CELENT

RENDERE OPERATIVA LA PREVENZIONE DELLE FRODI SU IBM Z16

Come ridurre le perdite nel settore bancario, delle carte e dei pagamenti

Neil Katkov

5 aprile 2022

Questo report è stato commissionato da IBM, che ha incaricato Celent di ideare e svolgere uno studio per suo conto. L'analisi e le conclusioni sono esclusivamente di Celent: IBM non ha avuto alcun controllo editoriale sui contenuti del report.

INDICE

Riassunto esecutivo **3**

Il costo elevato delle frodi nel settore bancario, delle carte e dei pagamenti **4**

Un aiuto in arrivo: i modelli di rilevamento delle frodi basati sull'apprendimento profondo 5

Limiti del rilevamento delle frodi allo stato attuale **7**

Riduzione delle perdite dovute alle frodi mediante l'inferenza AI su mainframe **9**

Eliminazione dei falsi positivi per limitare l'abbandono dei clienti **11**

Il percorso che ci aspetta **13**

Affidati alle competenze di Celent **14**

Sostegno agli istituti finanziari 14

Assistenza per i fornitori 14

Ricerche Celent correlate **15**

RIASSUNTO ESECUTIVO

I progressi dell'intelligenza artificiale (AI), come l'apprendimento profondo, stanno rendendo possibili dei miglioramenti significativi nel rilevamento delle frodi. Tuttavia, le grandi banche e i processori di pagamento che utilizzano i modelli AI spesso li eseguono solo su una piccola parte delle transazioni, a causa dei limiti legati a velocità di elaborazione e latenza dei propri sistemi di rilevamento delle frodi. Di conseguenza, molte transazioni fraudolente non vengono monitorate e rilevate.

IBM Integrated Accelerator for AI, che fa parte del nuovo processore mainframe Telum di IBM, è studiato per eseguire inferenze per carichi di lavoro in tempo reale su scala e a bassa latenza. Il chip è progettato per supportare il rilevamento delle frodi in tempo reale anche negli ambienti di elaborazione con volumi elevati, quali banche, carte e pagamenti.

Per aiutare le banche e i processori di pagamento a comprendere il valore potenziale di questa innovazione nella lotta alle frodi, Celent ha stilato delle stime sulla riduzione potenziale delle perdite causate da frodi qualora queste realtà applicassero l'inferenza AI al 100% delle proprie transazioni.

Ecco alcuni vantaggi quantificabili del rilevamento delle frodi basato sull'AI eseguito sui mainframe di IBM z16:

Riduzione delle perdite settoriali dovute a frodi di…		Riduzione delle perdite bancarie di…		Riduzione delle transazioni con carta rifiutate del…
Stati Uniti	A livello globale	Banca USA classe 1	Banca USA classe 2	
5,6 cent ogni 100 dollari	2,0 cent ogni 100 dollari	105 milioni di dollari	18 milioni di dollari	46%

Celent stima che l'applicazione di modelli di inferenza avanzati a tutte le transazioni bancarie, delle carte e di pagamento sui mainframe IBM zSystems potrebbe potenzialmente ridurre le perdite dovute a frodi di 161 miliardi di dollari a livello globale. In questo caso, le banche potrebbero evitare perdite per 140 miliardi di dollari, mentre per le carte e i pagamenti la cifra si attesta a 21 miliardi di dollari. Solo negli Stati Uniti, le perdite dovute a frodi bancarie potrebbero essere ridotte di 44 miliardi di dollari e di 6 miliardi di dollari per le carte e i pagamenti.

Certo, l'adozione dell'inferenza AI nel mainframe per le operazioni antifrode incontra alcuni ostacoli, quali i problemi di governance dei modelli, i costi legati alla sostituzione totale dei sistemi ("rip and replace"), la disponibilità di risorse interne di data science e la dimostrazione del caso di business.

Tuttavia, l'esecuzione diretta di modelli AI avanzati nell'ambiente mainframe rappresenta una forte innovazione in un settore in cui si stima che il 70% del valore delle transazioni globali avvenga su mainframe IBM. Il rilevamento delle frodi è un importante caso di utilizzo di questa nuova funzionalità IBM, con vantaggi dimostrabili sia per i profitti che per l'esperienza del cliente.

IL COSTO ELEVATO DELLE FRODI NEL SETTORE BANCARIO, DELLE CARTE E DEI PAGAMENTI

Si stima che nel 2021 le frodi abbiano generato perdite per 385 miliardi di dollari a livello globale nel settore bancario, delle carte e dei pagamenti.

Le frodi bancarie e nei pagamenti assumono molteplici forme nei settori retail e aziendale. Le frodi che colpiscono le banche includono l'acquisizione fraudolenta dei conti (ATO, Account Takeover), le frodi sui pagamenti push autorizzati (APP, Authorized Push Payments), le frodi sulle fatture e un'ampia gamma di schemi di phishing e ingegneria sociale progettati per attivare trasferimenti illeciti di denaro o per ottenere le credenziali dei conti correnti. Anche le carte e i pagamenti sono vulnerabili all'acquisizione di conti e al phishing, oltre che a schemi specifici come le frodi mediante identità sintetica o di tipo "bust-out" e "man-in-the-middle".

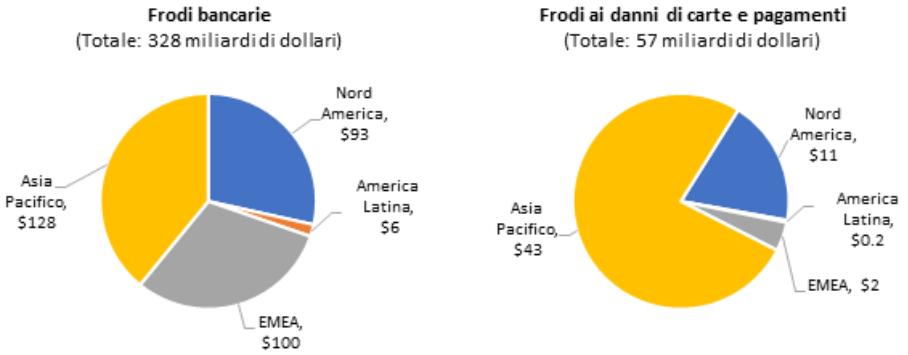
Figura 1: Schemi comuni di frode ai danni di conti bancari e carte

Frodi bancarie		Frodi ai danni delle carte	
	Account takeover		Frode ai danni delle applicazioni
	Frode ai danni di APP		Frode di tipo "bust-out"
	Frode su assegni		Man-in-the-middle
	Frode su fattura		Phishing
	Ingegneria sociale		Identità sintetica

Fonte: Celent

Queste e altre frodi ai danni di conti bancari, carte e pagamenti rappresentano una grave preoccupazione per gli istituti finanziari. Celent stima che negli Stati Uniti le perdite annuali per frode siano in media di 209 milioni di dollari per una banca di classe 1 (totale attivo superiore a 100 miliardi di dollari) e di 35 milioni di dollari per una banca di classe 2 (totale attivo fra 50 e 100 miliardi di dollari). Su scala settoriale, nel 2021 le banche hanno subito perdite dovute a frodi per 328 miliardi di dollari a livello globale. I settori delle carte e dei pagamenti hanno accumulato ulteriori 57 miliardi di dollari in perdite. Complessivamente, nel 2021 le frodi hanno generato perdite stimate per 385 miliardi di dollari nel settore bancario, delle carte e dei pagamenti in tutto il mondo.

Figura 2: Perdite da frode nel settore bancario, delle carte e dei pagamenti nel 2021



Fonte: stime Celent basate sui dati delle transazioni delle BRI e sui dati delle frodi delle banche centrali.
Nota bene: le frodi bancarie comprendono bonifici, addebiti diretti e assegni. Le frodi ai danni di carte e pagamenti colpiscono carte di credito e di debito, pagamenti elettronici e altri tipi di transazioni.

Benché le banche e i processori di pagamento siano impegnati da decenni nel contenimento delle frodi mediante sistemi di rilevamento e soluzioni di sicurezza basate su chip per le carte, le perdite hanno comunque continuato a salire. I truffatori sono sempre un passo avanti e sviluppano continuamente nuove tecnologie e schemi di ingegneria sociale.

La pandemia da COVID-19 ha fatto aumentare ulteriormente il numero delle frodi. Per le banche, cause importanti sono state il phishing e gli schemi di ingegneria sociale, capaci di sfruttare le ansie e le esigenze mediche legate alla pandemia. Per quanto riguarda le transazioni con carta, la pandemia ha portato a una diffusione dei servizi bancari digitali e dell'e-commerce, poiché i consumatori hanno evitato le transazioni in filiale e nei negozi. Dato che le transazioni di tipo card-not-present (CNP) rappresentano la maggior parte delle frodi legate alle carte (circa il 65%), questo tipo di frode si è diffuso ulteriormente.

Un aiuto in arrivo: i modelli di rilevamento delle frodi basati sull'apprendimento profondo

I progressi dell'intelligenza artificiale, quali l'apprendimento profondo, offrono alle banche gli strumenti per combattere le frodi in modo molto più efficace, poiché analizzano i dati su larga scala per trovare modelli che suggeriscono il verificarsi di attività illecite. Questi strumenti comprendono delle tipologie inedite.

L'apprendimento profondo è un tipo di modello di apprendimento automatico basato su una rete neurale profonda (DNN, Deep Neural Network). Una rete DNN è costituita da nodi computazionali, o neuroni, che utilizzano pesi progressivi per rafforzare le connessioni tra i nodi. I nodi sono disposti su più livelli e creano una rete "profonda" che aumenta la capacità e il tasso di apprendimento del modello. I modelli di apprendimento profondo vengono addestrati su dati pre-esistenti, quali ad esempio lo storico delle transazioni nel caso dei modelli di rilevamento delle frodi. Il modello addestrato viene quindi eseguito su dati in tempo reale, ad esempio una transazione in corso, per generare un risultato (detto anche "inferenza"). Nel caso dei modelli di rilevamento delle frodi, l'inferenza è in genere un punteggio che esprime la probabilità che la transazione sia fraudolenta.

Sulla base di dibattiti e ricerche di settore, Celent stima che l'inferenza AI basata su modelli di apprendimento profondo possa aumentare la precisione nel rilevamento delle frodi del 60% rispetto ai modelli attuali.

Il potenziale dell'inferenza per migliorare i tassi di rilevamento delle frodi è tuttavia drasticamente limitato dal fatto che negli ambienti mainframe a volumi elevati questi modelli sono spesso eseguiti solo su una frazione delle transazioni (meno del 10%) a causa di problematiche legate a latenza, costi e contrasti con i clienti. Questo significa che circa il 90% delle frodi potenzialmente prevenibili continua a non essere individuato. Ciò limita fortemente la capacità delle banche di approfittare dei progressi dell'AI per recuperare le perdite dovute alle frodi.

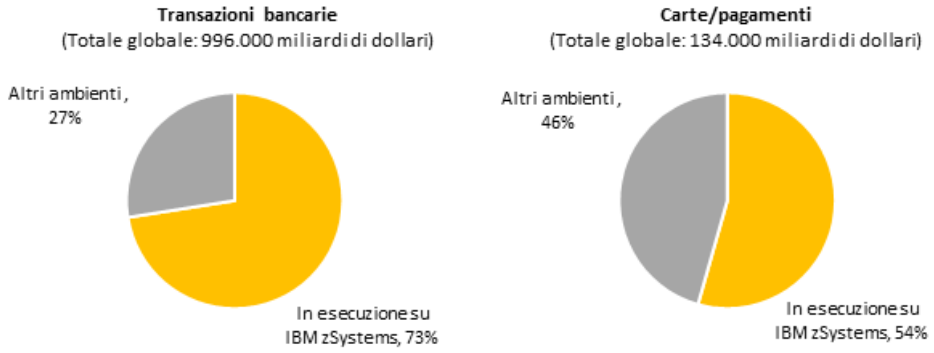
Oggi, tuttavia, gli ostacoli in termini di latenza e di costi che impediscono di elaborare il 100% delle transazioni bancarie e con carta mediante modelli avanzati potrebbero diventare un ricordo lontano. Il nuovo processore IBM z16 Telum contiene un acceleratore AI che, per la prima volta in IBM zSystems, può eseguire modelli AI direttamente sul chip in tempo reale. In questo modo si migliorano esponenzialmente la velocità effettiva e i tempi di risposta, rendendo possibile per la prima volta l'elaborazione di quasi tutte le transazioni mediante modelli di rilevamento delle frodi basati sull'apprendimento profondo.

LIMITI DEL RILEVAMENTO DELLE FRODI ALLO STATO ATTUALE

La tecnologia di rilevamento delle frodi e gli approcci operativi tipici degli ambienti mainframe prevedono l'esecuzione delle frodi su sistemi esterni alla piattaforma su transazioni selezionate e/o in uno scenario post-transazione. Questo limita drasticamente la capacità delle banche e dei processori di pagamento di eseguire modelli AI avanzati su tutte le transazioni.

I sistemi principali di molte grandi banche e società di elaborazione dei pagamenti sono eseguiti su ambienti di elaborazione mainframe. IBM stima che 45 delle 50 banche più importanti a livello globale utilizzano i mainframe IBM zSystems. Anche la maggior parte dei principali processori di carte e di pagamenti è in esecuzione su questa piattaforma. A livello globale, Celent stima che il 70% del valore delle transazioni di banche, carte e pagamenti sia in esecuzione su ambienti IBM zSystems.

Figura 3: Valore delle transazioni di banche, carte e pagamenti su IBM zSystems



Fonte: Celent

La latenza tra i sistemi principali e i sistemi di rilevamento esterni alla piattaforma può essere tollerata per alcune transazioni. Tuttavia, nel caso delle routine di inferenza AI ad alta intensità di dati applicate a transazioni in tempo reale (quali pagamenti in tempo reale, transazioni con carta e transazioni bancarie digitali), la latenza rende irrealizzabile l'esecuzione di tutte le transazioni attraverso una piattaforma di rilevamento AI in ambienti con volumi elevati. Quando le transazioni dei sistemi principali vengono inviate dal mainframe a un sistema di rilevamento esterno alla piattaforma per l'analisi in tempo reale, i tempi di risposta per la ricezione dei risultati del rilevamento variano da 50 a 80 millisecondi, mentre le transazioni rimangono in attesa. Vengono così rallentati i tempi di approvazione delle transazioni, creando potenziali contrasti con i clienti, in particolare nelle transazioni con carta.

In modo più sostanziale, un'elevata latenza può rendere impossibile l'esecuzione di tutte le transazioni attraverso un sistema di rilevamento delle frodi esterno alla piattaforma. La latenza tra il sistema principale e il software di rilevamento può ritardare la ricezione dei risultati del rilevamento da parte del sistema principale al punto che le transazioni in tempo reale si interrompono. Di conseguenza, alcune banche eseguono i modelli di apprendimento profondo per le frodi solo in una fase post-transazione.

Per questo, le banche inviano solo una frazione delle transazioni (meno del 10%) ai propri motori di rilevamento delle frodi in tempo reale. Questo approccio comporta gravi conseguenze. Attualmente, i modelli di apprendimento profondo consentono di ottenere un miglioramento significativo nei tassi di rilevamento: circa il 60%. Tuttavia, le banche non stanno approfittando di tutti i possibili vantaggi, dato che fanno elaborare da questi modelli solo un campione delle transazioni. Non viene quindi rilevata una quota superiore di frodi e aumentano le perdite a esse dovute. Visto che le frodi sono sempre più al centro dell'attenzione per quanto riguarda la conformità nell'ambito dei crimini finanziari, le banche possono incorrere in rischi a livello normativo se non sono in grado di far elaborare tutte le proprie transazioni da un sistema di rilevamento antifrode.

Problemi tradizionali presso una banca USA classe 1

Una banca di classe 1 negli Stati Uniti che gestisce il proprio sistema principale su una piattaforma IBM zSystems ha implementato un sistema di rilevamento delle frodi basato sull'AI ed esterno alla piattaforma. A causa di problemi legati a costi e latenza, la banca fa elaborare al sistema AI solo le transazioni ad alto rischio. Alla maggior parte delle transazioni viene applicato un punteggio basato su regole, approvato per comodità del cliente, e successivamente viene eseguita un'analisi post-transazione. I vantaggi dell'AI sono fortemente limitati dall'impossibilità di eseguire i modelli su tutte le transazioni, il che significa che l'AI non viene utilizzata al massimo delle sue potenzialità.

RIDUZIONE DELLE PERDITE DOVUTE ALLE FRODI MEDIANTE L'INFERENZA AI SU MAINFRAME

IBM ha sviluppato un processore per il proprio computer mainframe IBM z16 dotato di un acceleratore per l'AI progettato per eseguire inferenze avanzate direttamente sul chip e su larga scala. Secondo le stime di Celent, il nuovo processore IBM z16 è in grado di supportare il rilevamento delle frodi basato sull'apprendimento profondo per quasi tutte le transazioni, riducendo potenzialmente di 161 miliardi di dollari le perdite dovute a frodi bancarie, delle carte e dei pagamenti a livello globale.

Gli algoritmi di apprendimento profondo tendono a richiedere più risorse di elaborazione rispetto ai modelli tradizionali di rilevamento delle frodi. Quando le banche implementano l'inferenza AI basata sull'apprendimento profondo per le frodi si trovano ad affrontare delle sfide nella gestione di questi carichi di lavoro mission critical. Se il rilevamento viene eseguito su sistemi esterni alla piattaforma, i tempi di risposta possono raggiungere oltre gli 80 millisecondi, con tassi di velocità effettiva compresi tra le 1.000 e le 1.500 transazioni al secondo ("transactions per second", tps).

A causa di questi limiti di latenza e di velocità effettiva, le banche hanno riscontrato delle interruzioni delle transazioni in attesa dell'esito del rilevamento. Questi e altri problemi portano le banche a elaborare solo una frazione delle transazioni (meno del 10%) mediante i propri motori di rilevamento.

Apprendimento profondo su mainframe

Sulla base di un modello di apprendimento profondo per le frodi ai danni delle carte di credito, 32 chip IBM Telum in esecuzione su un singolo server possono fornire fino a 3,5 milioni di inferenze al secondo con un tempo di risposta medio di 1,2 millisecondi.

Fonte: Microbenchmark IBM, agosto 2021

AVVERTENZA: i risultati delle prestazioni sono ricavati da test interni di IBM.

IBM ha sviluppato un acceleratore per il proprio computer mainframe IBM z16 in grado di eseguire modelli di inferenza AI direttamente sul chip. Secondo IBM, la velocità effettiva e i miglioramenti derivanti dall'esecuzione di modelli AI sul mainframe sono sufficienti a supportare l'analisi delle frodi in tempo reale di praticamente tutte le transazioni, anche negli ambienti di elaborazione a volume elevato di banche, carte o pagamenti.

Inoltre, questo è possibile senza quasi alcun impatto sui tempi di elaborazione delle transazioni. IBM sostiene che IBM Integrated Accelerator for AI, che fa parte del suo nuovo processore Telum, può eseguire modelli AI sul mainframe con un tempo di risposta velocissimo di soli 1,2 millisecondi per ogni richiesta di inferenza. Nel caso specifico del rilevamento delle frodi ai danni delle carte, i primi benchmark indicano che una configurazione di 32 chip Telum può supportare fino a 3,5 milioni di inferenze al secondo.

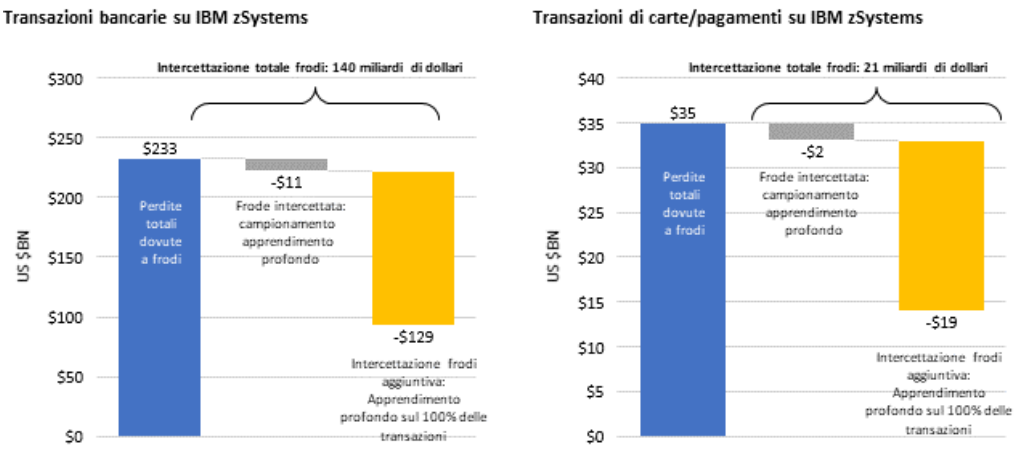
Si tratta di una scala sufficiente a supportare anche i picchi nei flussi delle transazioni, consentendo alle banche e ai processori di pagamento di eseguire praticamente tutte le transazioni attraverso modelli di apprendimento profondo.

Le banche e i processori di carte e pagamenti possono sfruttare appieno il potenziale delle tecnologie di inferenza moderne eseguendo modelli avanzati su tutte le transazioni. Celent stima che l'applicazione di modelli di inferenza avanzati a tutte le transazioni ridurrebbe potenzialmente le perdite per frode di 2,0 centesimi per ogni 100 dollari di transazioni a livello globale (2,0 punti base).

Negli Stati Uniti, dove i tassi delle frodi sono più alti della media mondiale (9,3 centesimi di dollaro per ogni 100 dollari rispetto ai 3,7 centesimi a livello globale), le perdite legate alle frodi potrebbero essere ridotte di 5,6 centesimi di dollaro per ogni 100 dollari. Equivale a un risparmio per la banca di 1,33 dollari per una transazione media di 2.375 dollari.

Celent stima che, teoricamente, elaborare mediante modelli di apprendimento profondo tutte le transazioni attualmente in esecuzione su IBM zSystems potrebbe ridurre le perdite legate alle frodi di 161 miliardi di dollari a livello globale. Le banche potrebbero evitare perdite legate alle frodi per 140 miliardi di dollari, mentre per le carte e i pagamenti la cifra si attesta a 21 miliardi di dollari. Solo negli Stati Uniti, il potenziale di riduzione delle frodi è di 44 miliardi di dollari per le banche e di 6 miliardi di dollari per carte e pagamenti.

Figura 4: Riduzione potenziale delle perdite dovute a frodi mediante i modelli di apprendimento profondo



Fonte: Celent

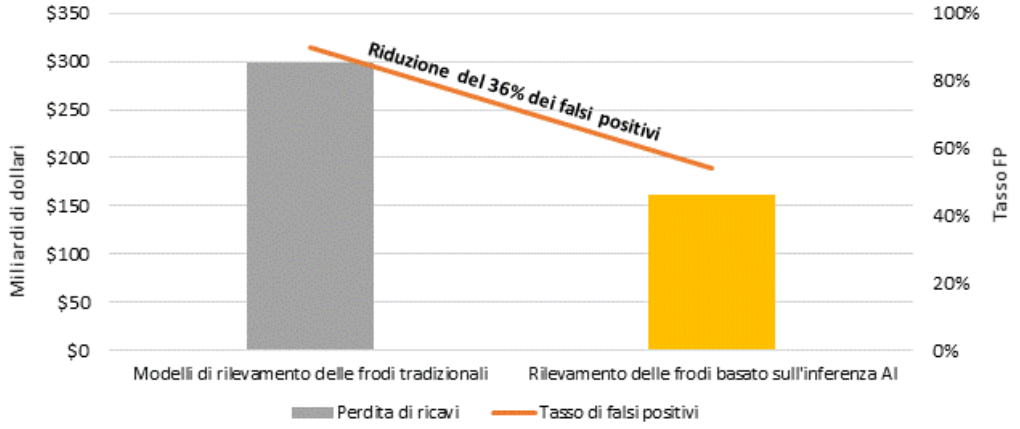
Celent stima che per una banca di classe 1 che utilizza IBM z16, l'elaborazione di tutte le transazioni mediante modelli di inferenza avanzati (rispetto all'attuale procedura considerata migliore, che prevede l'applicazione di modelli AI a solo il 10% circa delle transazioni) potrebbe ridurre le perdite legate alle frodi di ulteriori 105 milioni di dollari. Una banca di classe 2 potrebbe evitare perdite per ulteriori 18 milioni di dollari. L'elaborazione di tutte le transazioni mediante modelli avanzati migliorerebbe anche i modelli stessi. Un numero superiore di transazioni produrrebbe più dati con cui addestrare i modelli, traducendosi in una migliore precisione nel rilevamento delle frodi.

ELIMINAZIONE DEI FALSI POSITIVI PER LIMITARE L'ABBANDONO DEI CLIENTI

I modelli antifrode tradizionali hanno tassi di falsi positivi molto elevati (in genere pari o superiori al 90% di tutte le transazioni segnalate), che portano le banche a rifiutare anche le transazioni legittime. L'aumento dei falsi positivi e delle transazioni rifiutate non solo crea contrasti con i clienti, ma si traduce anche in consistenti perdite economiche, poiché i clienti tenderanno a usare un'altra carta di credito o debito per effettuare un acquisto. Secondo le stime di Celent, a livello globale le transazioni con carta di credito rifiutate costano al settore 298 miliardi di dollari di mancati ricavi da commissioni.

La necessità di equilibrare le attività antifrode con la riduzione al minimo dei contrasti con i clienti è un altro motivo per cui le banche limitano le routine di rilevamento delle frodi a un campione di tutte le transazioni. I falsi positivi si verificano quando le transazioni legittime vengono erroneamente segnalate come fraudolente dal software di rilevamento. La maggiore precisione dei modelli di apprendimento profondo può migliorare significativamente gli elevatissimi tassi di falsi positivi del settore. Questo ridurrebbe a propria volta il numero di transazioni erroneamente rifiutate. Ne consegue un miglioramento dell'esperienza dei clienti e una riduzione dei ricavi persi a causa del loro abbandono. Ciò significa anche che le banche possono elaborare tutte le proprie transazioni mediante i sistemi di rilevamento delle frodi e ridurre i danni derivanti dai contrasti con i clienti.

Figura 5: I modelli di apprendimento profondo migliorano i tassi dei falsi positivi



Fonte: Celent

I modelli di apprendimento profondo applicati a ogni transazione con carta potrebbero migliorare i tassi dei falsi positivi fino a circa il 55%. Pur essendo una cifra ancora molto

elevata, a livello globale sarebbe possibile ottenere una riduzione tra i 137 e i 161 miliardi di dollari di mancati introiti derivanti dalle commissioni sulle carte.

Un minor numero di falsi positivi avrebbe anche altri vantaggi. Gli analisti che si occupano di frodi potrebbero lavorare su un numero minore di segnalazioni, riducendo così i costi per le indagini sulle transazioni in fase post-transazione. In termini di benefici per la reputazione, la riduzione dei contrasti e della frustrazione dei clienti ne aumenterebbe la fidelizzazione.

I modelli avanzati possono anche migliorare l'individuazione di comportamenti sospetti che possono indicare episodi di riciclaggio di denaro. Il Bank Secrecy Act negli Stati Uniti, le direttive europee sul riciclaggio di denaro e altre normative pongono i programmi antiriciclaggio delle banche sotto un intenso controllo da parte delle autorità di regolamentazione. Negli Stati Uniti le autorità di regolamentazione sono particolarmente attive nel citare in giudizio le banche in caso di programmi antiriciclaggio inadeguati, con multe che in alcuni casi superano il miliardo di dollari. Anche le operazioni antiriciclaggio soffrono di tassi di falsi positivi molto elevati, in genere superiori al 95%, che impongono alle banche un grave onere operativo. Inoltre, il monitoraggio dell'antiriciclaggio viene generalmente eseguito nella fase post-transazione, il che espone le banche a un rischio maggiore. L'utilizzo di modelli basati sull'AI per le operazioni antiriciclaggio può aiutare a risolvere questi problemi migliorando la precisione del rilevamento dei comportamenti antiriciclaggio e riducendo i falsi positivi.

IL PERCORSO CHE CI ASPETTA

La nostra analisi evidenzia che l'esecuzione di modelli di apprendimento profondo sul 100% delle transazioni può portare a vantaggi significativi e quantificabili. IBM ritiene che il suo nuovo acceleratore sia in grado di supportarli per le transazioni in esecuzione sui mainframe IBM z16, anche in ambienti con volumi estremamente elevati. Rimangono tuttavia una serie di fattori da prendere in considerazione per le banche e i processori che vogliono fare il salto di qualità.

Alle banche e ai processori di carte e pagamenti che stanno valutando i vantaggi di implementare sul mainframe il rilevamento delle frodi basato sull'apprendimento profondo, Celent consiglia di tenere conto di aspetti quali:

- **Governance dei modelli.** Le autorità di regolamentazione e i revisori interni richiedono una robusta governance da applicare ai modelli antifrode. Questo significa che i modelli AI devono essere trasparenti ed esplicabili. Sebbene i fornitori di piattaforme AI stiano generalmente abbandonando gli approcci di tipo "black box", la governance dei modelli AI rimane una sfida complessa.
- **Resistenze normative.** Le autorità di regolamentazione si trovano a proprio agio con il rilevamento tradizionale basato su regole, ma hanno meno familiarità con le tecniche avanzate di apprendimento profondo. In alcuni casi le banche, i data scientist e i loro fornitori potrebbero dover istruire le autorità di regolamentazione sull'efficacia e l'affidabilità dell'AI avanzata in corso d'opera.
- **Costi di sostituzione.** Molte realtà hanno già implementato dei sistemi di rilevamento delle frodi basati sull'AI. Queste aziende dovranno sviluppare il caso di business per trasferire il rilevamento al mainframe, decidendo anche se mantenere i sistemi in dotazione in qualche forma (ad esempio, per supportare l'analisi post-transazione o settori di attività più ridotti) o se eliminarli del tutto.
- **Risorse di data science.** Integrated Accelerator for AI di IBM è ottimizzato per l'esecuzione dei modelli, compresi quelli sviluppati con framework open source come Pytorch e TensorFlow. Tuttavia, non è ancora stata dimostrata la sua capacità di supportare software di rilevamento delle frodi basati su pacchetti, anche se ci aspettiamo che alcuni fornitori di soluzioni antifrode si facciano avanti con pacchetti in grado di essere eseguiti sull'acceleratore. In ogni caso, le realtà che stanno passando a IBM z16 per il rilevamento basato sull'AI avranno bisogno di competenze di data science per sviluppare e supportare modelli avanzati di apprendimento profondo per le frodi, sia internamente che tramite fornitori di modelli specializzati.

Gli istituti finanziari dovranno considerare con attenzione e debita diligenza questi fattori nell'adottare il nuovo acceleratore AI di IBM. Tuttavia, i potenziali vantaggi in termini di riduzione delle perdite dovute a frodi e transazioni rifiutate, nonché di riduzione dei conflitti e di miglioramento dell'esperienza cliente, sono convincenti. Le aziende che utilizzano IBM zSystems devono valutare con attenzione i vantaggi che possono derivare dallo spostamento sul mainframe del rilevamento delle frodi.

AFFIDATI ALLE COMPETENZE DI CELENT

Se questo report ti è sembrato utile, prendi in considerazione la possibilità di collaborare con Celent per analisi e ricerche su misura per la tua azienda. La nostra esperienza collettiva e le conoscenze acquisite durante la stesura di questo report possono aiutarti a semplificare la creazione, il perfezionamento e l'esecuzione delle tue strategie.

Sostegno agli istituti finanziari

I tipici progetti che supportiamo includono:

Selezione dei fornitori. Effettuiamo una ricerca specifica per l'attività e il business per comprendere meglio le sue esigenze specifiche. Creiamo e gestiamo una richiesta di informazioni personalizzata in base a fornitori selezionati per aiutarti a fare scelte rapide ed efficaci.

Valutazione delle prassi aziendali. Dedichiamo tempo alla valutazione dei tuoi processi e requisiti aziendali. Grazie alla nostra conoscenza del mercato, rileviamo i potenziali vincoli tecnologici o relativi ai processi e forniamo indicazioni chiare che ti aiuteranno a implementare le migliori procedure del settore.

Creazione di strategie IT e aziendali. Raccogliamo i punti di vista del tuo team dirigenziale, del personale aziendale e IT in prima linea e dei clienti. Quindi, analizziamo la posizione attuale dell'azienda, le sue capacità istituzionali e le tecnologie rispetto agli obiettivi fissati. Se necessario, ti aiutiamo a riformulare i piani tecnologici e aziendali per soddisfare le esigenze a breve e a lungo termine.

Assistenza per i fornitori

Forniamo servizi che ti aiutano a perfezionare le offerte di prodotti e servizi. Ecco alcuni esempi:

Valutazione delle strategie legate a prodotti e servizi. Ti aiutiamo a valutare la tua posizione sul mercato in termini di funzionalità, tecnologia e servizi. I nostri seminari sulle strategie ti aiuteranno a individuare il giusto target di clientela e a mappare le tue offerte in base alle sue esigenze.

Revisione della comunicazione di mercato e del marketing. Sulla base della nostra vasta esperienza coi tuoi potenziali clienti, valutiamo i tuoi materiali di marketing e di vendita, compresi il sito web e qualsiasi risorsa supplementare.

RICERCHE CELENT CORRELATE

Remaking Risk: A Taxonomy of Regtech
Ottobre 2021

Technology Trends Previsory: Risk, 2022 Edition
Ottobre 2021

IT and Operational Spending in AML-KYC: 2021 Edition
Dicembre 2021

IT and Operational Spending on Fraud: 2021 Edition
Febbraio 2021

Innovation In Risk: A Snapshot Through the Lens of Model Risk Manager 2021
Aprile 2021

Fino Payments Bank: Remote Implementation of Enterprise-Wide Fraud Management During the Pandemic
Marzo 2021

Swedbank: Modernizing Card Fraud Management and Improving Customer Experience
Marzo 2021

INFORMAZIONI RELATIVE ALLE LEGGI SUL DIRITTO D'AUTORE

Per ulteriori informazioni, contattare info@celent.com oppure:

Neil Katkov nkatkov@celent.com

Americhe

Stati Uniti
99 High Street, 32nd Floor
Boston, MA 02110-2320

+1.617.424.3200

Stati Uniti
1166 Avenue of the Americas
New York, NY 10036

+1.212.345.8000

Stati Uniti
Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

+1.415.743.7800

Brasile
Rua Arquiteto Olavo Redig
de Campos, 105
Edifício EZ Tower – Torre B – 26º andar
04711-904 – San Paolo

+55 11 3878 2000

EMEA

Svizzera
Tessinerplatz 5
Zurigo 8027

+41.44.5533.333

Francia
1 Rue Euler
Parigi 75008

+33 1 45 02 30 00

Italia
Galleria San Babila 4B
20122 Milano

+39.02.305.771

Regno Unito
55 Baker Street
Londra W1U 8EW

+44.20.7333.8333

Asia-Pacifico

Giappone
Midtown Tower 16F
9-7-1, Akasaka
Minato-ku, Tokyo 107-6216

+81.3.6871.7008

Hong Kong
Unit 04, 9th Floor
Central Plaza
18 Harbour Road
Wanchai

+852 2301 7500

Singapore
138 Market Street
#07-01 CapitaGreen
Singapore 048946

+65 6510 9700