AI application to Strong Customer Authentication: examples from the Payment Processing Industry

The why, how and what of dynamic fraud detection through SCA generated data

Barbara Di Stefano

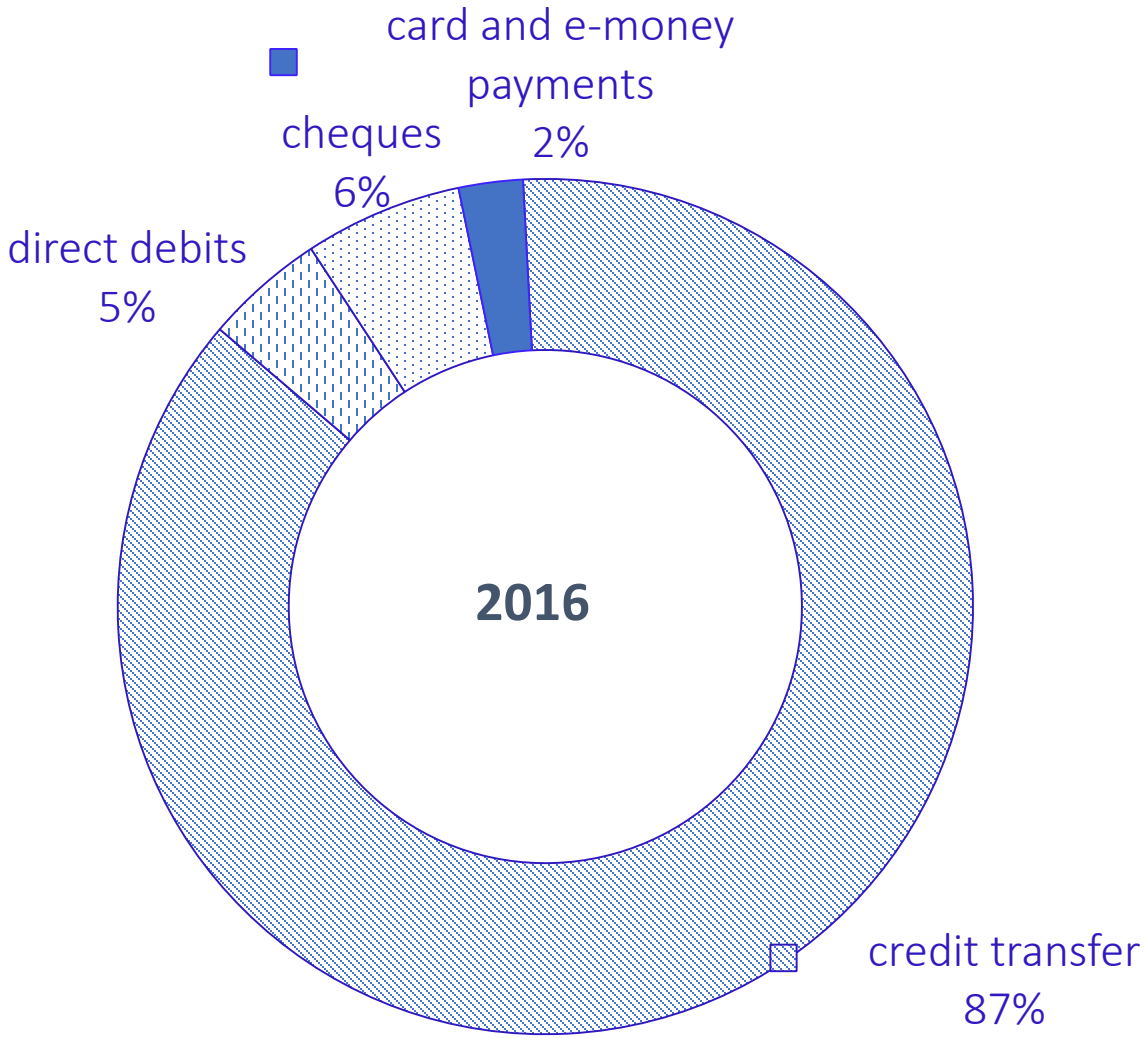
1 st European Conference on Risk Management and Big Data in Finance,
3rd of September 2019, Winterthur

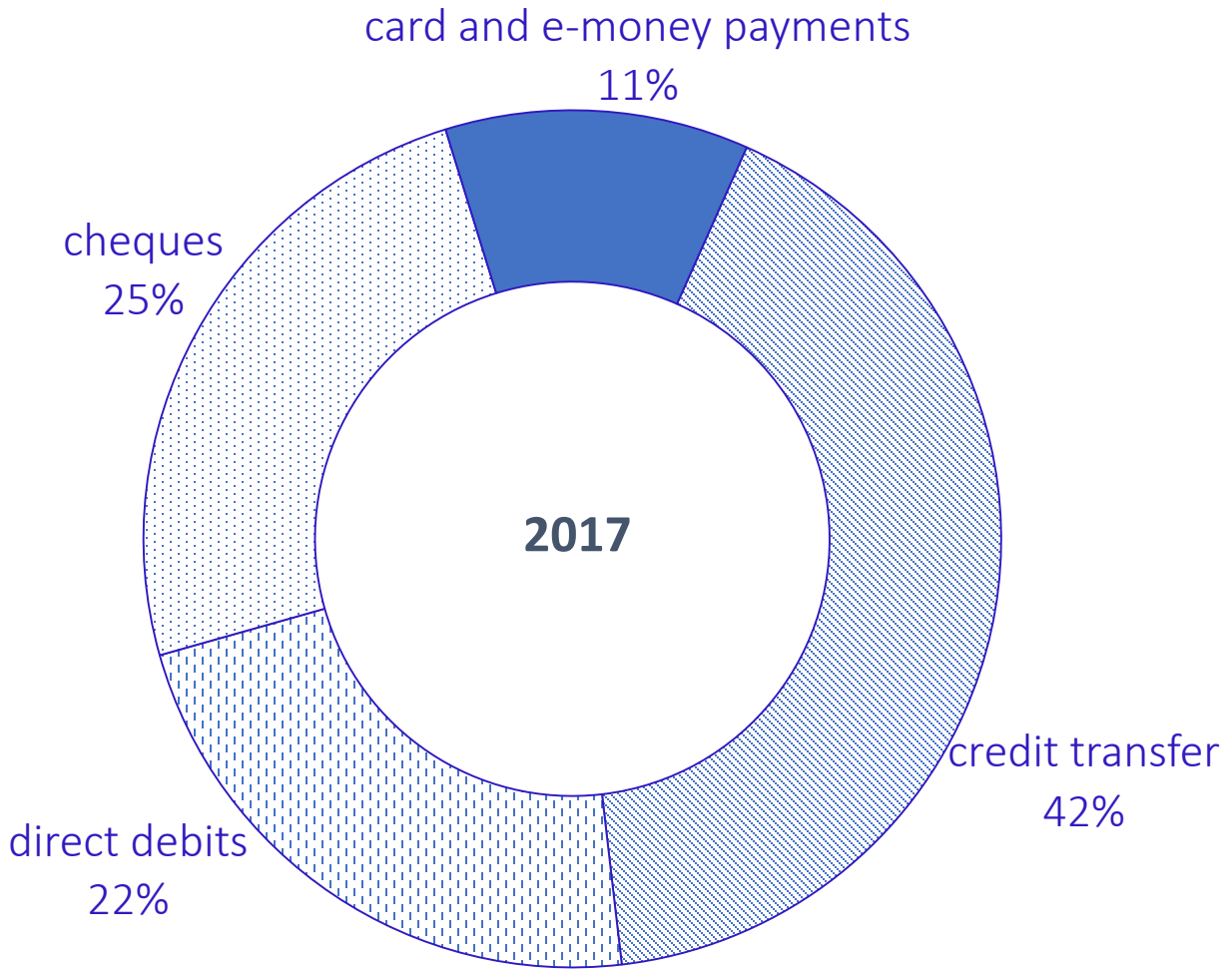
Context

- Digital payment system is significantly changing consumers' expectations and behaviour.
- Making or accepting payments presents a major challenge to payment service providers (PSPs) through these new and emerging delivery channels while simultaneously ensuring interests are protected from fraud, deceptive practices and lack of reliability of devices and infrastructures.
- Digital services have introduced a completely remote bigger problem - false positives and drop off, where good transactions are getting blocked or aborted. The ratio of false positives and drop off to fraud varies a depending on the merchant's anti-fraud setup, and can go from 5:1 to as high as 30:1. Improved customer experience means more data available whenever and wherever users want it, smarter security and most of all – less purchase friction (i.e. false declines).
- Thus, in the context of both meeting regulatory provisions (PSD2) and enabling growth of retail volume seamlessly across all channels, payment service should adopt robust identification and authentication systems to detect or prevent fraud.

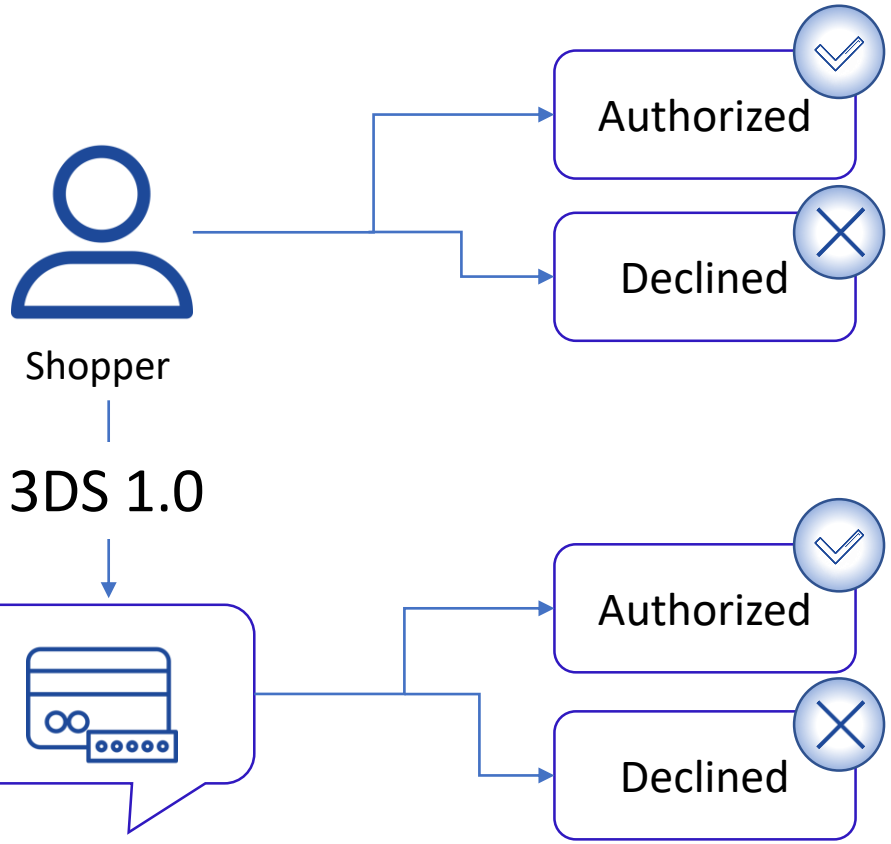
Cashless payments in Italy (Million Euros)

- Source: Internal elaboration from Bank for International Settlements (BIS) data (in Million Euros)





3D Secure



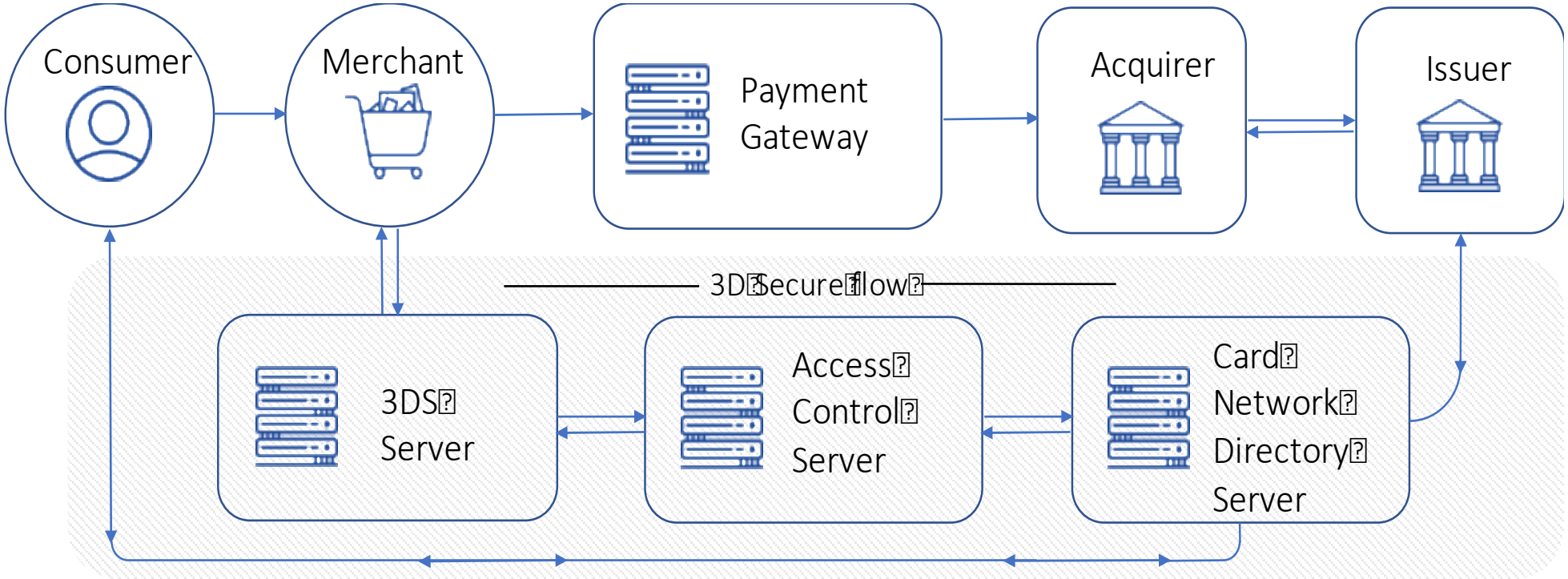
Challenge: Static screen requiring a PIN, passcode, OTP via SMS, etc..

- 3D Secure 1.0 first emerged as a fraud prevention framework in a bid to protect credit and debit card transactions.
- Even though, the benefits that 3D Secure 1.0 came with in terms of fighting fraud were indeed a positive sign for merchants, the technology, which only supported browser transactions contributed to a drop in conversions as it was not able to enhance customer experience.

3DS 2.0

The latest version of the protocol makes mobile, in-app and digital wallet transactions a reality and is equipped with advanced functionalities and features which include processing of end-to-end messages and risk-based authentication.

- 3D Secure 2.0 eliminates the need of static passwords in favor of biometric authentication.

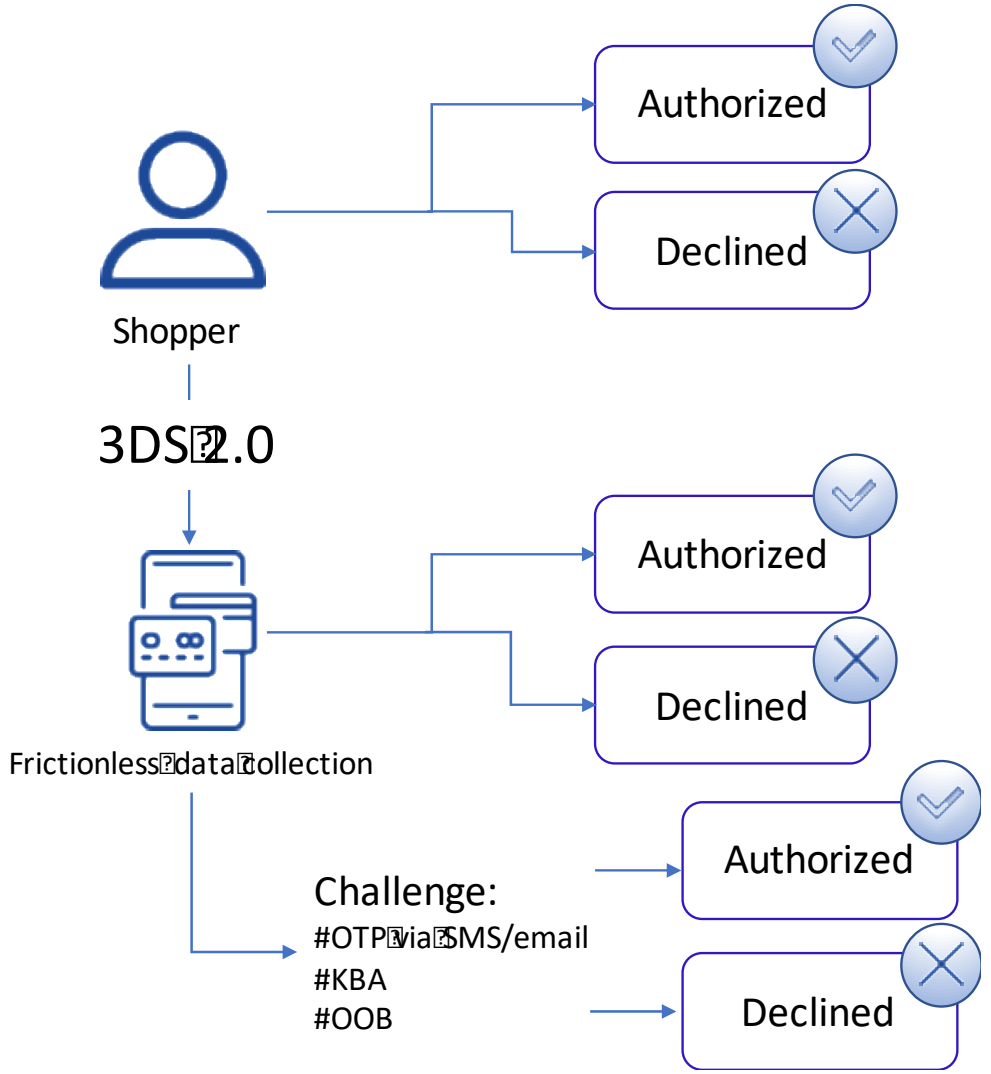


- 3DS 2 facilitates rich data exchange between merchants, card-holders and issuers, more so than ever before to achieve more accurate authentication

(*) EMVCo's work is overseen by EMVCo's six member organisations—American Express, Discover, JCB, Mastercard, UnionPay, and Visa—and supported by dozens of banks, merchants, processors, vendors and other industry stakeholders who participate as EMVCo Associates.

3DS 2.0 : frictionless payment

- One major change of 3DS 2.0 is that it will offer the ability to authenticate a transaction using a biometric method. By using finger prints or facial recognition the amount of fraud is potentially going to be greatly reduced while also increasing convenience for consumers.
- Another major implication of 3DS 2.0 is that when a customer makes a purchase, the merchant will have the option of agreeing to '**frictionless flow**' – where the payment is authorised without additional security measures.
- Alternatively, they can request that the payment is challenged resulting in the issuer making a risk-based authentication of the consumer and potentially (Transaction Risk Assessment) asking for further security, such as two-factor authentication.



European Payment Service Directive (PSD2 - September 2019)

Strong Customer Authentication (SCA)
Unless the payment qualifies as low risk, customers must authenticate transaction with at least two independent factors

Something you **own**

Something you **know**

Something you **are**

Largest impact will be on remote electronic payments SCA must be applied to all electronic payments unless out of scope or exempted.
Financial transactions can be classified in two ways:

Cardholder initiated transaction (CIT)

Merchant initiated transaction (MIT)

Low Risk

Transaction Value Band	PSP Fraud Rate
<€100	13 bps/0.13%
€100-€250	6 bps/0.06%
€250-€500	1 bps/0.01%

Exemptions

- Contactless payments at point of sale (*)
- Unattended transport and parking terminals
- Recurring transactions
- Low value transactions
- Secure corporate payments
- Transaction risk analysis
- Trusted beneficiaries

(*)Contactless transactions are exempt from SCA unless transactions exceed the count/amount thresholds

Strong Customer Authentication

- SCA is a new European requirement created to make online payments more secure. When a European shopper makes a payment, extra levels of authentication will be required at the time of the transaction.

- This means that merchants who contract with an acquirer licensed in the EEA will likely see an increase in declines on transactions processed on credit cards issued in the EEA region if SCA requirements are not met. This should not be the case on transactions processed on a non-EEA issued card, however, nor would it apply to merchants contracting with acquirers licensed outside the EEA, regardless of whether the card is issued in the EEA region.

Transaction Risk analysis and Risk Based Authentication

The fight against fraud has also matured emerging technologies and thrust them into the legislator's limelight as solutions to the seamless UX/strong authentication paradox.

Notably, Fintechs have been investing in machine learning and neural networks to apply artificial intelligence (AI) to learn from each payment iteration or sequence to paint a picture of what 'normal behaviour' looks like for each customer. With normal behaviour accounted for, PSPs can dedicate resources to flagging abnormalities, thereby making the fight against fraud far more cost effective and bumping up the demand for machine learning solutions at the same time.

Following industry appeal and particularly complimentary to the concept of machine learning techniques, regulators have accepted that risk analysis parameters can be applied to make fraud monitoring more effective and efficient. They have been forthcoming in providing guidance on how to determine which transactions can be exempt from SCA; namely the EBA's Transaction Risk Analysis (TRA) and EMVCo's Risk Based Authentication (RBA).

Risk assessment

- Here is where Fintechs play an interesting role, by helping acquirers to assess transactions at their inception, so that when exemptions for frictionless transactions is recommended to issuers these are accepted and put into action.

- AI technology enables to bring accuracy to the market and to understand the user behaviour. In addition to accuracy, AI technology brings new advantages in scalability and speed. These are very important topics in the risk management world because the more friction you bring into a checkout process, the higher is the chance that you have a drop-off.

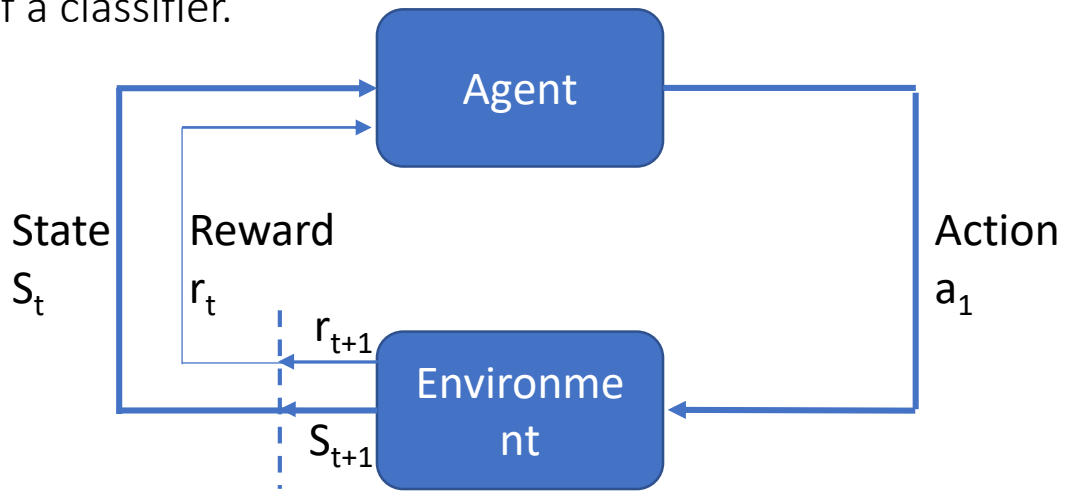
- AI technology offers users, as well as merchants and businesses two main advantages. One is to increase the accuracy. Data availability itself is not enough: It is about what you do with it.

Account Risk Assessment - Methodology

Our analysis is rooted primarily in reinforcement learning.
Adversarial learning is a subfield of machine learning that focuses on the ability of an actor to generate high-volume, low-cost observations to prod the capabilities of a classifier.

The reinforcement learning agent itself is going to be an adversary to a classifier and the training process is unmolested (classifier focused approach).

The data set contains nearly 86 million observations which are anonymized credit card transactions over 12 months from September 2017 to August 2018.



The other attributes range from

- transaction level data such as transaction amount, merchant category code, distance between the transaction and home
- account level data such as account balance, account opening date, days since phone number change on account, registration to Nexi Pay, Apple Pay, Samsung Pay, Active biometric data authentication.

The dataset was large enough that we built a set of 25 randomly-sampled sets of the transaction history of 5,000 credit card accounts. On average, each of these sets had 130,000 transactions and all of these sets contained some fraud.

Analysis Execution

Our experimental classifier was trained on the credit card dataset and tested on a held-out dataset randomly sampled from the original dataset.
We built a logistic regression model to act as the fraud classifier environment designed to interpret state and action information coming from the agent.
This fraud classifier is fairly simple with just 4 predictors:

- # of low € -amount transactions
- # of high € -amount transactions
- whether the action is a low or high € -amount
- cardholder use digital payment through SCA at least once in the last 30 days.

We used €78 as the cutoff for a low/high € -amount transaction based on median transaction amount across all fraudulent transactions in the dataset.

We trained our model using data from one of the 25 random samples across accounts by randomly selecting an account, and then randomly selecting a sequence of five contiguous transactions from that account.

One of the immediate issues with our data was a significant class imbalance. In our dataset, fraud makes up ~0.1% of all credit card transactions. To this end, we down-sampled the non-fraud transactions to achieve an ~15% fraud representation during our model-building step.

Results

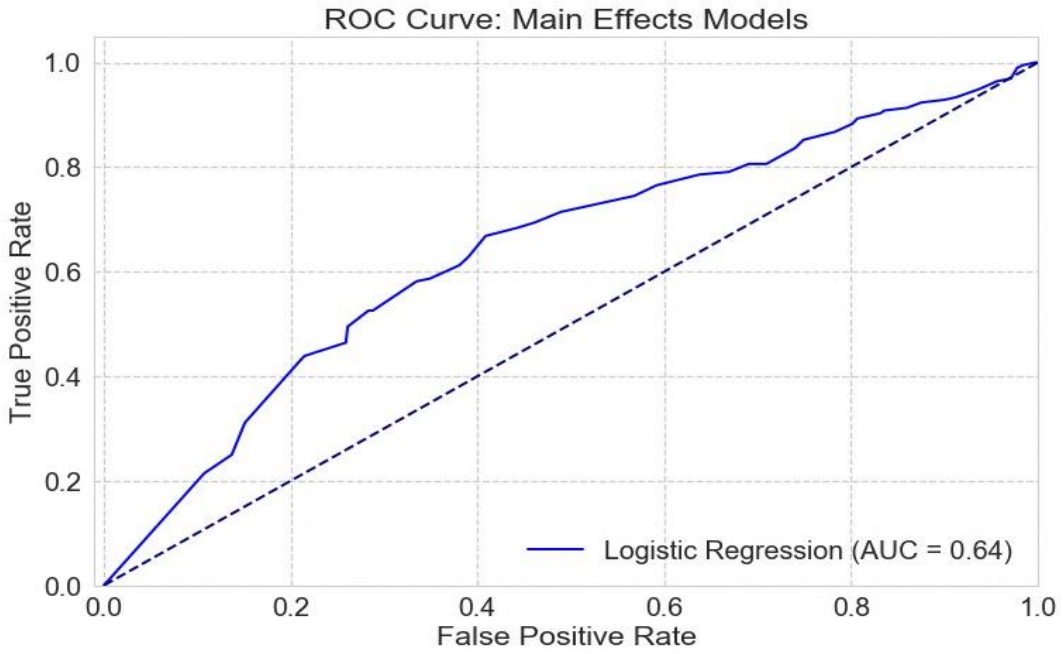
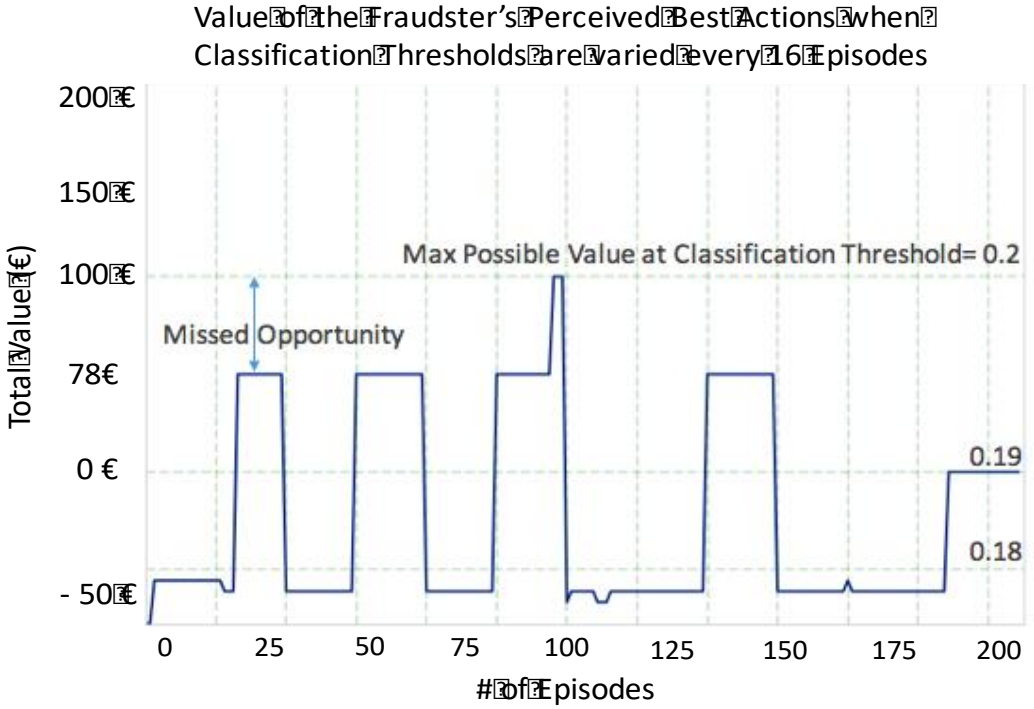


Figure above shows the effectiveness of our classifier in a Receiver Operating Characteristics (ROC) curve. Despite only using four predictive features when the original space had 69, the model still has reasonable predictive power with an AUC of 0.64.



Then our classifier was used to train the fraud agent through interaction with the environment at different classification thresholds. Once the optimal policy was reached, the total value of the policy was recorded, as was the number of episodes it took to converge on the optimal policy.

Key Takeways

PSD2 will challenge the payments industry but it will also bring an opportunity for players & solutions to excel

– Biometrics & 3DS 2.0 meets the demand of both regulators and consumers

- Issuers & merchants:

– Understand what frictionless payments impacts has to their business

– Plan and prioritize implementation of 3DS 2.0, authorization message enhancements, tokenization, and biometrics

– Work with service providers on timing for SCA readiness and how to address exemptions

- Service providers:

– Innovate and continue to work with industry groups (EMVCo, etc.) to prepare the next generation of solutions

Thank you!

For questions and/or more details on the analysis email
bmdistef@gmail.com