Il Fraud Management nell'era PSD2 e Instant

Milano, 07/11/2018

Roberto Scognamiglio
Program Manager Global Payments Solutions

Amedeo Borin
CEO and Founder Mantica

Federico Stivoli
Senior Data Scientist

Agenda

- **Il punto di partenza** 
- La soluzione antifrode AS IS
- L’intelligenza artificiale
- La soluzione antifrode TO BE
- L’intelligenza adattiva

Il punto di partenza

Il fenomeno delle **frodi** è un fenomeno in **continua evoluzione** e i prestatori di servizi di pagamento sono chiamati a mettere in campo sempre **nuove soluzioni** per salvaguardare la **sicurezza delle transazioni di pagamento**. La stessa **European Banking Authority** ha definito e tiene costantemente aggiornate delle **linee guida** specifiche sul tema (cfr. EBA/GL/2014/12 del 19 dicembre 2014)

Il numero di transazioni effettuate con carte di pagamento è in continuo aumento. Le operazioni **Card-Not-Present** (CNP) costituiscono un canale in rapida crescita, soprattutto in ambito internet e mobile, esponendo maggiormente le banche a:

- **Rischi operativi**, legati all'eventuale perdita economica derivante da un evento fraudolento;
- **Rischi reputazionali**, legati al deterioramento dell'immagine aziendale e di aumento della conflittualità con la clientela per la scarsa qualità dei servizi offerti

Un sistema di **Fraud Management** deve garantire la possibilità di gestire i processi di monitoraggio delle transazioni al fine di ottenere un equilibrio tra:

- **Efficacia:** capacità di individuare correttamente le attività sospette o ridurre al minimo il numero dei «falsi negativi»;
- **Efficienza:** capacità di identificare correttamente l'attività non sospetta o ridurre al minimo il numero di «falsi positivi».

Agenda

- Il punto di partenza
- **La soluzione antifrode AS IS**
  - **Le principali caratteristiche**
  - **Le componenti e le funzionalità**
- L'intelligenza artificiale
- La soluzione antifrode TO BE
- L'intelligenza adattiva

La soluzione antifrode AS IS: le principali caratteristiche

Il principale punto di forza della **soluzione Plus2Fraud** realizzata da TAS è **l'integrazione del motore delle regole deterministiche** con la **feature dei modelli predittivi**, che intercetta le opportunità offerte dai big data.

- Un sistema basato solo sull'utilizzo di regole deterministiche non riesce a rispondere in maniera tempestiva al **cambiamento continuo** dei comportamenti fraudolenti;
- L'approccio utilizzato da TAS prevede quindi **l'integrazione del motore delle regole deterministiche con un motore specifico di analisi delle transazioni** basato sull'elaborazione di modelli predittivi

Integrare il motore delle regole deterministiche con l'implementazione dei modelli predittivi, permette di sottoporre la transazione ad un **duplice controllo**, garantendo **un'elevata performance** del sistema antifrode ed una **forte complementarietà** dei due sistemi

Regole Deterministiche

- Le regole deterministiche sono **regole di monitoraggio** che in funzione di specifici **controlli** segnalano le transazioni con una più elevata probabilità di essere in frode;
- I controlli implementati nelle regole derivano dall'**osservazione** dei fenomeni fraudolenti già avvenuti **nel passato**

Modelli predittivi

- I modelli predittivi sono algoritmi statistici in grado di analizzare un **gran numero di dati** e informazioni e di identificare i **possibili comportamenti fraudolenti**;
- Il motore degli algoritmi predittivi ha lo scopo di **individuare le deviazioni dai pattern abituali** di comportamento identificando una varietà maggiore di attacchi fraudolenti e rilevando **velocemente nuovi fenomeni** di frode

La soluzione antifrode AS IS: le componenti e le funzionalità

La logica di Plus2Fraud prevede **l'alimentazione di due moduli distinti** e completamente **integrati** tra loro, che applicano logiche di monitoraggio differenti, la componente di **Prevention** e la componente di **Detection,** ognuna delle quali permette la **configurazione dinamica** di **regole di monitoraggio** e **l'utilizzo di specifiche liste**

FUNZIONALITA'	COMPONENTI	
	PREVENTION: è la componente che elabora la transazione **prima che essa venga autorizzata**. Se i controlli di Prevention non vengono superati, la **transazione viene rifiutata**	**DETECTION:** è la componente che elabora la transazione **dopo l'autorizzazione**. Le transazioni che violano le regole di detection, **generano una segnalazione** su un apposito **form di monitoraggio**
Regole dinamiche Le regole di monitoraggio vengono create in maniera **tempestiva** dall'utente che, in **totale autonomia**, può **configurare i controlli** da implementare sulle transazioni.	*Configurazione di **regole deterministiche** in **modalità dinamica** che **bloccano la transazione** in funzione dei **dati elementari** della transazione stessa*	*Configurazione di **regole deterministiche** che **elaborano la transazione** non solo in funzione dei **dati elementari** della transazione stessa, ma **anche della storia pregressa** della carta che sta operando*
Liste Le liste sono alimentate con un numero indefinito di dati. Contengono dati come **numeri di carta**, **indirizzi IP**, indirizzi e-mail, ecc. per cui si vuole **bloccare o segnalare** una transazione. Le liste sono **integrate** con il **sistema di regole di monitoraggio**	*Sul modulo di **Prevention** sono applicabili:* • ***Blacklist**: contiene dati su entità da cui si vogliono bloccare le transazioni (canali fisici e virtuali, IP, rapporto, …)* • ***Whitelist**: contengono dati per cui, anche se vengono violate altre regole di monitoraggio, si vuole autorizzare la transazione*	*Sul modulo di **Detection** sono applicabili:* • ***Greylist**: contiene dati su entità sospette per cui non si vuole procedere al blocco della transazione ma ad una segnalazione;* • ***Whitelist**: contengono dati per cui, anche se vengono violate altre regole di monitoraggio, non è necessario segnalare la transazione*
Modelli predittivi I modelli predittivi integrano il motore delle regole deterministiche, aumentando l'accuratezza dei controlli antifrode, ed elaborando grandi mole di dati	*Sul modulo di **Prevention** è implementato un modello che, in funzione dei dati caratteristici della transazione, intercetta le carte per cui **la prossima transazione** sarà **probabilmente in frode***	*Sul modulo di **Detection** è implementato un modello che, in funzione della storia pregressa della carta, **assegna a ciascuna transazione uno score**. Valori di score al di sopra di un certo valore vengono **segnalate ed analizzate** dalle strutture preposte al monitoraggio*

Agenda

- Il punto di partenza
- La soluzione antifrode AS IS
- **L’intelligenza artificiale**
- La soluzione antifrode TO BE
- L’intelligenza adattiva

L’Intelligenza Artificiale

L‘**Intelligenza Artificiale** (IA) è l'intelligenza espressa dalle macchine.
È quel campo della computer science che studia agenti intelligenti: qualsiasi strumento che **percepisce** in qualche modo l'ambiente intorno a sé e fa delle **azioni per perseguire un qualche obiettivo**.

L'Intelligenza Artificiale: il gioco

IA

1997

Deep Blue vs. Kasparov

Deep Mind Alpha Go vs. Lee Sedol

2015

2017

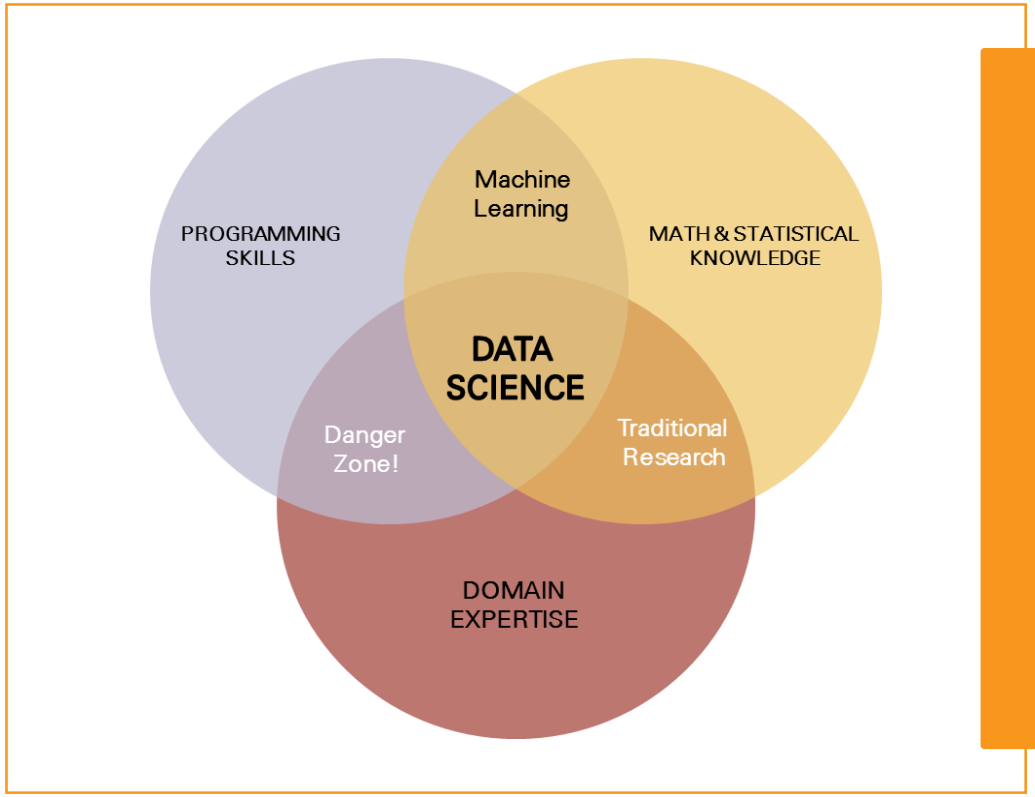
Alpha ZERO

"Durante il match, ***AlphaGo*** ha giocato diverse mosse vincenti estremamente creative, alcune delle quali – come la mossa 37 della seconda partita – così sorprendenti che hanno **rovesciato centinaia di anni di conoscenze** tramandate e sono ora oggetto di studio di giocatori a tutti i livelli.

AlphaGo in qualche modo ha insegnato al mondo una nuova conoscenza di quello che probabilmente è il gioco più giocato nella storia umana."

L’Intelligenza Artificiale: perché oggi

Sono diversi i fattori che hanno accelerato l’utilizzo dell’Intelligenza Artificiale. In particolare si intende per **Data Science** la capacità di estrarre dai dati disponibili informazioni importanti, in modo **efficiente e efficace** con **metodologie interdisciplinari**.



- ***Aumento nella mole di dati disponibili***
- ***Aumento delle connessioni tra dati***
- ***Sviluppi tecnologici in ambito di computazione, immaganizzamento dati e management dei dati***
- ***Sviluppi di nuovi algoritmi***

L’intelligenza artificiale: tassonomia del Machine Learning

In base ai dati disponibili

Supervised learning

Si conoscono una o più delle variabili di output desiderate e la macchina deve imparare a classificarle

Unsupervised learning

Le variabili di output non sono definite, la macchina deve imparare a identificare cluster, relazioni tra variabili e fornire insight sui dati.

Reinforcement learning

All'algoritmo viene dato un feedback positivo o negativo in base alle prestazioni che fornisce.

In base all'output

Classificazione

Ha lo scopo di classificare a quale categoria appartengono delle osservazioni. Tipicamente un task supervisionato.

Regressione

La variabile target è di tipo continuo. Anche questo supervisionato

Clustering

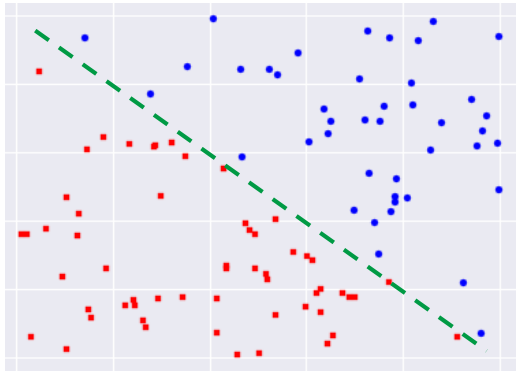
I dati vengono separate in gruppi, secondo una qualche metrica. Unsupervised.

Riduzione della dimensionalità

Ha lo scopo di semplificare data-set con troppe dimensioni, manentenendo comunque gran parte dell'informazione presente nei dati stessi.

L’intelligenza artificiale: i problemi affrontati dal machine learning

Classificazione

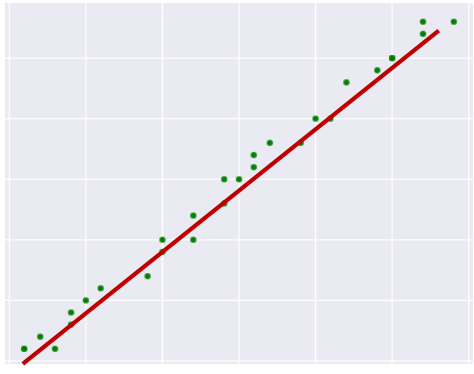


I dati usati per l'addestramento sono sia di input che di output.

Output è una **categoria**.

- *Classificazione binaria*: e.g. spam.
- *Classificazione multipla*: e.g. object detection.

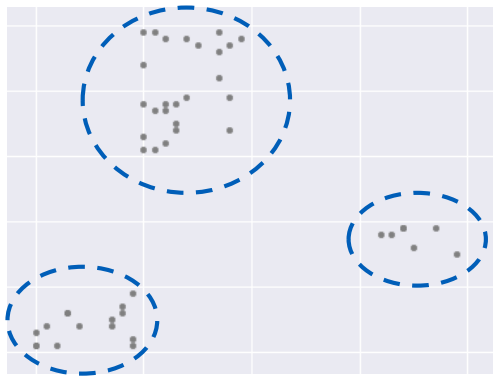
Regressione



I dati usati per l'addestramento sono sia di input che di output

L'output è una **variabile continua**, e.g. stipendi.

Clustering



I dati sono solo di input, e il target non è conosciuto a priori.

L'output è una **categoria per ogni input**, in base a similarità e.g. segmentazione di clienti.

L’intelligenza artificiale: applicazioni del machine learning

Machine Learning

- **Supervised Learning**
- **Unsupervised learning**
- **Reinforcement learning**

- **Albero Decisionale/ Random Forests**
- **Reti Neutrali, SVM**
- **Reinforcement learning**
- **Algoritmi Genetici**
- **Association rules**
- **Clustering**
- **Network Bayesiani**

Applicazioni Machine Learning

CHURN ANALYSIS	Quali sono le cause per la dipartizione di un cliente? Quali sono i clienti che cambieranno fornitore? Banche/ Assicurazioni/ Telecomunicazioni/ Servizi
PREDICTIVE MAINTENANCE	Quali risorse potrebbero rompersi? Cosa posso fare per prevenire dei danni? Banche/ Telecomunicazioni/ Servizi/ P.A.
NBP & CAMPAIGN FORECASTING	Qual è l'impatto di promozioni e campagne marketing sulle vendite? Perché? Manifattura/Assicurazione / Banche / …
RISK FORECASTING	Qual è il profilo di rischio di un cliente? Quali sono i motivi principali? Banche / Assicurazioni / Biomedico / P. A.
PRODUCT RECOMMENDING	Quali sono i prodotti migliori da vendere ai miei clienti? Banche/ Assicurazioni / Telecomunicazioni / …
FRAUD DETECTION	Quali sono i comportamenti tipicamente fraudolenti? Quali sono i clienti che probabilmente stanno commettendo una frode? Come possiamo anticipare questi comportamenti? Banche/ Assicurazioni

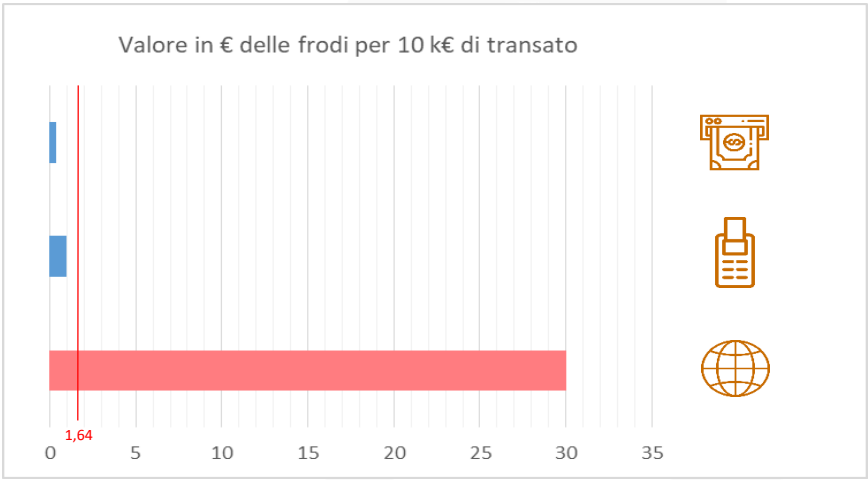
Agenda

- Il punto di partenza
- La soluzione antifrode AS IS
- L'intelligenza artificiale
- **La soluzione antifrode TO BE**
  - **Il contesto**
  - **I driver normativi**
  - **L'architettura applicativa**
  - **Use Case**
  - **Il Monitoring Form**
  - **Lo schema cooperativo**
- L'intelligenza adattiva

La soluzione antifrode TO BE: il contesto

Il rapporto statistico sulle **frodi con le carte di pagamento** 2017 del **Ministero dell'Economia e delle Finanze** mostra come i fenomeni fraudolenti stanno **evolvendo**

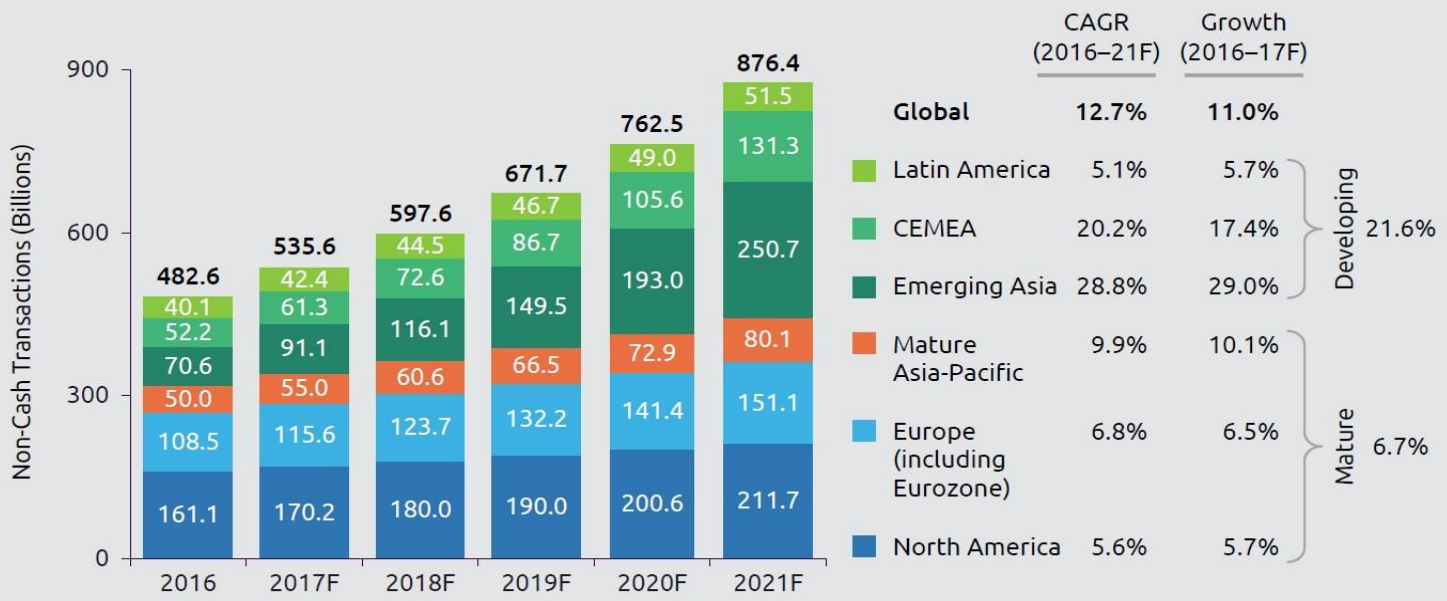
Il **valore delle frodi è sostanzialmente stabile** sui livelli dell'anno precedente (+0,5%), a differenza del **numero** delle stesse che **è aumentato sensibilmente** (+26%), con una **diminuzione del valore medio delle singole transazioni**, che passa da 159€ a 127€. Il totale dei pagamenti genuini, sia in valore sia in numero, è aumentato nel 2016 rispettivamente del 5% e 8%



La soluzione antifrode TO BE: il contesto

Il grafico di seguito riportato mostra la **distribuzione del numero di pagamenti Non-Cash** nel mondo (*)

Figure 1.5 Number of Worldwide Non-Cash Transactions (Billions), by Region, 2016–2021F



> Disruption of the payments market **is accelerating as new technologies take hold** and BigTechs and FinTechs make their presence felt. In particular, **e-wallets are on the rise** and present a **major market opportunity** for **non-traditional payments** providers.

In 2016, **e-wallets accounted for 8.6% of non-cash transactions** (a volume of 41.8 billion), of which 71% were facilitated by **BigTech providers**.

(*) World Payments Report 2018, a cura di Capgemini e BNP PARIBAS, 14° edizione

La soluzione antifrode TO BE: i driver normativi

PSD2 TIMELINE

1 *23 febbraio 2017*
EBA/RTS/2017/02
Final report Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)

2 *24 maggio 2017*
Ref. Ares(2017)2639906
Parere della Commissione europea per emendare gli RTS (EBA/RTS/2017/02)

3 *29 giugno 2017*
EBA/Op/2017/09
Opinion of the European Banking Authority on the European Commission's intention **to partially endorse and amend the EBA's final draft regulatory technical standards on strong customer authentication** and common and secure communication under PSD2

4 *27 novembre 2017*
Pubblicazione da parte della Commissione Europea delle **norme tecniche di regolamentazione** per **l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri**

5 *13 marzo 2018*
Pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea del **REGOLAMENTO DELEGATO** (UE) 2018/389 DELLA COMMISSIONE del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le **norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri** (Testo rilevante ai fini del SEE)

6 *13 giugno 2018*
EBA-Op-2018-04
Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC

7 *18 luglio 2018*
EBA/GL/2018/05
Final report
Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2)

La soluzione antifrode TO BE: i driver normativi

Il **REGOLAMENTO DELEGATO (UE) 2018/389 DELLA COMMISSIONE** del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le **norme tecniche** di regolamentazione per **l'autenticazione forte del cliente** e gli standard aperti di comunicazione comuni e sicuri recita:

CAPO I - DISPOSIZIONI GENERALI

Articolo 1 - Oggetto

Il presente regolamento stabilisce i requisiti cui devono conformarsi i prestatori di servizi di pagamento ai fini dell'attuazione di misure di sicurezza che consentano loro di:

a) applicare la procedura dell'autenticazione forte del cliente conformemente all'articolo 97 della direttiva (UE) 2015/2366;
b) esonerare dall'applicazione dei requisiti di sicurezza dell'autenticazione forte del cliente, a condizioni specifiche e limitate, sulla base del livello di rischio, dell'importo e della frequenza dell'operazione di pagamento e del canale di pagamento utilizzato per l'esecuzione dell'operazione;

Articolo 2 - Obblighi generali di autenticazione

I prestatori di servizi di pagamento dispongono di meccanismi di monitoraggio delle operazioni che consentono loro di rilevare le operazioni di pagamento non autorizzate o fraudolente ai fini dell'attuazione delle misure di sicurezza di cui all'articolo 1, lettere a) e b).

CAPO III ESENZIONI ALL'AUTENTICAZIONE FORTE DEL CLIENTE

Articolo 10 - Informazioni sui conti di pagamento

TIPOLOGIA DI OPERAZIONE

Articolo 11 - Pagamenti senza contatto fisico al punto vendita
Articolo 12 - Terminali incustoditi per le tariffe di trasporto e le tariffe di parcheggio
Articolo 13 - Beneficiari di fiducia
Articolo 14 - Operazioni ricorrenti
Articolo 15 - Bonifici tra conti detenuti dalla stessa persona fisica o giuridica
Articolo 16 - Operazioni di modesta entità
Articolo 17 - Processi e protocolli di pagamento sicuri per le imprese

REGOLE DETERMINISTICHE

Articolo 18 - Analisi dei rischi connessi alle operazioni

SCHEMI DI COMPORTAMENTO

Articolo 19 - Calcolo dei tassi di frode
Articolo 20 - Cessazione delle esenzioni sulla base dell'analisi dei rischi connessi alle operazioni
Articolo 21 - Monitoraggio

AZIONI E SEGNALAZIONI

La soluzione antifrode TO BE: i driver normativi

Il documento EBA-Op-2018-04 **«Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC"** recita:

> **38.** The articles mentioned above are to be read in conjunction with one another, which means that the **PSP applying SCA** is the PSP that **issues the personalised security credentials**. It is consequently also the same provider that **decides whether or not to apply an exemption** in the context of AIS and PIS. The ASPSP may, however, choose to contract with other providers such as wallet providers or PISPs and AISPs for them to conduct SCA on the ASPSP's behalf and determine the liability between them. The EBA also notes that a number of **governmental** (national) **agreements** on universal sets of **personalised security credentials** that can be used by PSUs with multiple PSPs already exist in some Member States.
>
> **40.** With Regard to the use of the exemptions under Articles 10 to 18 of the RTS on SCA and CSC, the EBA hereby clarifies that **payees can never decide whether or not to use an exemption**. Table 2 provides an overview of whether or the payer's PSP (issuer) and the payee's PSP (acquirer) can decide on each of the exemptions set out under Articles 10 to 18.

Table 2. Summary table on who may apply an exemption

RTS article	Exemption	Payer's PSP	Payee's PSP	
			Credit transfers	Cards
Access to information	Access to payment account information	Yes	N/A	N/A
Article 11	Contactless payments at POS	Yes	No	Yes*
Article 12	Unattended terminal for transport and parking	Yes	No	Yes*
Article 13	Trusted beneficiaries	Yes	No	No
Article 14	Recurring transactions	Yes	No	Yes*
Article 15	Credit transfers to self	Yes	No	N/A
Article 16	Low-value transactions	Yes	No	Yes*
Article 17	Secure corporate payment processes and protocols	Yes	No	N/A
Article 18	Transaction risk analysis	Yes	No	Yes*

*The payer's PSP always makes the ultimate decision on whether or not to accept or apply an exemption; the payer's PSP may wish to revert to applying SCA to execute the transaction if technically feasible or decline the initiation of the transaction.

La soluzione antifrode TO BE: l'architettura applicativa

La soluzione **Fraud Protect** rappresenta un asset strategico che è inserito nel percorso evolutivo delle soluzioni e piattaforme applicative offerte da TAS per il mercato della Monetica e dei Sistemi di Pagamento. Gli investimenti effettuati da TAS per Fraud Protect prendono le mosse dalla **PSD2**, seguendone il paradigma che favorisce la **convergenza tra le aree della Monetica e dei Pagamenti**.

Fraud Protect elabora le transazioni che addebitano una carta di pagamento oppure un conto corrente, qualunque sia il canale di origine:

- **Electronic Banking (home banking, APP, wallet, ecc.);**
- **ATM, dell'Istituto e di altri;**
- **POS, fisici e virtuali.**

Il modulo di **SCA Exemption** ha il compito di stabilire se la transazione di pagamento disposta dal cliente può essere eseguita in modalità **frictionless** oppure necessita di una **SCA**.
Lavora in modalità **real-time** ed applica la **Transaction Risk Analysis**.

Il Modulo di **Prevention**, in modalità **real-time**, applica regole di controllo e verifica specifiche blacklist/whitelist restituendo un esito:

- **KO**, la transazione non viene autorizzata e lo strumento di pagamento ordinante viene inserito in una blacklist
- **OK**, la transazione viene autorizzata

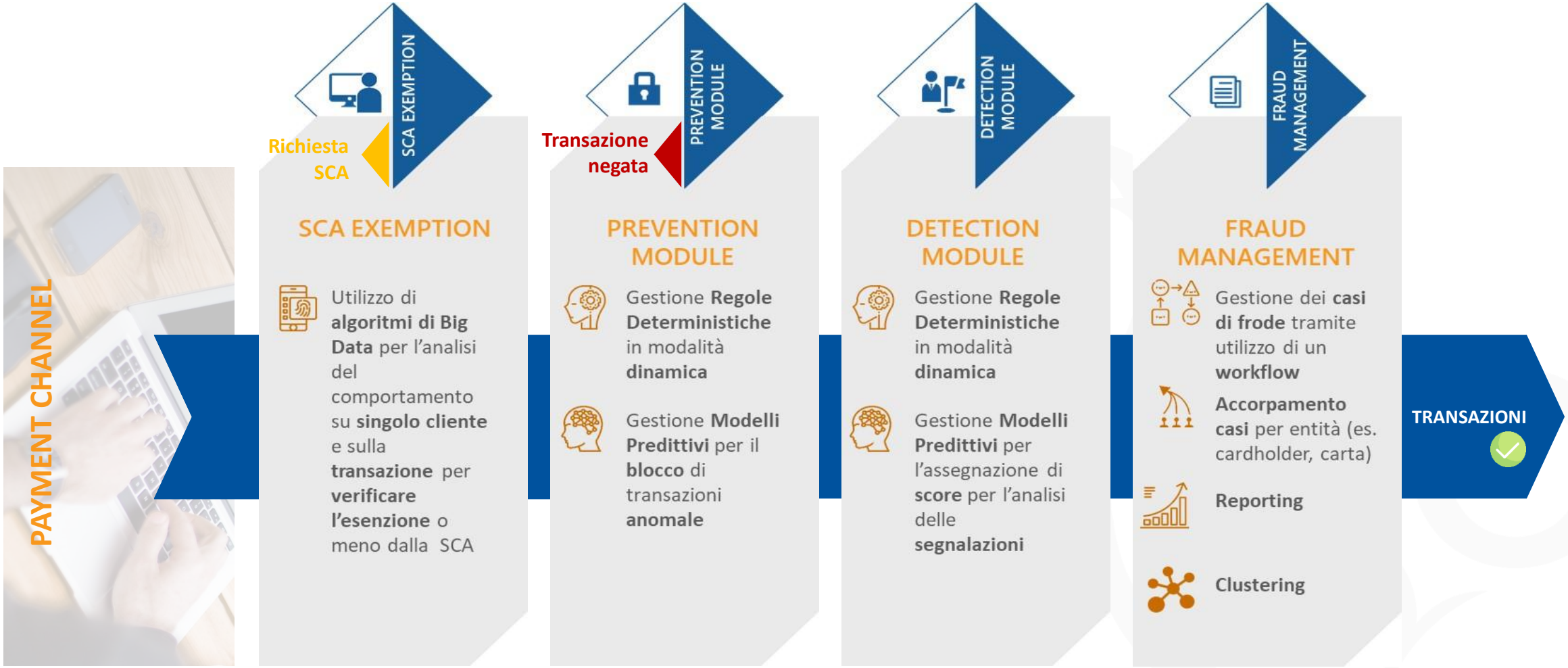
Utilizza modelli predittivi specializzati.

Il modulo di **Detection**, in modalità **near real-time**, elabora le transazioni autorizzate e, nel caso in cui la transazione violi una regola di monitoraggio, genera una **segnalazione**. Utilizza modelli predittivi specializzati.

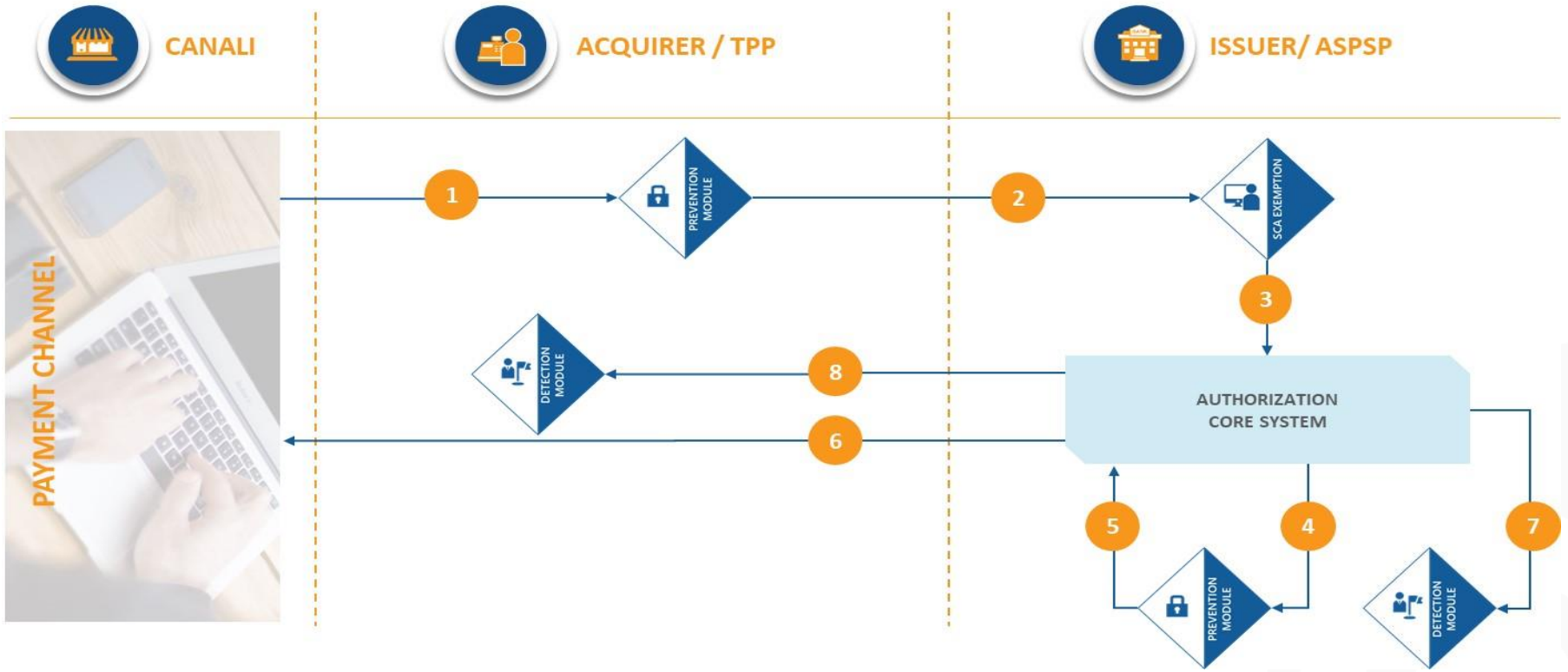
La **segnalazione** viene presa in carico dalla struttura organizzativa preposta al monitoraggio e, dopo le verifiche del caso, la transazione viene **chiusa in frode** o Le attività dell'operatore sono instradate da un **workflow**.
Sono disponibili funzioni di **reporting** e strumenti di analisi basati sul **clustering**

La soluzione antifrode TO BE: l'architettura applicativa

I moduli di **Fraud Protect** analizzano la transazione di pagamento nel suo ciclo di vita per stabilire se può essere esentata dalla SCA, se deve essere bloccata perché fraudolenta, se deve essere analizzata perché sospetta.

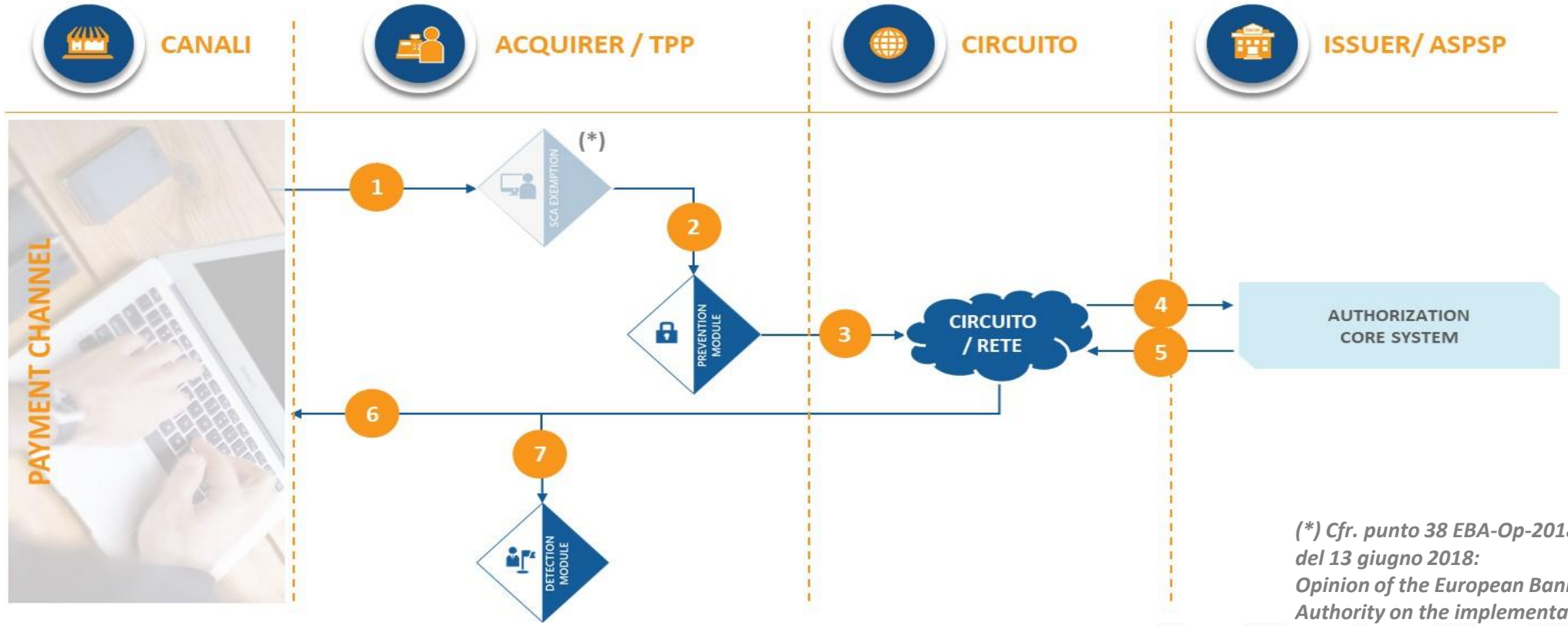


La soluzione antifrode TO BE: Use Case OK – Fraud Protect installato su Acquirer e Issuer (Acquirer ≡ Issuer)



1. La **richiesta di pagamento** è raccolta dall'Acquirer/TPP
2. Il componente di **Prevention/Acquirer** effettua le valutazioni per dare seguito alla richiesta o declinarla. In caso positivo, la **richiesta** è **inoltrata verso l'Issuer/ASPSP**
3. L'Issuer/ASPSP valuta se la transazione può essere **esentata dalla SCA** e in caso affermativo la inoltra verso il verticale per l'autorizzazione (es. disponibilità fondi)
4. **Contestualmente** all'autorizzazione (real time) è attivato il modulo di **Prevention/Issuer** per valutare se la transazione è genuina oppure in frode.
5. Nel caso in cui la **transazione sia stata valutata come genuina** viene addebitato il rapporto del cliente
6. Viene notificato al cliente l'**avvenuto pagamento**
7. La transazione di pagamento alimenta il modulo di **Detection/Issuer** che su un **monitoring form segnala le operazioni sospette** agli specialisti del centro antifrode
8. La transazione viene analizzata dal componente di **Detection/Acquirer** e, se sospetta, viene **segnalata sul monitoring form**.

La soluzione antifrode TO BE: Use Case OK - Fraud Protect installato su Acquirer e strumento di pagamento di terzi

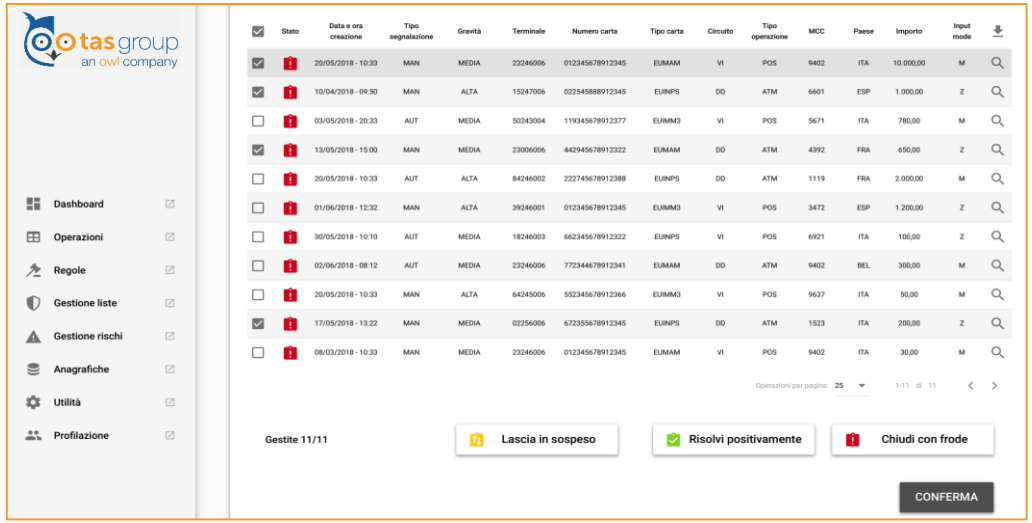


(*) Cfr. punto 38 EBA-Op-2018-04 del 13 giugno 2018: Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC

1. La **richiesta di pagamento** è raccolta dall'Acquirer/TPP che valuta (opzionale) se la transazione può essere **esentata dalla SCA**
2. Il componente di **Prevention/Acquirer** effettua le valutazioni per dare seguito alla richiesta o declinarla
3. Nel caso in cui la richiesta non venga bloccata dal Prevention/Acquirer, la **richiesta** è **inoltrata verso la rete**
4. La rete inoltra la richiesta verso l'Issuer per verificare la disponibilità dei fondi
5. L'Issuer fornisce riscontro alla rete
6. Viene notificato al cliente l'**avvenuto pagamento**
7. La transazione di pagamento alimenta il modulo di **Detection/Acquirer** che su un **monitoring form segnala le operazioni sospette** agli specialisti del centro antifrode

La soluzione antifrode TO BE: il monitoring form

Tutte le **transazioni di pagamento**, qualunque sia il canale con il quale sono state acquisite, sono visualizzate su un **monitoring form** generalizzato.



Alcuni **attributi caratteristici** possono essere disponibili per delle transazioni e non per altre, a seconda del canale di accettazione e dello strumento di pagamento utilizzati.

Criteri di ricerca dinamicamente configurabili consentono di filtrare le transazioni secondo le preferenze degli utenti.

Funzioni di **case consolidation** consentono di raggruppare i casi secondo più livelli abilitando così distinti **coni di visibilità**.

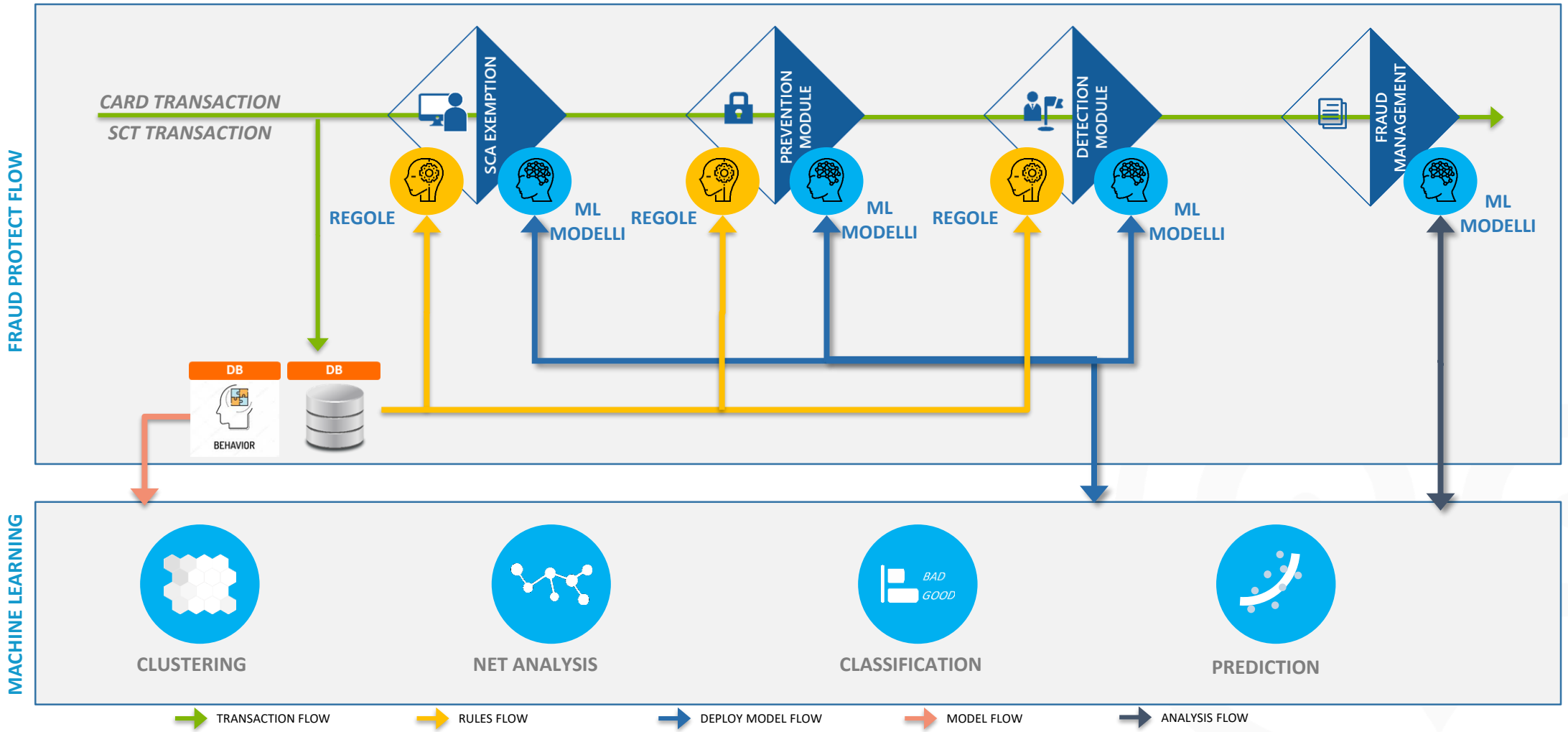
Dashboard dedicati consentono di avere sotto controllo in real time l'andamento dei fenomeni di frode e di tentata frode.

I **totalizzatori di stato** per le attività di lavorazione delle segnalazioni è uno strumento indispensabile per la distribuzione dei carichi di lavoro.

Sono gestiti **profili autorizzativi e workflow** di lavorazione.

La soluzione antifrode TO BE: lo schema cooperativo

La soluzione **Fraud Protect** si basa su uno **schema cooperativo tra regole deterministiche e modelli predittivi** che utilizzano dati elementari e dati comportamentali per aumentare precisione, capacità e rapidità di individuazione delle transazioni in frode



Agenda

- Il punto di partenza
- La soluzione antifrode AS IS
- L'intelligenza artificiale
- La soluzione antifrode TO BE
- **L'intelligenza adattiva**
  - **Apprendimento Continuo e Modelli Predittivi**
  - **Il valore dei Modelli Predittivi**
  - **Modelli Predittivi e Transaction Monitoring**

L’intelligenza adattiva: Apprendimento Continuo e Modelli Predittivi

TRANSACTIONS

CARD TRANSACTIONS

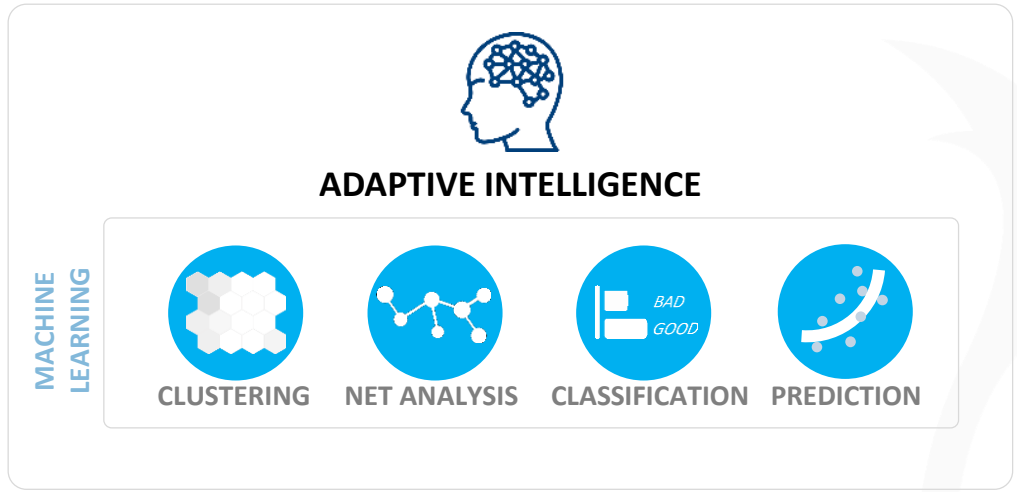
SCT TRANSACTIONS

INTERNAL DATA

HISTORY OF TRANSACTIONS

HISTORY OF RISK RESULTS & CUSTOMER BEHAVIORS

- Frodi in **continua e costante evoluzione**
- **Intelligenza Adattiva** per imparare e **anticipare schemi di Comportamento** e probabili **situazioni di Rischio**
- Introduzione di Modelli Predittivi per **Fraud Detection** e **Risk Analytics**, nel **rispetto delle disposizioni PSD2**



MACHINE LEARNING nel ciclo di **TRANSACTION MONITORING**

Potenziare

il Sistema a Regole (**DETERMINISTICO** e approccio **REATTIVO**)

con

MODELLI PREDITTIVI che agiscono in modo **PREVENTIVO**

MODELS

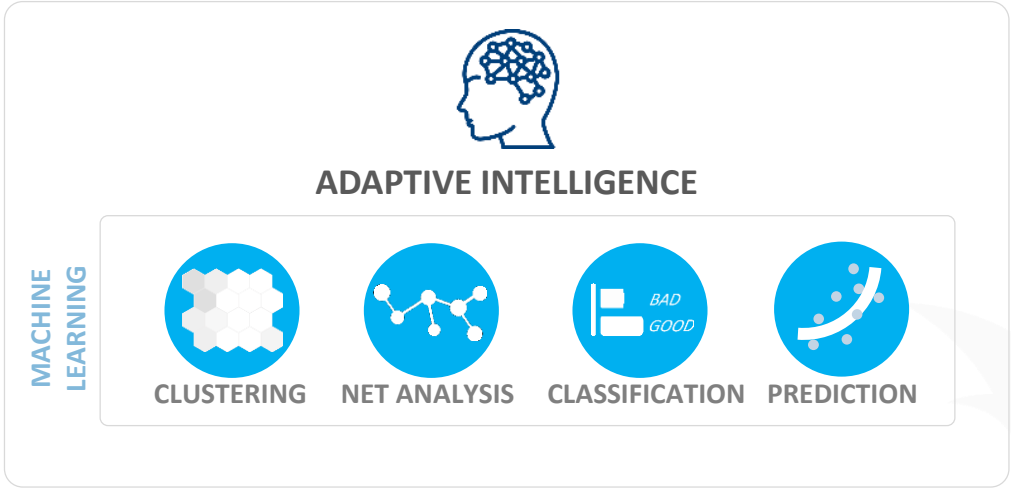
CUSTOMER RISK BEHAVIORS

RISK OF CARD TRANSACTIONS

RISK OF SCT TRANSACTIONS

HISTORY OF RISK RESULTS & CUSTOMER BEHAVIORS

L’intelligenza adattiva: il valore dei Modelli Predittivi



Adaptive & Continuous Learning

I Modelli sono naturalmente adattivi, in grado di intercettare le continue variazioni negli **schemi di frode** che il tradizionale sistema a regole non è in grado di catturare.

I nuovi pattern di frode identificati possono così **aggiornare il sistema a regole**.

Model Calibration

Riduzione drastica della necessità di calibrare i Modelli di Frode **manualmente**.

E’ possibile **programmare la calibrazione dei modelli** in funzione dei cambiamenti dei behaviors legati alle frodi.

Explainable Models

Modelli sofisticati e tracciabili basati su **Reti Neurali** in grado di fornire una **analisi quantitativa e qualitativa delle dinamiche fraudolente** attraverso l’interpretazione degli elementi del tracciato delle transazioni.

L’intelligenza adattiva: Modelli Predittivi e Transaction Monitoring

FRAUD MANAGEMENT

RISK ANALYTICS

Agiscono **in fase di Transaction Monitoring**.

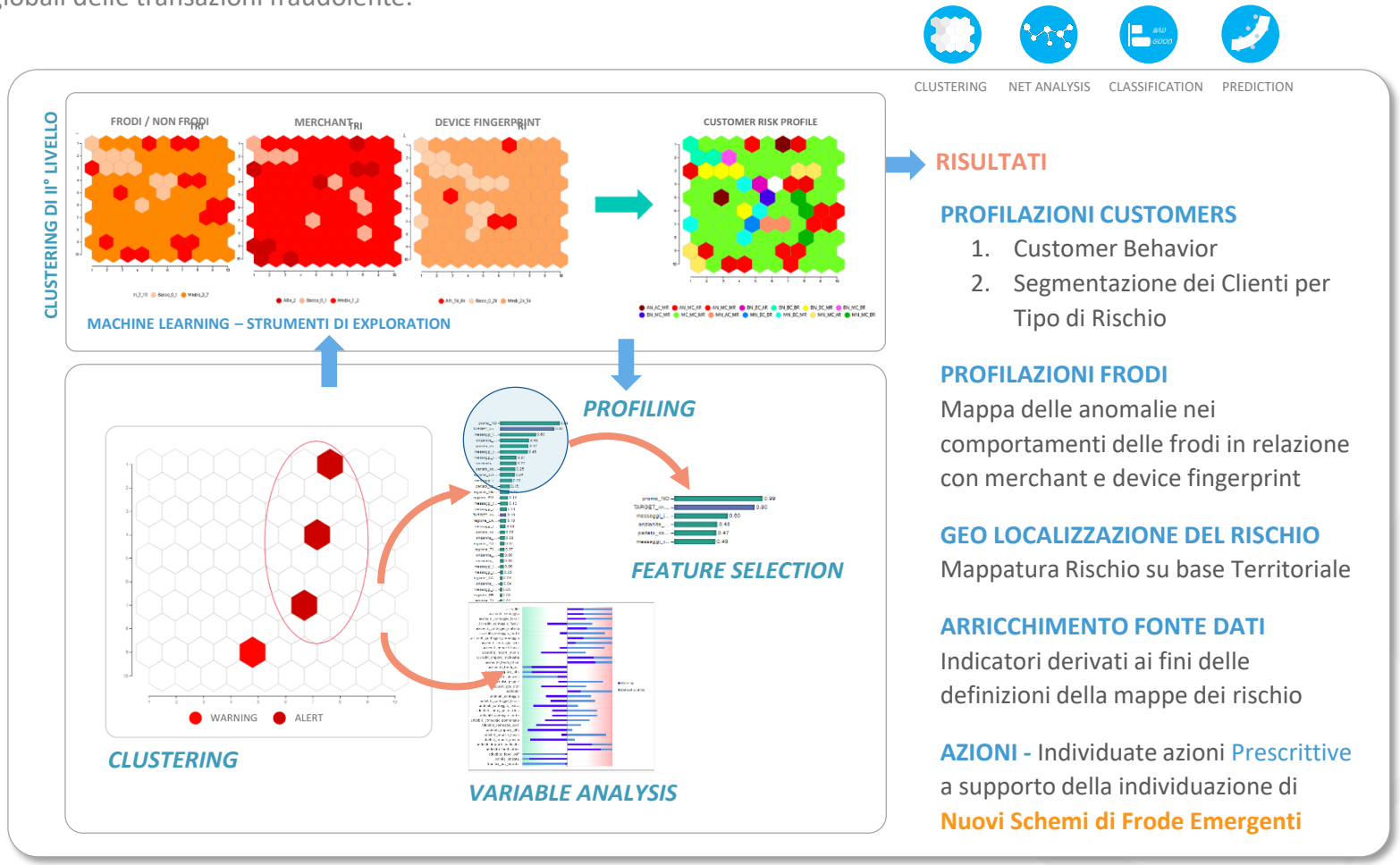
Sono algoritmi che sfruttano tecniche avanzate di **Clustering** e **Net Analysis** in grado di determinare **relazioni nascoste, outliers e nuovi patterns**.

In questa fase i Modelli prodotti sono molto utili per fini esplorativi per determinare **nuovi schemi di frode emergenti**.

RISK ANALYTICS – Ciclo di Apprendimento, Esplorazione, Modelli, Risultati

I Modelli determinano l’appartenenza di un soggetto ad un profilo comportamentale omogeneo comune a più soggetti.

- La **Customer Behaviors in logica “verticale”** è estesa **ad una visione “orizzontale”**, relativa a dinamiche comportamentali globali delle transazioni fraudolente.



L'intelligenza adattiva: Modelli Predittivi e Transaction Monitoring

BEHAVIOR PROFILE MODELS

Agiscono **in tempo reale**.

Sono Modelli in grado di tracciare il **comportamento** di ogni **singolo individuo**.

Sono gli algoritmi di ML più adatti per la copertura richiesta dalla **Normativa Europea in tema di SCA.**

In questa fase un RISCHIO elevato determina una **richiesta di SCA**

MODELLI PER BEHAVIORS PROFILE

Le **tecniche di profiling** basate su Machine Learning sono in grado di definire il **comportamento tipico di ogni individuo** nei termini delle componenti del tracciato delle proprie transazioni.

La risposta in tempo reale sulla transazione da analizzare soddisfa i requisiti previsti dalla Normativa Europea in tema di SCA.

Questi Modelli sono basati sui fattori:

- Distribuzioni degli importi
- Frequenza di transazioni in un intervallo
- Distribuzioni fasce orarie
- Distribuzione Merchant
- Distribuzione canali
- Device fingerprinting

Gli algoritmi di questa fase determinano un LIVELLO di RISCHIO, sulla base di **anomalie** e **distanze** riscontrate dal comportamento tipico del singolo individuo.

Come agiscono: i**n tempo reale**, per ogni nuova transazione:

- si confronta la transazione con il profilo conosciuto
- si calcolano coefficienti di distanza da questo profilo, che se si discostano da un certo valore soglia definito, determinano ALERT che possono scatenare una RICHIESTA di SCA.

Esempio

Transazione in ingresso:

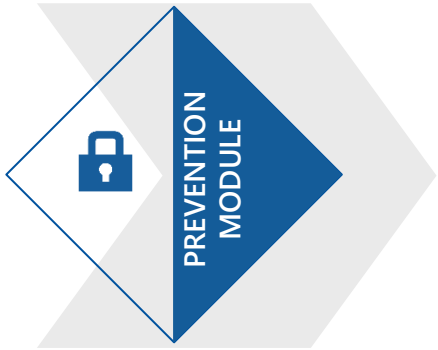
- Importo: 12 Euro
- Ora: 23.50
- Merchants: Clothing
- Country: Malesia
- Channel: INTERNET

Profilo:

- 10 < importi < 50
- 2 Transazioni Mensili
- Fasce orarie: 09-12, 18-20
- Merchants: Clothing (10%), Books (60%), Computers (30%)
- Country: Italia
- Channel: POS (95%), INTERNET (5%)

Esito Matching: **0.96**
Richiesta di SCA

L’intelligenza adattiva: Modelli Predittivi e Transaction Monitoring



FRAUD PREVENTION MODELS

Agiscono **in tempo reale**. Classificano ogni transazione come “**frode**” o “**non frode**”.

In questa fase i livelli di **RISCHIO** possono determinare **il BLOCCO della transazione** se superano una soglia molto rilevante.

FRAUD PREVENTION MODELS

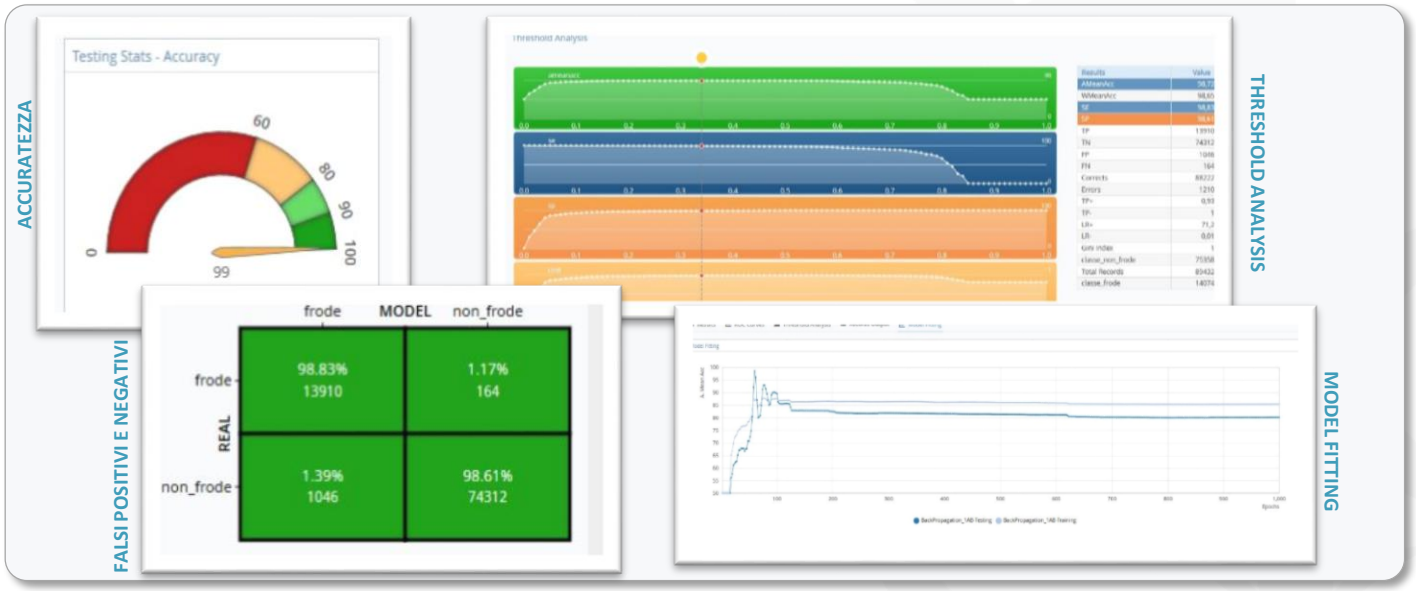
Hanno la capacità di classificare ogni transazione come “**frode**” o “**non frode**”, affrontano efficacemente tali problemi al fine di ottimizzare ad es. la riduzione dei “**Falsi Positivi**”

Un insieme di differenti **Modelli Predittivi** concorre alla **Classificazione** e assegnazione **Real Time** di uno **SCORING** alla singola **Transazione**, considerati anche gli esiti della **Fase di SCA EXEMPTION**.

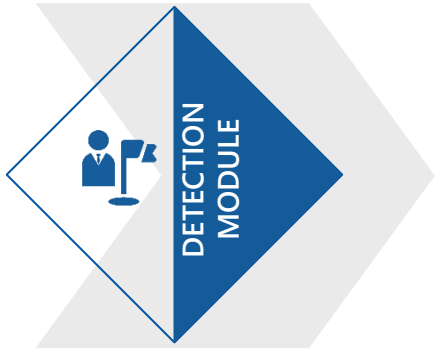
Possono determinare il **BLOCCO della TRANSAZIONE** in presenza di **SCORING prossimo al 100%**.

Highlights

- Modelli adeguati per risposte **rapide, precise**, **sicure** per la fase di **Prevention**.
- La **Normativa** definisce le soglie ammesse nei termini **di tipo di transazione** e **importi.**
- La **calibrazione dei modelli** consente di soddisfare i requisiti richiesti.



L'intelligenza adattiva: Modelli Predittivi e Transaction Monitoring



FRAUD DETECTION MODELS

Agiscono **in near real-time**. Classificano ogni transazione come "**frode**" o "**non frode**" analizzando ogni elemento utile **della storia delle transazioni**.

VERTICAL MODELS

Agiscono **in near real-time**. Sono Modelli "**specializzati**". Ad esempio: Transazioni "Card Not Present" sul Channel Internet

I livelli di **RISCHIO** alimentano Il sistema di **segnalazioni**. Possono determinare aggiornamenti sia dei **Profili** che delle **white e black list.**

FRAUD DETECTION MODELS

Classificano ogni transazione come "**frode**" o "**non frode**" analizzando ogni elemento utile della **storia delle transazioni**.

Si caratterizzano per la capacità di analizzare:

- La storia del Profilo dell'individuo
- La storia delle Transazioni recenti (es. detection tempestivo di casi di sciame di transazioni fraudolente)
- Altre misure disponibili o definite insieme all'Istituto di Credito

VERTICAL MODELS

Utilizzando modelli Supervisionati, non Supervisionati e Behavior Profiles, è possibile costruire analytics e nuovi modelli "**specializzati**".

Ad esempio:

- Transazioni "**Card Not Present**" **sul Channel Internet**
- Transazioni per **POS**
- Transazioni per **tipo di carta di pagamento**
- Profilo **SCT per transazioni in ingresso e in uscita**

Modelli di questo tipo sono generalmente più robusti e statisticamente consistenti poiché specializzati su tracciati specifici di frode.

L’intelligenza adattiva: Modelli Predittivi e Transaction Monitoring

MACHINE LEARNING nel ciclo di **TRANSACTION MONITORING**

In conformità alla Normativa

Potenziare il Sistema a Regole (**DETERMINISTICO** e con approccio **REATTIVO**) con

MODELLI PREDITTIVI che agiscono in modo **PREVENTIVO**

SCA EXEMPTION

BEHAVIOR PROFILE MODELS

Agiscono **in tempo reale**.

Sono Modelli in grado di tracciare il **comportamento** di ogni **singolo individuo**.

Sono gli algoritmi di ML più adatti per la copertura richiesta dalla **Normativa Europea in tema di SCA.**

In questa fase un **RISCHIO** elevato determina una **richiesta di SCA**

PREVENTION MODULE

FRAUD PREVENTION MODELS

Agiscono **in tempo reale**. Classificano ogni transazione come “**frode**” o “**non frode**”.

In questa fase i livelli di **RISCHIO** possono determinare **il BLOCCO della transazione** se superano una soglia molto rilevante.

DETECTION MODULE

FRAUD DETECTION MODELS

Agiscono **in near real-time**. Classificano ogni transazione come “**frode**” o “**non frode**” analizzando ogni elemento utile della **storia delle transazioni**.

VERTICAL MODELS

Agiscono **in near real-time**. Sono Modelli “**specializzati**”. Ad esempio: Transazioni “Card Not Present” sul Channel Internet.

I livelli di **RISCHIO** alimentano Il sistema di **segnalazioni**. Possono determinare aggiornamenti sia dei **Profili** che delle **white e black list.**

FRAUD MANAGEMENT

RISK ANALYTICS

Agiscono **in fase di Transaction Monitoring**

Sono algoritmi che sfruttano tecniche avanzate di **Clustering** e **Net Analysis** in grado di determinare **relazioni nascoste, outliers e nuovi patterns**.

In questa fase i Modelli prodotti sono molto utili per fini esplorativi per determinare **nuovi schemi di frode emergenti**.

Questions & Answers

tas group
an owl company

CONTATTI

www.tasgroup.it

soluzioni@tasgroup.it

Grazie!

IDC FINTECH RANKINGS 2018 TOP100

CIO Review 50 MOST PROMISING FINTECH SOLUTION PROVIDERS - 2018