IL CONTRASTO AL CRIMINE FINANZIARIO E IL MONDO DEI PAGAMENTI: EVOLUZIONI IN CORSO

La visione di **Sopra Steria**

Milano, 22 Novembre 2023

The world is how we shape it

MILAN
NOV 22-24, 2023

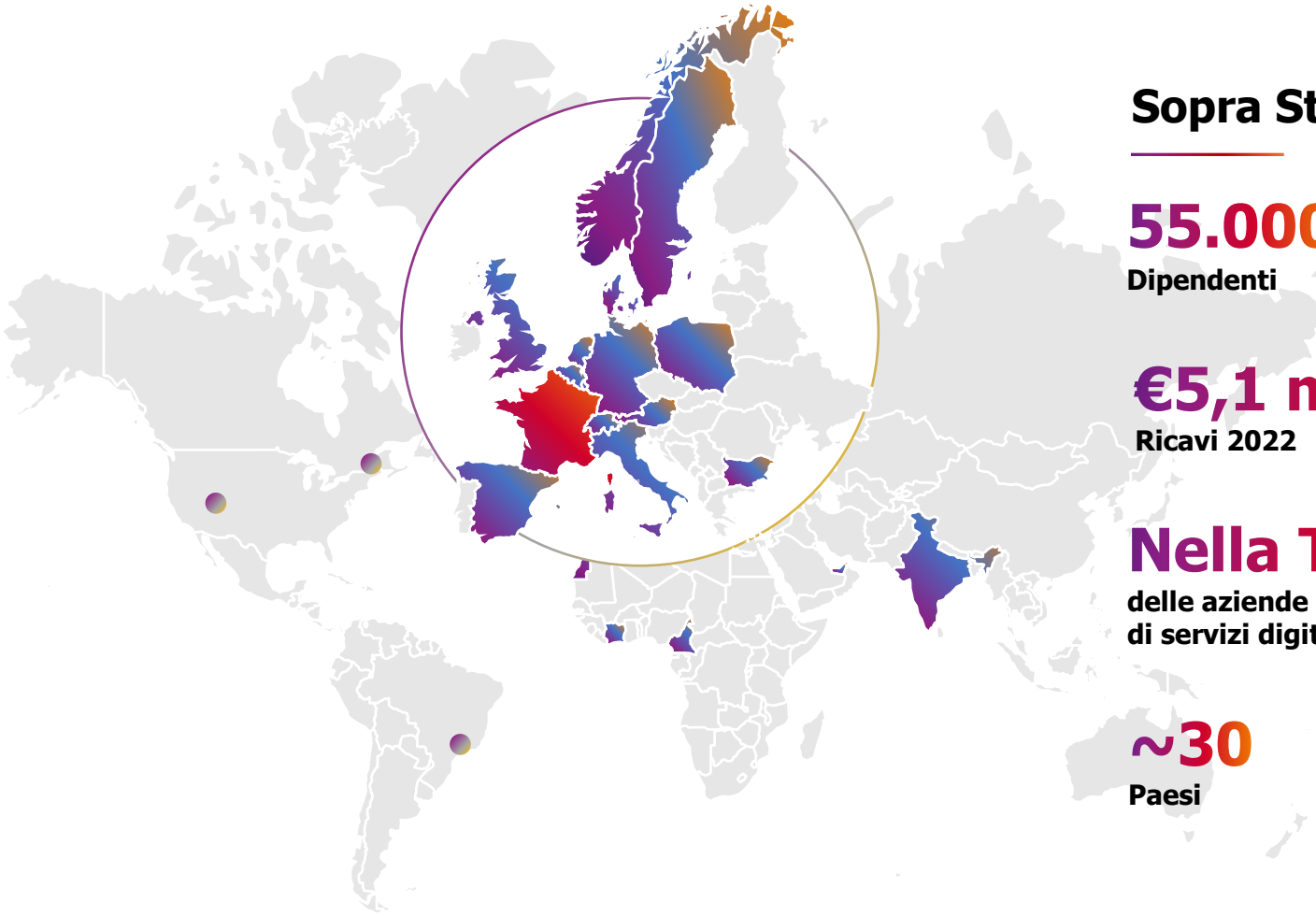
sopra steria

Sopra Steria, Tech Leader in Europa

Un Gruppo europeo specializzato in consulenza, servizi digitali e sviluppo di software

Leader globale nel campo della consulenza, dei **servizi digitali** e **dello sviluppo di software.**

- Modello indipendente
- Cultura imprenditoriale
- Focus sul capitale umano
- Un partner fidato



Sopra Steria

55.000
Dipendenti

€5,1 miliardi
Ricavi 2022

Nella Top 5
delle aziende europee di servizi digitali

~30
Paesi

AGENDA

1  DATA

2  CUSTOMER JOURNEY

3  STRONG CUSTOMER AUTHENTICATION & AFC

4  AI & MACHINE LEARNING: IL CASO SPAGNOLO IBERPAY

01

DATA

Dati di Mercato

Il rischio rappresentato dai **reati finanziari nell'industria dei pagamenti** è concreto e non dovrebbe essere sottovalutato. Il valore totale delle transazioni dei pagamenti digitali, raggiungerà circa i **9,46 trilioni di dollari nel 2023**, in aumento rispetto **ai 5,44 trilioni di dollari nel 2020.**

- Fonte: *Finextra (4 luglio 2023)*

L'importo di denaro riciclato ogni anno è stimato tra **il 2% e il 5% del PIL globale**, equivalente ad una cifra compresa tra gli **800 miliardi e i 2 trilioni di dollari annualmente.**

- Fonte: *UN (United Nations) Office on Drugs and Crime*

$1.9B

PERDITE DOVUTE ALLE FRODI

Nel 2022, si stima che siano state commesse frodi per un valore di 1,9 miliardi di dollari nell'Unione Europea, registrando un aumento del 7 % rispetto al 2021.

- Fonte*: Politico (27 luglio 2023)*

30%

CRIMINI FINANZIARI IN AUMENTO

Stima dell'aumento dei reati finanziari nei prossimi anni.

50%

SANZIONI

Sanzioni globali dovute al riciclaggio di denaro sono aumentate del 50% nel 2022

- Fonte: *Financial Times (18 Jan 2023)*

Market Insights

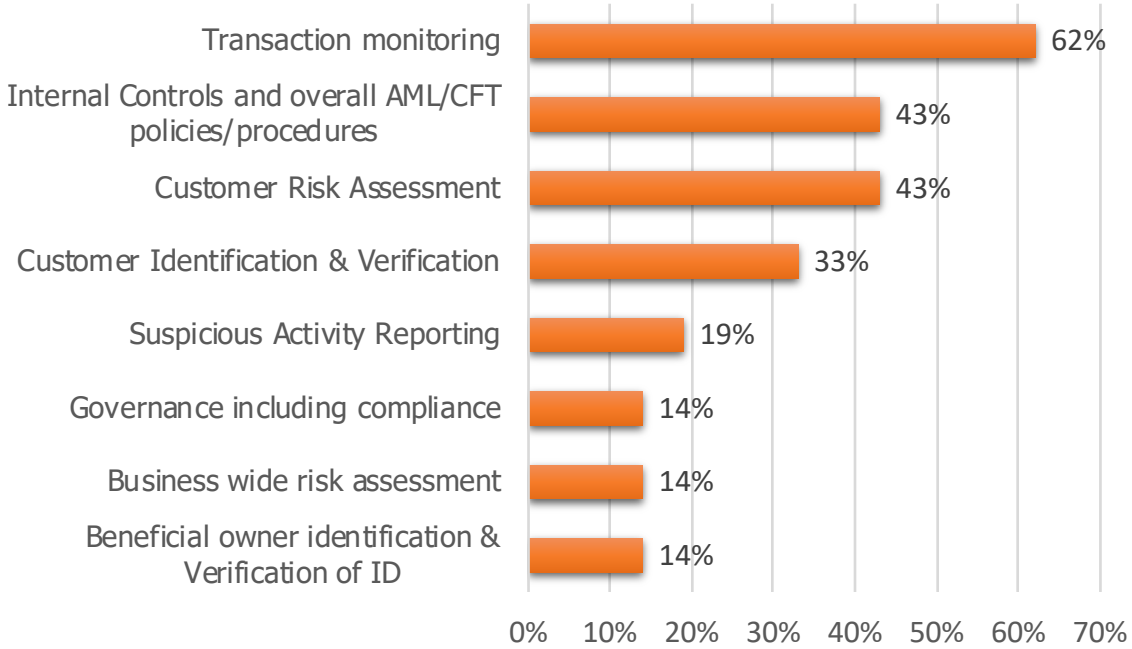
rapporto ABE 2023 sui rischi legati al riciclaggio di denaro

L'inefficacia delle misure AML implementate e i controlli effettuati dalle banche.

CRITICITÀ AML IDENTIFICATE DAI SUPERVISORI UE

- Scarso livello di consapevolezza del rischio di riciclaggio di denaro
- Insufficienza delle procedure di transaction monitoring
- Insufficienza delle procedure di identificazione delle transazioni sospette e della loro reportistica
- Mancanza di implementazione dei sistemi di controllo conformi alle misure restrittive
- Scarso adeguamento alla governance interna
- Onboarding da remoto/online senza le appropriate misire di sicurezza e validazione (spesso gli istituti di pagamento non riescono ad identificare I client ad alto rischio inclusi i **PEP**)

I PROCESSI CHE HANNO PORTATO A PIÙ VIOLAZIONI NEL 2022

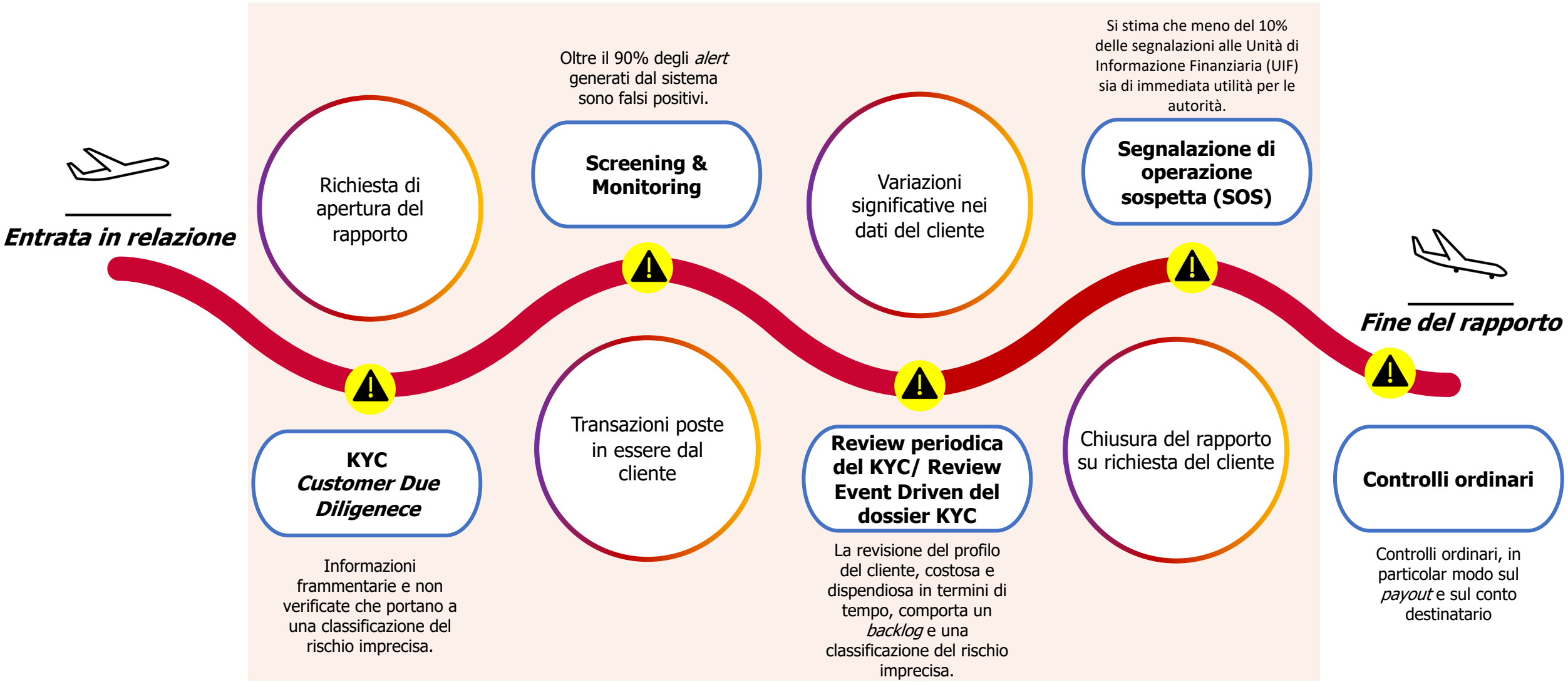


L'uso del Virtual IBANs e del White Labelling sono emergenti fattori di rischio

02

CUSTOMER JOURNEY

Controlli chiave durante l'esperienza del cliente



Potenziale frode attuata in costanza di rapporto

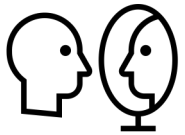
Interazioni con i clienti

Punti deboli

	ATM	Carte e pagamenti digitali	E-banking	Filiale
APERTURA DEL CONTO Il cliente apre un nuovo conto corrente o aggiunge un altro conto corrente tramite ATM, Online, Mobile o filiale)	• **Furto d'identità** • **Falsa identità** • **Conto creato (per fini illeciti) dal dipendente** • ***Malware***			
MODIFICA DEL CONTO (Il cliente aggiorna il conto corrente esistente, ad esempio aggiungendo un beneficiario o cambiando l'indirizzo)	• ***Malware***	• ***Account Takeover*** • **Cambio di indirizzo** • **Seconda carta** • ***Malware***	• **Beneficiario falso o aggiunto** • ***Account Takeover*** • ***Malware***	• ***Account Takeover***
EFFETTUARE UN PAGAMENTO (Il cliente paga se stesso o un terzo tramite bonifico, carta o online)	• ***Card skimming/trapping*** • **Pin Pad falso** • **Trapping di contanti** • **Carta duplicata** • **Revoca (impropria) di transazione** • ***Malware***	• **Frode con carta non presente** • ***Skimming* di carte di credito** • ***Malware*** • **Cyberattacco**	• **Transazioni guidate (con dolo) dai dipendenti** • ***Malware*** • **Cyberattacco**	
EFFETTUARE UN DEPOSITO (Il cliente effettua un bonifico o un versamento sul proprio conto)	• **Riciclaggio di denaro o finanziamento del terrorismo** • **Malware «*balance multiplier*»)**			

03

STRONG CUSTOMER AUTHENTICATION & AFC



Strong Authentication

La Strong Customer Authentication (SCA) prevista dalla PSD2 richiede un'**autenticazione più sicura** per le transazioni finanziarie online, come l'uso di due o più fattori per confermare l'identità dell'utente. **Questa autenticazione più robusta può essere un alleato utile nella lotta al riciclaggio di denaro.** L'uso di più fattori, come password, biometria o dispositivi secondari, riduce il rischio di transazioni non autorizzate, fornendo un ulteriore livello di sicurezza. **La SCA può contribuire a identificare e prevenire attività sospette, limitando le opportunità per i riciclatori di aggirare i controlli e di compiere attività illecite**. Di seguito riportata una **best practice** nell'ambito di verifica dell'identità:

IL DIGITAL ONBOARDING

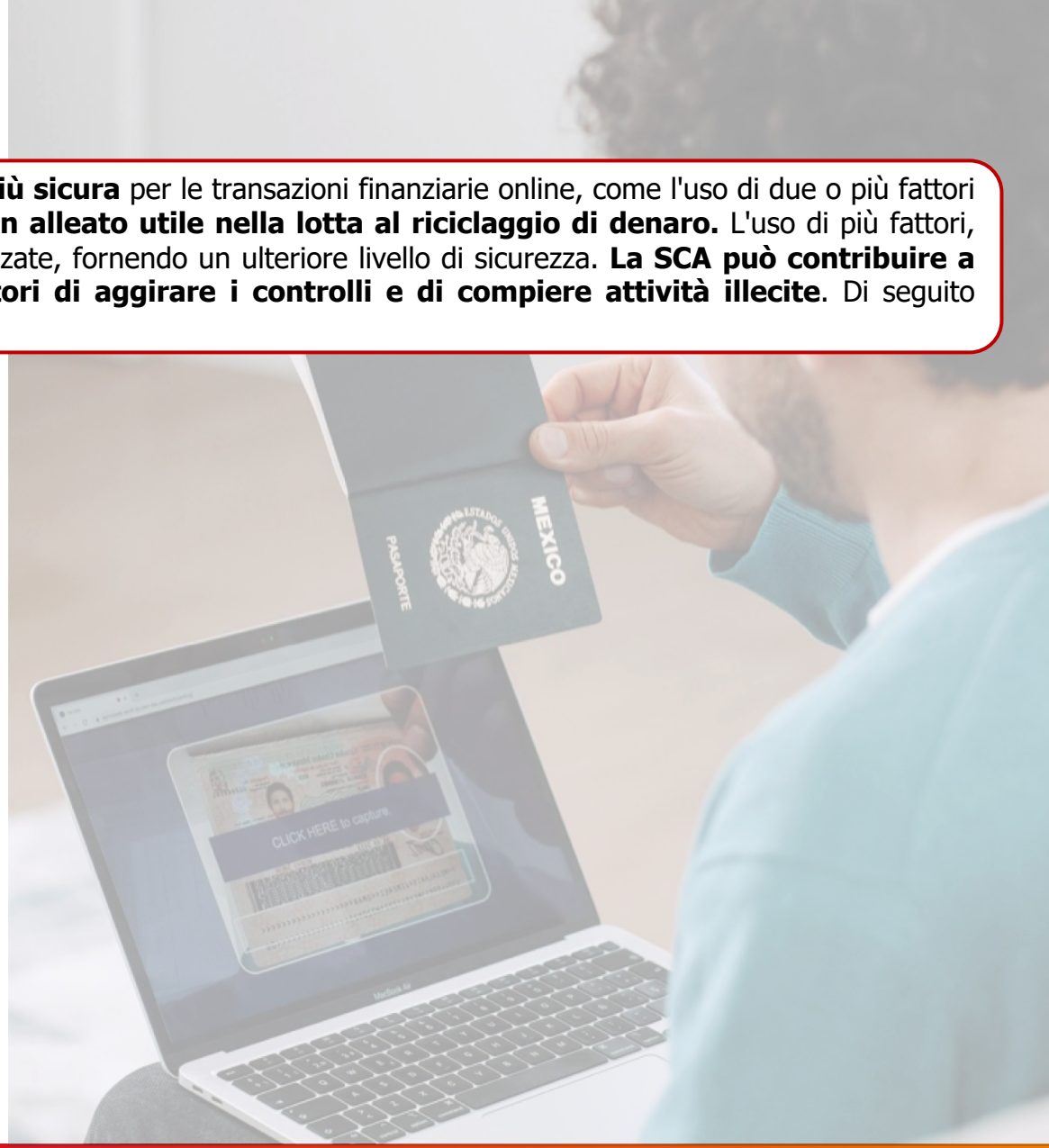
Si tratta di una procedura completamente automatizzata (**senza interazione umana, e quindi con ridottissimi o assenti margini di errore**) e con copertura globale in tutto il mondo. Ricordiamo che la *customer experience* in questi casi è importante in quanto la rapidità e la facilità di inserimento dati è un incentivo per il cliente ad essere collaborativo e, in definitiva, ad essere tutelato.

SCANSIONE DEI DOCUMENTI D'IDENTITÀ

Il cliente deve scansionare entrambi i lati del suo documento di identità. La tecnologia, attraverso molteplici algoritmi di **intelligenza artificiale,** aiuterà ad analizzare quasi istantaneamente l'autenticità del documento.

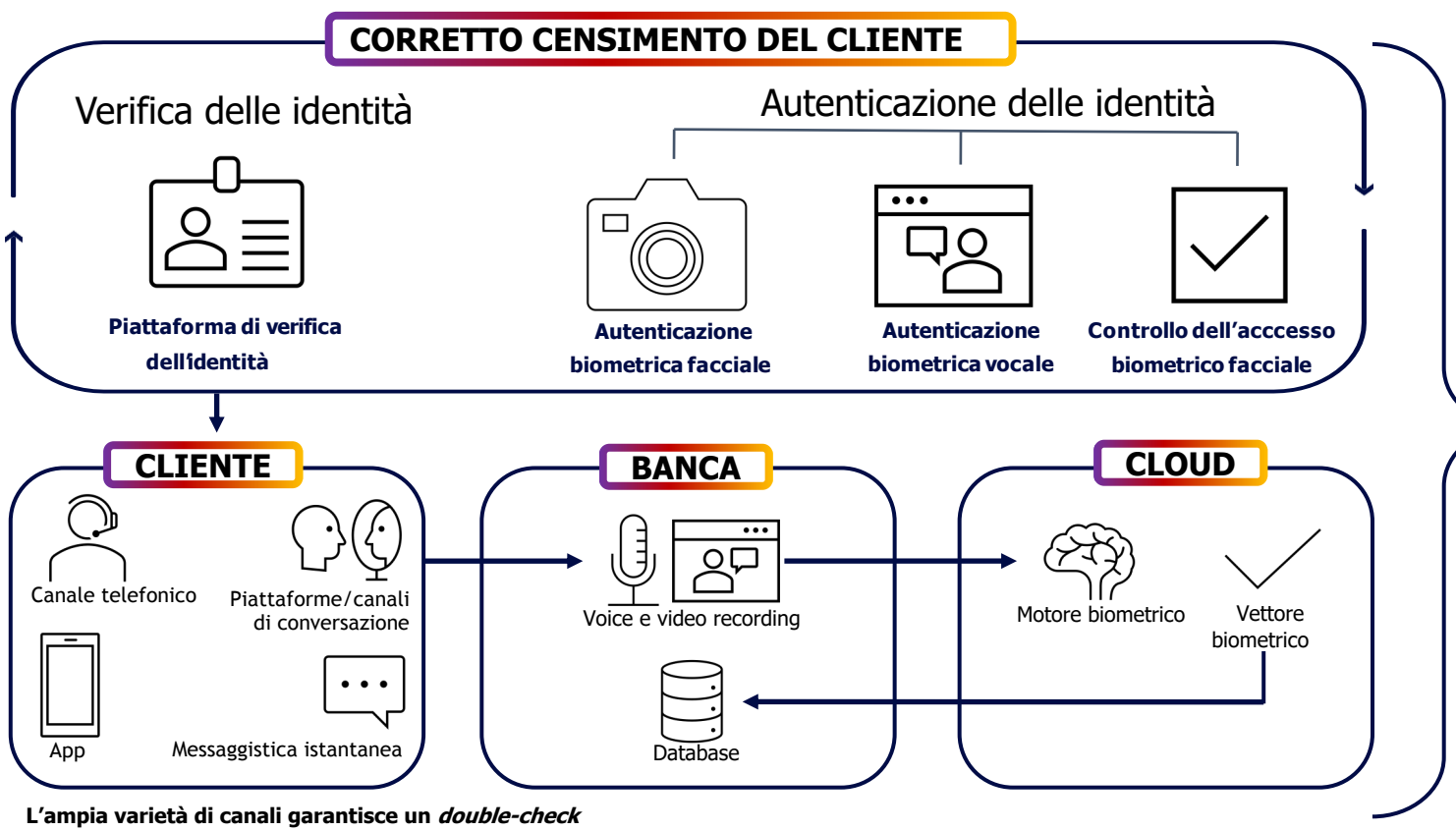
CHECK DEI DUPLICATI

Gli algoritmi di intelligenza artificiale offrono vantaggi cruciali nel prevenire l'associazione di un documento di identità a più soggetti o viceversa. Grazie alla loro capacità di riconoscere *pattern* complessi, questi algoritmi migliorano l'efficienza nell'identificazione di comportamenti sospetti, contribuendo a prevenire frodi e abusi, garantendo al contempo un'associazione corretta tra documento di identità e individuo.

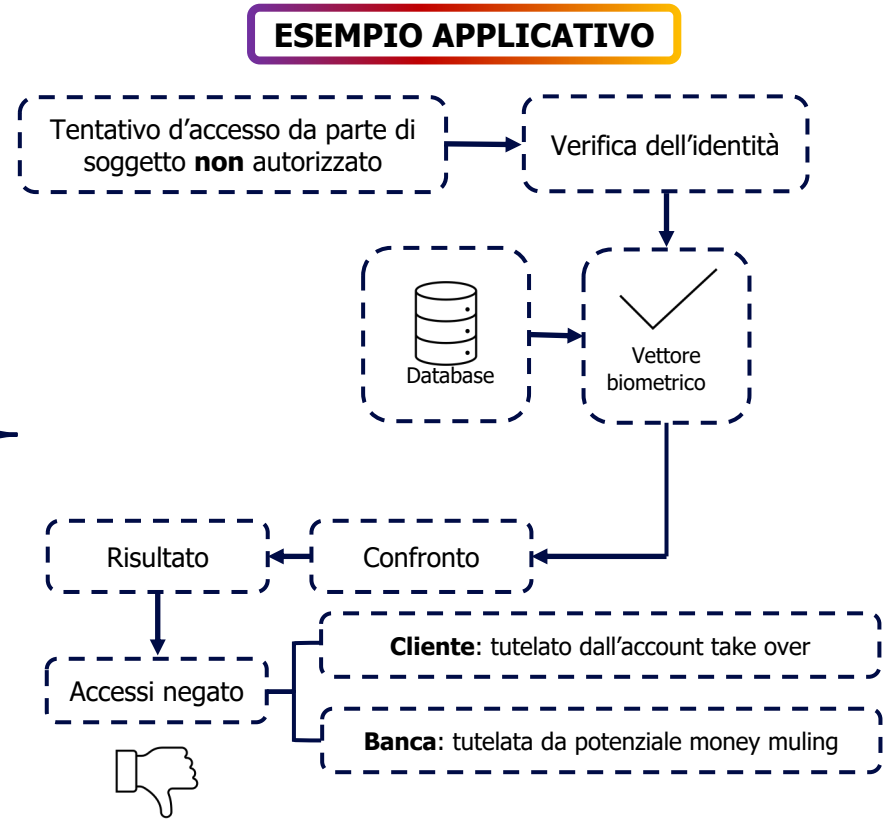


Autenticazione facciale e vocale

L'impiego della **biometria** durante la fase iniziale di acquisizione del cliente non si limita ai suoi vantaggi iniziali ma **si estende su tutta la durata del rapporto**. Attraverso una precisa identificazione del cliente ed una SCA applicata ad ogni operazione rilevante, è possibile prevenire più del 90% delle **frodi**, in particolare quelle legate all'appropriazione indebita di conti, garantendo la sicurezza continua del rapporto e **dimostrando l'importanza delle misure preventive** come di seguito illustrate**.**

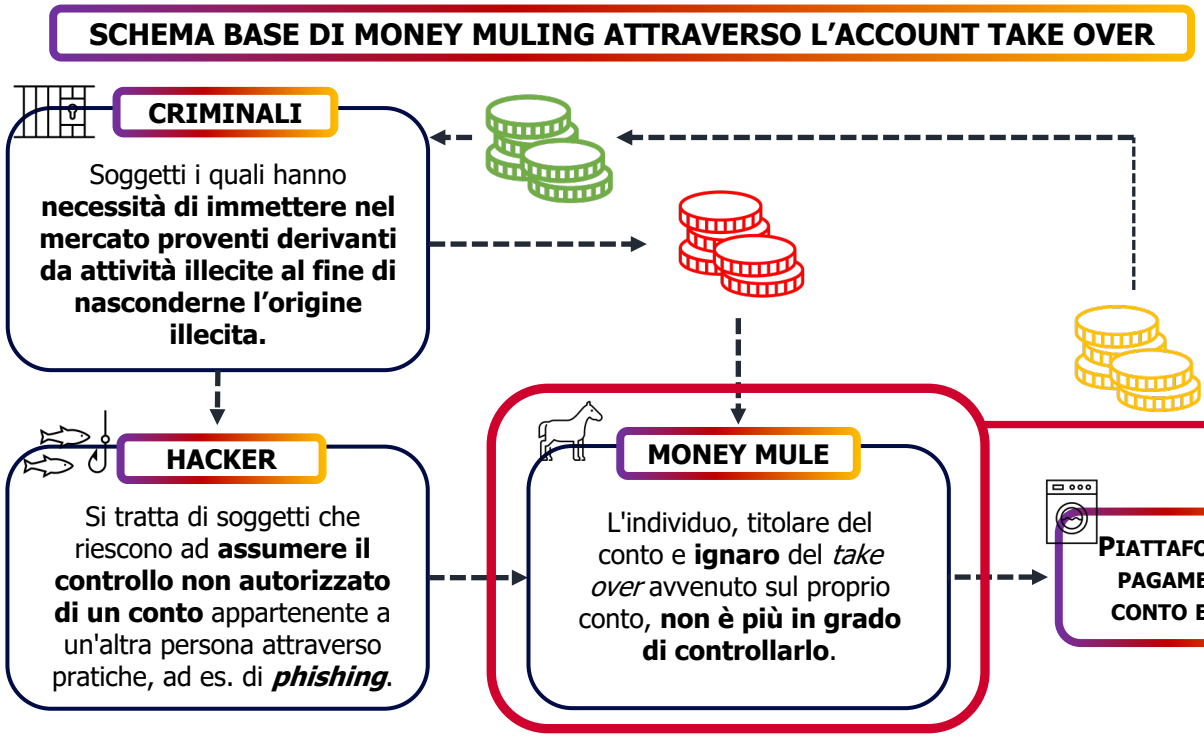


L'ampia varietà di canali garantisce un *double-check*



Use case contro il money muling

Il money muling coinvolge individui che fungono da intermediari per trasferire denaro illecito. Secondo il **rapporto annuale della Banca d'Italia del 2022, sono stati identificati casi di money muling legati a pagamenti anomali con carte prepagate presso esercizi commerciali**. Questi pagamenti, provenienti da **frodi informatiche**, coinvolgono una rete di individui che agiscono come money mule, utilizzando il denaro illecito per acquistare carte regalo o buoni spesa anonimi e trasferibili.



La Strong Customer Authentication (SCA) è fondamentale per prevenire gli attacchi di tipo *account takeover* (ATO). Questo è possibile perché la SCA richiede più di un'identificazione per confermare l'accesso o le transazioni, rendendo più difficile per i truffatori ottenere l'accesso non autorizzato.

Poiché la SCA richiede più fattori di autenticazione (come password, dispositivi di sicurezza, autenticazione biometrica), **anche se un truffatore riesce a ottenere una delle informazioni di accesso (ad esempio una password), non avrà accesso completo senza gli altri elementi di autenticazione richiesti dalla SCA**.

In sostanza, **la SCA riduce la vulnerabilità agli attacchi di tipo ATO richiedendo una verifica multipla, rendendo più difficile per i truffatori assumere il controllo di un account utilizzando solo una parte delle informazioni di accesso**.

04

AI & MACHINE LEARNING – IL CASO SPAGNOLO iBERPAY

Iberpay – processo pagamenti istantanei

Iberpay gestisce il sistema di pagamento nazionale spagnolo (SNCE), tramite l'**elaborazione, la compensazione e il regolamento di strumenti di pagamento basati sul conto corrente bancario**.
Iberpay svolge inoltre un **ruolo chiave nella distribuzione di contanti** alle istituzioni finanziarie spagnole in quanto gestore del Sistema di Deposito Ausiliario (SDA) e fornisce **altri servizi tecnologici e digitali ad alto valore aggiunto nel campo dei pagamenti**.

Iberpay è il primo CSM (Clearing & Settlement Mechanism) in Europa ad aver ottenuto dal Consiglio Europeo dei Pagamenti (EPC) il certificato di approvazione per l'elaborazione di transazioni basate sullo schema SEPA **Request-to-Pay** per le proprie entità. Il Request-to-Pay consente ad aziende e privati di **richiedere pagamenti istantanei ai propri clienti o controparti online, in modo digitale** e senza attriti. Questo nuovo tipo di pagamento istantaneo **"pull"** (il processo è avviato dal destinatario del pagamento) integra gli attuali bonifici istantanei, che rappresentano il pagamento **"push"** (il pagamento è avviato dall'ordinante).

Le banche spagnole sostengono da tempo l'adozione di questo nuovo standard europeo e stanno lavorando con Iberpay per ottenere la certificazione e incorporare tale modello nei loro servizi. Ciò contribuirà a consentire l'**adozione diffusa di questa nuova funzionalità** e lo **sviluppo di nuove soluzioni di pagamento istantaneo e digitale**.

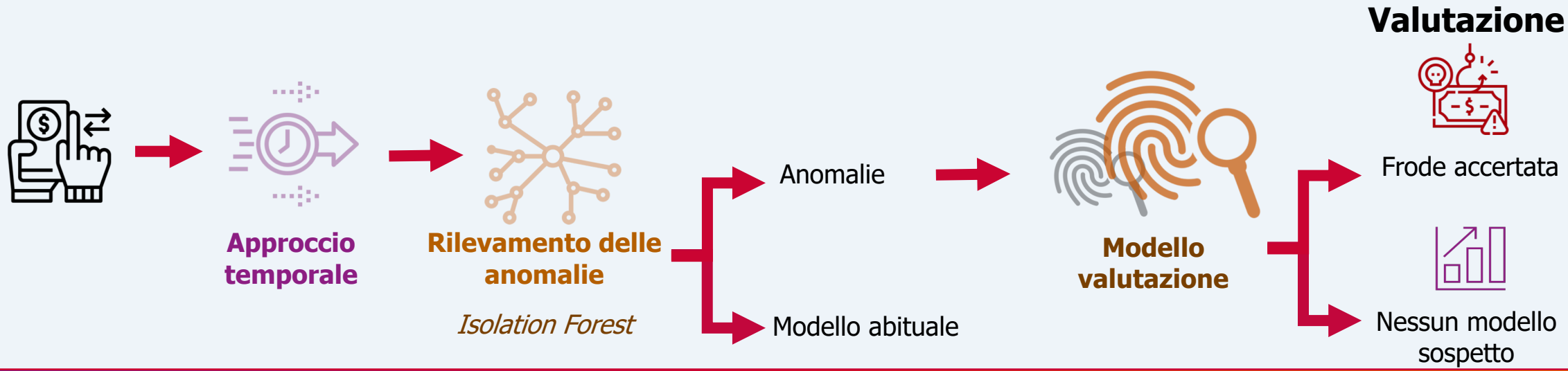
Benefici:

- individuazione di **frodi bancarie**;
- Collaborazione continua con le banche nella lotta contro le frodi, grazie alla visione privilegiata di Iberpay del **corridoio bancario end-to-end**;
- Affiancamento efficace alle azioni già intraprese dalle banche per rilevare le frodi, grazie alla capacità di individuare potenziali frodi end-to-end.

Iberpay - Metodologia

- **Situazione:** Le banche spagnole hanno notato un ***aumento dei casi di frode*** e delle risorse necessarie per identificarli correttamente e indagare su di essi con ***un'alta percentuale di falsi positivi.***
- **Soluzione**: Sviluppo e implementazione di un modello di ***prevenzione delle frodi attraverso un algoritmo e l'apprendimento automatico*** per identificare i potenziali conti fraudolenti, condividendo i risultati con l'ente competente per ulteriori decisioni.
- **Benefici**: ***accuratezza*** degli avvisi investigati, lasciando più tempo agli enti per concentrarsi su altre attività.

Apprendimento automatico nel rilevamento delle frodi



Iberpay - Metodologia

Apprendimento

Analisi (intensiva) **dei dati**

Dati grezzi del database

Sviluppo

Focus sul tempo

Rilevamento delle anomalie

Valutazione dei modelli

Trasformazioni, aggregazioni e ingegneria delle caratteristiche

Prodotto

Registro delle Anomalie

Elenco IBAN (Valutazioni)

Consegna delle statistiche sul comportamento fraudolento

Dati aziendali con valore operativo

\- → +

Valore dei Dati

RELATORE:

MANUELE MASON

Senior Manager

T. +39 342 3914790
manuele.mason@soprasteria.com

MILAN
NOV 22-24, 2023