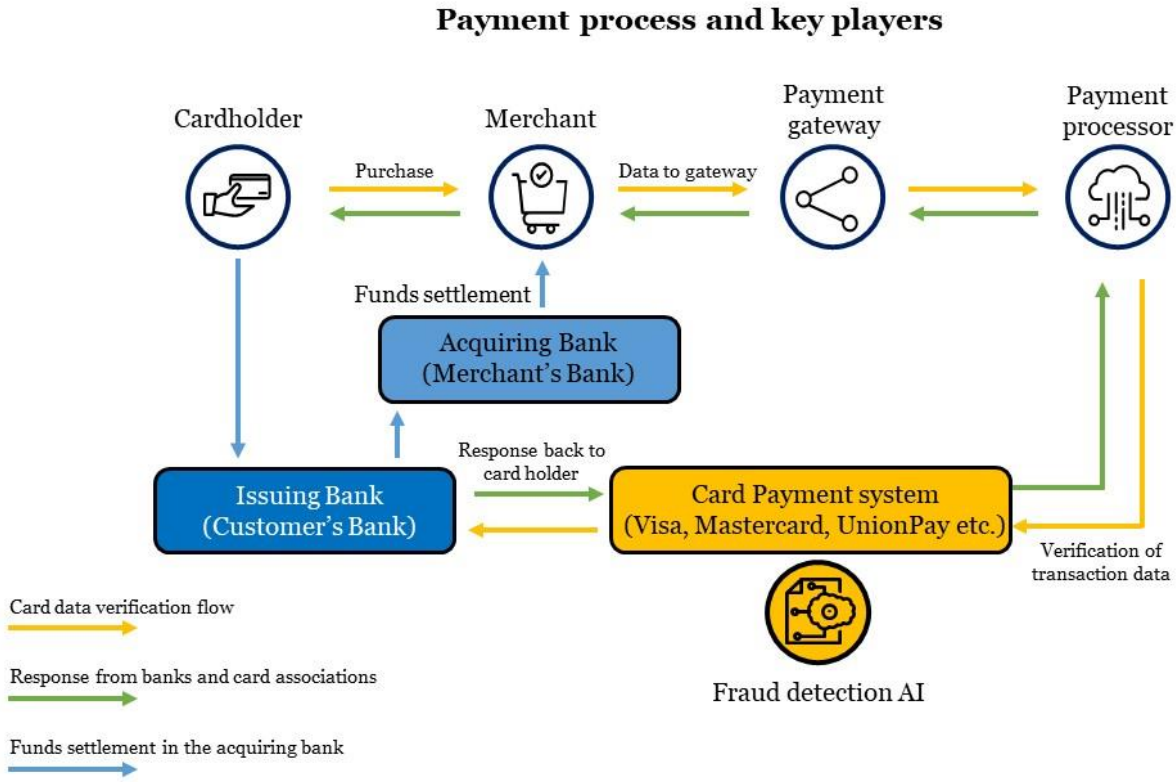
To keep pace and combat these challenges, it is vital to continue developing and deploying the latest fraud detection and prevention systems globally. Data and its behavioural analysis provide the cornerstone that enables sophisticated machine learning based fraud detection to continue to evolve and fight emerging fraud trends. This relies on sharing fraud data and intelligence across the global ecosystems as well as maintaining the integrity of sophisticated machine learning based fraud detection and prevention platforms that are used to combat these threats.

Restriction on transaction and cross-border data flows will weaken and fragment fraud detection and prevention capabilities while allowing fraudsters more opportunities to commit their crimes. The financial impact of payment fraud on economic participants in the financial eco-system is significant and broad based. MSMEs and consumers are significantly impacted given their more limited resources and skilled talent in this specialized area. Third parties, including payment providers, are essential to help these enterprises mitigate risks while growing their businesses. Increases in fraud not only impacts job creation and societal wellbeing in general, but also transmits to the real economy where it ends up harming consumers.

Appendix A – Fraud detection and prevention value chain

The card payment process

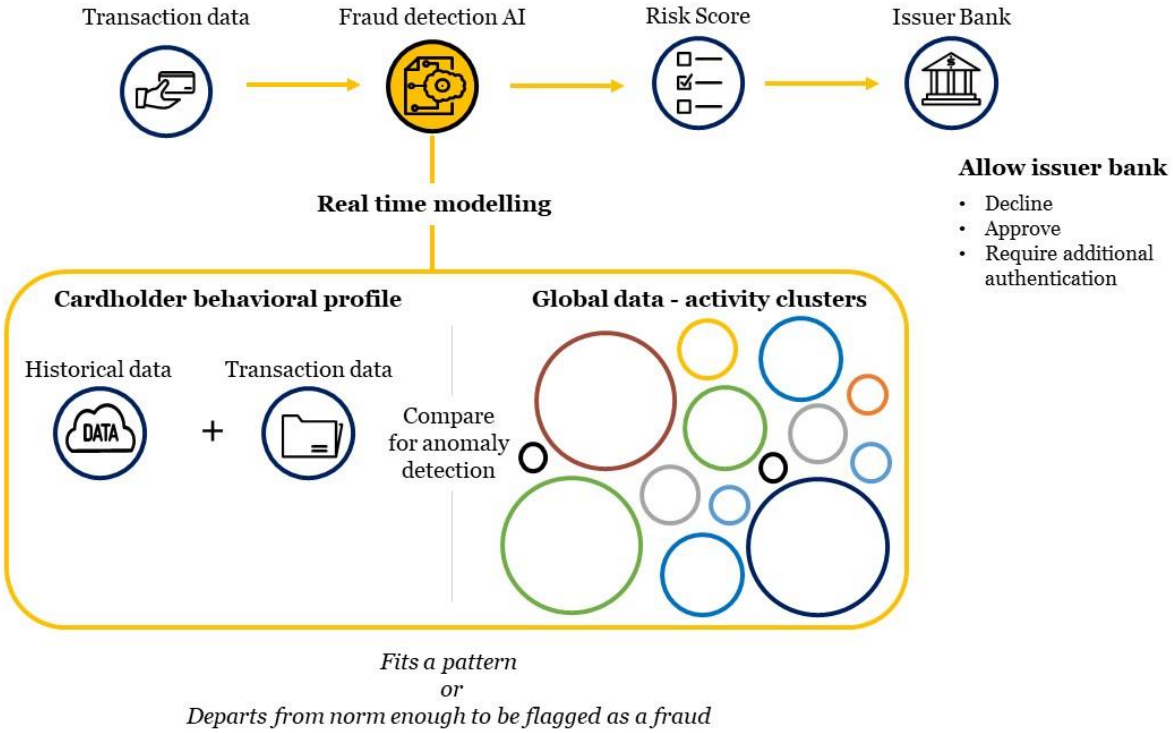
Retail payment systems are important for the advancement and smooth functioning of economic activity in society. A typical retail payment process is illustrated below:



Card payment systems are complex global networks that make use of advanced machine learning (Artificial Intelligence) technology that that enables transaction approval in less than a second.

As part of this network, fraud detection and prevention modelling and analysis is performed real-time at scale, to determine if a particular transaction fits a pattern that is in line with expectations, or if the transaction departs from the norm of modelled behavioural patterns that indicates a high probability for fraud. The model produces a risk score as illustrated below, that enables the issuing bank to decide if they should approve or decline the transaction or require additional forms of authentication.

Real time fraud detection and prevention machine learning models deployed by leading payment system providers rely on vast amounts of data to enable identification and modelling of behavioural patterns that enable the machine learning algorithms to distinguish between legitimate vs. fraudulent behaviour.



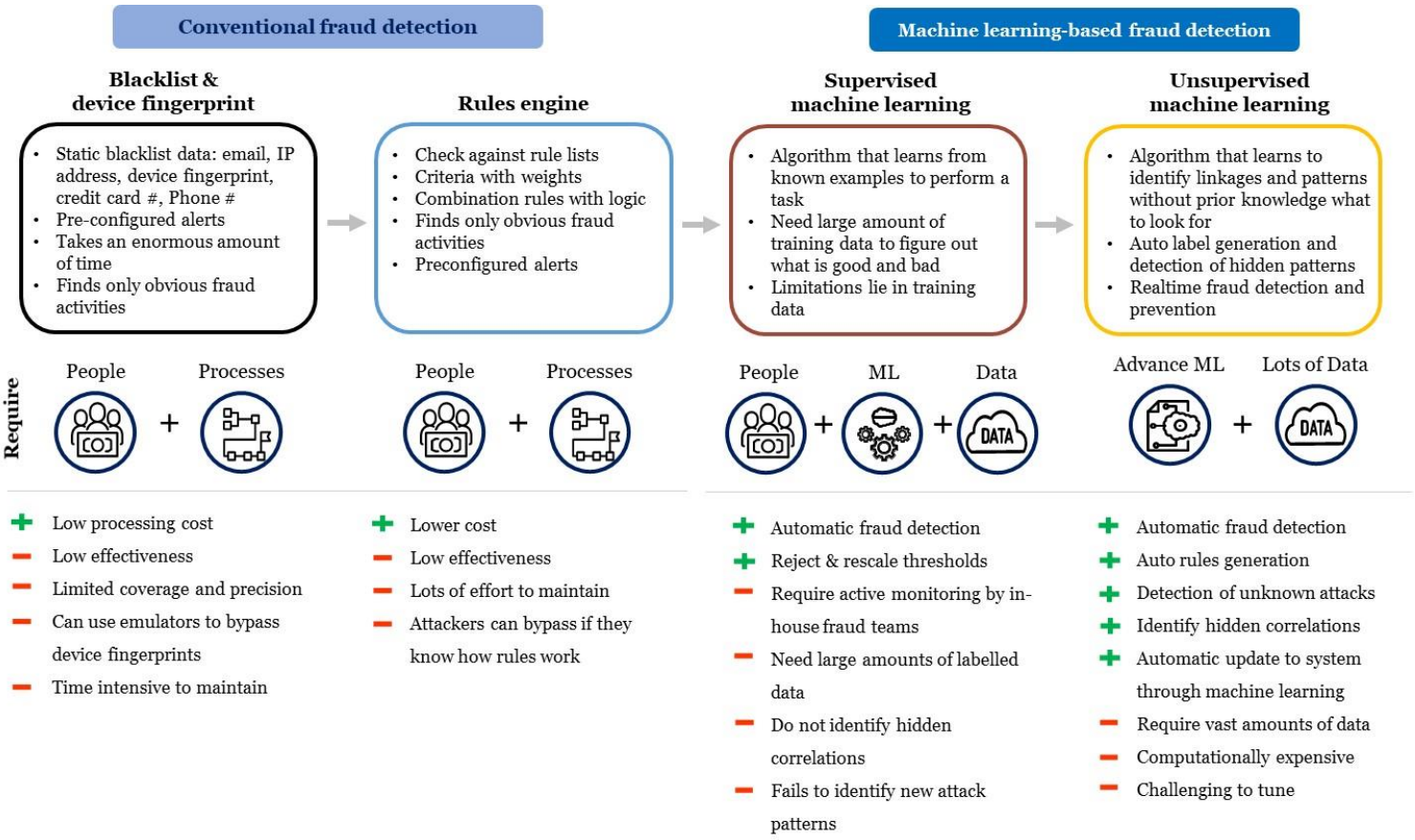
A significant number of fraudulent transactions are sophisticated in nature, for example linked to identity theft, which is difficult to detect. Therefore, fraud detection systems must incorporate behavioural analysis to determine which transactions fall outside the expected regularity of a client's spending patterns. Metrics such as standard deviation, averages and high/low values are most useful to spot irregular behaviour.

For machine learning algorithms to operate effectively, a rich data set of transactional and historical data is required across territories. The following data are typically required for fraud detection & prevention modelling purposes:

- Date and time of transaction
- IP address
- Geolocation (latitude/longitude)
- BIN data
- Device authentication data
- Product category
- Transaction amount
- Provider (Seller)
- Account profile
- Agent information
- Historical transaction patterns

Advances in Fraud detection and prevention technologies

Payment fraud detection and prevention technologies have evolved significantly in recent years from conventional fraud detection practices such as black lists, device fingerprints and rules engines, towards much more advanced machine learning based systems, as illustrated below.



Conventional fraud detection systems, consisting of backlist, device fingerprints and rules engines, were developed mostly on a standalone basis and have the following limitations:

- The rules for making a decision on determining schemes should be set manually.
- Takes an enormous amount of time.
- Multiple verification methods are needed, thus inconvenient for the user.
- Finds only obvious fraud activities.

Conventional fraud detection systems are not efficient in distinguishing a fraudulent transaction from irregular or mistaken transactions, for example, a user who clicked a purchase button twice by accident or ordered the same item twice could be identified as fraudulent. Machine learning systems are better placed to differentiate a fraudulent transaction, for example a cloned transaction, from one made in error.

Machine learning based fraud detection systems have been developed on the back of advances in the application of Artificial Intelligence (AI) algorithms that learn from big data sets and incorporate transactional data and behavioural profiles across all territories. Machine learning based fraud detection systems have the following benefits:

- Detects fraud automatically.
- Real-time streaming.
- Less time needed for verification methods.
- Identify hidden correlations in data.

In order to achieve the above-mentioned benefits, machine learning based fraud detection solutions make use of either supervised or unsupervised learning.

- **Supervised machine learning** means that a model learns from previous examples and is trained on labeled data. The dataset has tags that tell the model which patterns are related to fraud, and which represent normal behavior. This type of model requires active involvement from the in-house fraud detection team to ensure that labelled data is constantly updated to reflect new fraud trends.
- **Unsupervised learning** is also called anomaly detection as it automatically captures unusual patterns. Unsupervised learning does not require datasets with labels or instructions as the algorithms are programmed to detect the patterns from the data set. Unsupervised learning can achieve less accuracy than supervised learning, especially when the algorithms are not well tuned, but it is far superior in detecting hidden fraud patterns and other unknown insights.

Most advance fraud detection systems deployed currently combine both machine learning-based approaches that complement each other. These systems typically require vast and complex infrastructure that is made available using hyperscale cloud-based data centres, and cross-border flow of transactional and fraud data is a vital requirement for efficient and effective fraud detection and prevention.

Machine learning based fraud detection is required to identify sophisticated fraud

Criminals embrace technology and have become very sophisticated in their methods used to commit fraud. Conventional fraud detection mechanisms are not able to detect most of the sophisticated forms of fraud, instead sophisticated machine learning based systems are required to identify and detect these forms of fraud as illustrated in the examples below:

Type of fraud	How machine learning is used to identify fraudulent activities
Clone transactions	• Clone transactions involve creation of fraudulent transaction similar to the original transaction, much like sending the same invoice to multiple departments for payment. • Machine learning is used to differentiate fraudulent clone transactions from duplicate transactions cause by human error, based on behavioral analysis and pattern identification.
Identity theft	• Criminals can use stolen personal information to impersonate an individual and conduct fraudulent transactions using the stolen credentials. • Machine learning is used to identify irregular spending patterns, for example an unusual location and amount different from the customers normal behavior could be considered irregular, requiring additional forms of authentication.
Application Fraud	• Application fraud is often accompanied by identity theft, where criminals apply for a new credit account or card using stolen or counterfeit documents and credentials. • Machine learning is used to detect application fraud by means of using anomaly detection algorithms to identify whether a transaction has any unusual patterns, such as device used, location, date and time or the number of goods.
Credit Card skimming (electronic or manual)	• Credit card skimming entails making an illegal copy credit or bank card with a device that reads and duplicates the information from the original card. Such skimmed cards are normally produced and sold to criminals on the black market. • Machine learning uses classification techniques that can identify fraudulent transactions based on the hardware used, geolocation and information about a client's behavioral patterns to identify fraudulent activity.

Account takeover	• Fraudsters can gain access to account holder information via techniques such a deceptive emails, called phishing or deployment of sophisticated malware to steal personal information, account details and passwords. • Machine learning solutions rely on neural networks or pattern recognition to learn suspicious looking patterns, such as abnormal location and time activity, as well as detect classes and clusters to use these patterns for fraud detection.
Use of mule accounts for money laundering	• The use of mule accounts is increasing rapidly to launder proceeds of crime. Mule accounts are legitimate accounts that are "rented" for a fee to process large transactions, for example the transfer of stolen fund that is then instantly cashed out or used to purchase luxury items. • Machine learning solutions can identify unusual patterns and behaviors associated with the use of mule accounts, whereas conventional AML and fraud detection methods would not be able to detect such activities.

Requirements for machine learning solutions

Predictive machine learning models require large volumes of high-quality data in order to function. The following components are required for effective and efficient machine learning models:

1. **Amount of data**:
   - Training high-quality machine learning models requires significant amounts of historical data.
   - Machine learning models cannot run effectively on smaller data sets, as the quality of the training process depends on the quality of the inputs.

2. **Quality of data**:
   - Models may be subject to biases based on the nature and quality of historical data.
   - Therefore, errors, omissions and miss classification of the data set will likely cause a major bias in the model results.
   - Global data sets offer much higher quality data that tends to be unbiased.

3. **Data mining setup**:
   - Prior to any form of analysis, the collection and storage of large volume of historical transaction and fraud data across territories are required
   - Classification and grouping of data are required
   - Segmentation of data to search millions of transactions to find patterns and identify fraud is required.

4. **Pattern recognition modelling:**
   - Algorithm modelling entails detecting the classes, clusters and patterns of suspicious behavior.
   - Algorithms require tuning and fitting as part of the implementation process, and ongoing maintenance of the system.
   - Neural networks are used to automatically identify the characteristics most often found in fraudulent transactions.

Fragmentated architecture scenarios

Imposing restrictions on the sharing and flow of transactional & fraud data across borders will lead to a path of fragmentation. Two main scenarios could be envisioned:

1. Rebuild a local machine learning based fraud detection instance:

- This scenario would occur where large countries or trading blocks impose restrictions on the transfer and storage of transactional and fraud data outside their borders.
- These countries will be required to have sufficient access to hyperscale cloud based data center technology and skills to be able to build a localized fraud detection solution instead of continued use of global solutions currently deployed.

2. Loose access to advance global scale fraud detection platforms:
   - This scenario would occur where smaller countries, mostly emerging markets or countries under sanction restrictions, impose data restrictions and require localized infrastructure,
   - Under this scenario countries may not have sufficient access to hyperscale cloud based data center technology in country, large data sets and skills to develop sophisticated machine learning based fraud detection solutions.

Each of the fragmentation scenarios brings about significant breakdowns and conflicts that will inhibit sophisticated fraud detection and prevention, as detailed below.

	Rebuild local instance using ML technology	**Isolated system – loss of advance technology**
Feasibility requirements	• Only possible for countries with advance payment systems and technologies. • Require hyperscale cloud based data centers for computation power. • Require large high quality historical data sets.	• Most countries or territories will be able be revert to conventional fraud detection system, however, these will be inadequate for fraud detection and prevention purposes.
Conflicts & breakdowns	• An imbalanced data set would exist due to loss of fraud data outside the territory, this will create limitations in the effectiveness of machine learning algorithms. • Integration with domestic and foreign payment systems will be exceedingly difficult to achieve, expensive and take a considerable amount of time. • User experiences would deteriorate due to inefficiencies and new system integration challenges. • It would not be possible to detect emerging fraud patterns that occur outside the territory given data limitations. • Fraud committed outside the borders would not be identified easily and could spiral out of control. • Cross-border law enforcement outside the territories will be hampered.	• Cross-border law enforcement cooperation would be significantly hampered. • Integration with payment systems will be problematic with significant delays in transaction approval times, resulting in huge frustration from users. • Interoperability with cross-border payment systems would be problematic. • The country will lose all advance fraud detection benefits providing advanced criminals with a great advantage.

Potential financial impact	• It would require extensive cost and multiple years of effort to re-establish a new localized fraud detection and prevention architecture. • Fraud losses could increase significantly due to reduced efficiency in detecting emerging fraud patterns.	• Potential for unlimited increase in payment fraud for businesses and the financial system.

Appendix B - Resource list

There are several very insightful publications, articles, videos and reports available that have been used as input to our research. The list below provides a reference of key resources used.

Altexsoft Software r&d engineering, Aug 2020, "Credit Card Fraud Detection: How Machine Learning Can Protect Your Business From Scams "

Altexsoft Software r&d engineering, "Fraud detection: How Machine Learning Systems Help Reveal Scams in Fintech, Healthcare , and eCommerce"

AWS Summit April 2019, Datavison, "Fraud detection Platform using AI and Big Data"

Businesswire, "Visa Prevents Approximately $25 Billion in Fraud Using Artificial Intelligence article"

Credit Card Fraud Detection, SPD Group, "Top ML Solutions in 2021"

Detecting Credit Card Fraud Using Machine Learning, Towards data science, "Catching bad guys with Data Science"

Department of Computer Engineering, Istanbul Technical University, Yusuf Yazici, "Approaches to Fraud Detection on Credit Card Transactions using Artificial Intelligence Methods"

European Banking Authority, January 2020, "EBA Report on Big Data and Advanced Analytics"Version 1

SAS, Gerhard Svolba, "Quantifying the Effect of Missing Values on Model Accuracy in Supervised Machine Learning Models"

International Journal of Engineering and Advanced technology, Volume-8, August 2019, "Machine Learning Methods for Analysis Fraud Credit Card Transaction"

International Journal of Engineering & Technology, "Machine Learning Approaches for Credit Card Fraud Detection"

Intel Case study, Financial Services Machine Learning, "China UnionPay takes a proactive approach to risk mitigation"

London Stock Exchange Group, "Unlocking the Value of Data Flows in the Digital Economy"

MAP, Member access processing, "Visa's AI Fraud Detection Is a Step Above The Rest"

Merchant Savvy, "Global Payment Fraud Statistics, Trends & Forecasts"

Nilson Report, December 2021, "Card Fraud Losses Worldwide"

OECD, Artificial Intelligence, Machine Learning and Big Data in Finance, "Opportunities, Challenges and Implications for Policy Makers"

PYMNTS.com, "How Mastercard Uses AI to fight fraud and make better credit decisions"

PYMNTS.com, "AI in Focus: Gaining Ground on Merchant Monitoring"

South African Bank Risk Information Centre (SABRIC), "Sabric Annual Crime Statistics 2020"

SPD Group, Oleba Kovalenko & Roman Chuprina, "E-Commerce Fraud Detection and Prevention: The In-depth Guide"

Visa Economic Empowerment Institute, "Small Business in the Digital Age: Recommendations for Recovery and Resilience"

Visa's artificial intelligence (A.I.) for payment authorization and fraud detection, "How it works"

Visa AI Security, "Transforming Payment Security Through Artificial Intelligence"

Authors

Jaco Grobler
Founder, New Paradigm Finance
jaco@newparadigmfinance.com

Conan French
Director, Digital Finance
cfrench@iif.com

Contributors

Jessica Renier
Managing Director, Digital Finance
jrenier@iif.com