

Cyber-crime e frodi online: sfida per tutto l'ecosistema Ecommerce

Axerve • Whitepaper



Il presente documento è di proprietà esclusiva di Axerve S.p.A., che ne detiene tutti i diritti di riproduzione, diffusione, distribuzione e alienazione, nonché ogni ulteriore diritto individuato dalla vigente normativa in materia di diritto d'autore. Il presente documento e il suo contenuto non possono pertanto essere ceduti, copiati, diffusi o riprodotti, né citati, sintetizzati o modificati, anche parzialmente, senza l'esplicito consenso di Axerve S.p.A.

Agenda

Le truffe online e l'impatto sulla fiducia dei consumatori	3
Il cyber-crime in Europa	7
La situazione delle frodi online in Italia	9
Le tecniche utilizzate per le frodi online	10
Le frodi Ecommerce: quanto costano all'intero sistema e come prevenirle	16
Frodi Ecommerce in Europa e Stati Uniti: il punto di vista di merchant e consumatori	21
PSD2 e Strong Customer Authentication al fianco di tutto l'ecosistema Ecommerce	22
Analisi del rischio e intelligenza artificiale: la risposta di Axerve alle frodi	24
Axerve Guaranteed Payments: l'intelligenza artificiale al servizio della prevenzione frodi	24
Axerve Advice: come migliorare il conversion rate sulle autenticazioni	25
Ecommerce e la rivoluzione dei Payment Orchestrator	26
Prevenzione frodi e Payment Orchestration	27
Fonti e riferimenti	28

Le truffe online e l'impatto sulla fiducia dei consumatori

L'avvento di internet ha rivoluzionato molti aspetti della nostra vita, non ultimo quello degli acquisti e, di conseguenza, dei pagamenti. Allo stesso tempo il web, sin dai suoi albori, è stato anche terreno fertile per truffe telematiche a scapito di consumatori ed esercenti. Dai finti merchant che una volta ricevuto il pagamento non spediscono la merce a chi effettua acquisti con numeri di carte di credito clonate o sottratte ai legittimi proprietari, le frodi online sono cresciute nel tempo, non solo in termini di volumi ma anche di complessità delle minacce e continuano a frenare lo sviluppo dell'Ecommerce nel mondo.

Nonostante nel corso dei decenni le soluzioni per tutelare acquirenti e venditori si siano moltiplicate ed evolute, il commercio elettronico ancora

oggi non è esente da rischi, anche a causa degli strumenti sempre più sofisticati a disposizione di chi commette questi atti illeciti. A contribuire alla propagazione di software e dati necessari per perpetrare frodi online c'è poi il cosiddetto *dark web*, ossia l'insieme di contenuti e risorse web, spesso illegali, accessibili solo attraverso piattaforme e autorizzazioni specifiche, tramite il quale proliferano il commercio di strumenti utili alle attività criminali.

Secondo l'"Internet Crime Report 2020" pubblicato dall'organo dell'FBI Internet Crime Complaint Center (IC3), solo nel 2020 le segnalazioni di truffe online sono state quasi 800mila, il 69% in più rispetto al 2019, per un valore complessivo di 4,1 miliardi di dollari.



Fonte: Internet Crime



Nel quinquennio 2016-2020, IC3 ha ricevuto un totale di 2.211.396 segnalazioni per un totale di 13,3 miliardi di perdite ai danni di aziende e consumatori. Dopo gli Stati Uniti, che nel 2020 hanno registrato 540.710 vittime di frodi online, il Paese nel mondo più coinvolto è stato il Regno Unito che con 216.633 casi ha superato di gran lunga il Canada, al terzo posto con 5.399 segnalazioni.

Dal report di IC3 si evince che nel 2020 le tre fasce di età più colpite negli Stati Uniti sono state quella degli over 60 (105.301 casi di frode che hanno generato 966.062.236 di dollari di frodi), a seguire la fascia 50-59 (91.568 casi che hanno causato perdite per 717.161.726 dollari) e poi quella 40-49 (85.967 casi, per un volume di 847.948.101 di dollari).

2020 VICTIMS BY AGE GROUP

Age range	Total count	Total loss
Under 20	23,186	\$70,980,763
20-29	70,791	\$197,402,240
30-39	88,364	\$492,176,845
40-49	91,568	\$717,161,726
50-59	85,967	\$847,948,101
Over 60	105,301	\$966,062,236

Grafico 1 - Fonte: Internet Crime Report 2020

Sono quindi le generazioni più mature ad essere colpite maggiormente. Analizzando le perdite medie si può notare come, sebbene gli over 60 siano la fascia d'età con il numero maggiore di persone colpite, è la popolazione compresa tra i 50 e 59 anni, terza nella classifica per numero di frodi, che ha generato la perdita media più alta, con un valore che intorno ai 9.864 dollari.

È evidente dunque che la popolazione più a rischio è quella con minore confidenza con gli strumenti digitali, preda più facile dei cosiddetti *scammers* che spesso utilizzano pratiche subdole per convincere le loro vittime a fornire dati personali. Un esempio su tutti sono le frodi telefoniche, particolarmente adatte perché sfruttano un canale congeniale alle vittime, a cui seguono e-mail di phishing tramite le quali vengono carpiti i dati personali.

I dati riportati da IC3 non rappresentano la totalità delle truffe online a livello mondiale, sia perché moltissime non vengono denunciate o scoperte sia perché esiste una moltitudine di enti governativi o organizzazioni che si occupano di raccogliere ed investigare questi fenomeni.

Tra queste c'è anche econsumer.gov, un'iniziativa dell'International Consumer Protection and Enforcement Network (ICPEN) che, dall'aprile del 2001, raccogliendo e condividendo con gli Stati membri segnalazioni di truffe correlate

all'Ecommerce, rappresenta una rete di organizzazioni governative di più di 40 nazioni per l'applicazione delle leggi sulla pratica del commercio equo e altre attività di protezione dei consumatori.

Le segnalazioni cross-border raccolte da econsumer.gov, che collabora tra gli altri anche con l'agenzia governativa statunitense a tutela dei consumatori (Federal Trade Commission) e con l'Autorità Garante della Concorrenza e del Mercato italiano (AGCOM), dal 2017 ad oggi sono aumentate drasticamente così come i danni economici generati dalle truffe ad esse correlate.

Se nel 2017¹ le segnalazioni ricevute da econsumer.gov sono state 19.545, il 77% delle quali ha generato effettivamente delle perdite per un totale di oltre 73 milioni di dollari, già a fine 2020 le lamentele raccolte sono salite a 60.835 e ben l'85% ha generato danni economici, per un totale di 211,6 milioni di dollari.

Dati pubblicati recentemente dalla Federal Trade Commission² sul mercato americano offrono uno spaccato delle frodi online negli Stati Uniti, da sempre pionieri del commercio elettronico e quindi riferimento da monitorare anche per identificare in anticipo possibili trend a livello globale.

Nel periodo 1 gennaio 2020 - 5 agosto 2021, dunque in pieno periodo pandemico, il totale delle frodi registrate da FTC sono state 347.945 per un totale di 519,43 milioni di dollari e una perdita media di 376 dollari. Come si evince dal grafico 2, buona parte delle attività illecite sono proprio riconducibili allo shopping online e ad attività collegate.

Solo nel 26% delle segnalazioni sono stati specificati i canali di contatto utilizzati dai malintenzionati e nel 37,3% dei casi è stato indicato il metodo di pagamento utilizzato per finalizzare i pagamenti. Dai grafici pubblicati da FTC, l'e-mail guida la classifica dei canali di comunicazione più utilizzati ma sono siti e app ad aver generato gli introiti fraudolenti più remunerativi, facendo registrare un totale di 46,06 milioni di dollari di perdite.

1 - econsumer.gov International Fraud Report
2 - FTC COVID-19 and Stimulus Report

Top Fraud Reports

Online Shopping



Vacation & Travel



Diet Products, Plans & Centers



Government Impostors



Business Impostors



Online Shopping



Vacation & Travel



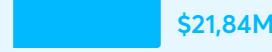
Diet Products, Plans & Centers



Government Impostors



Business Impostors



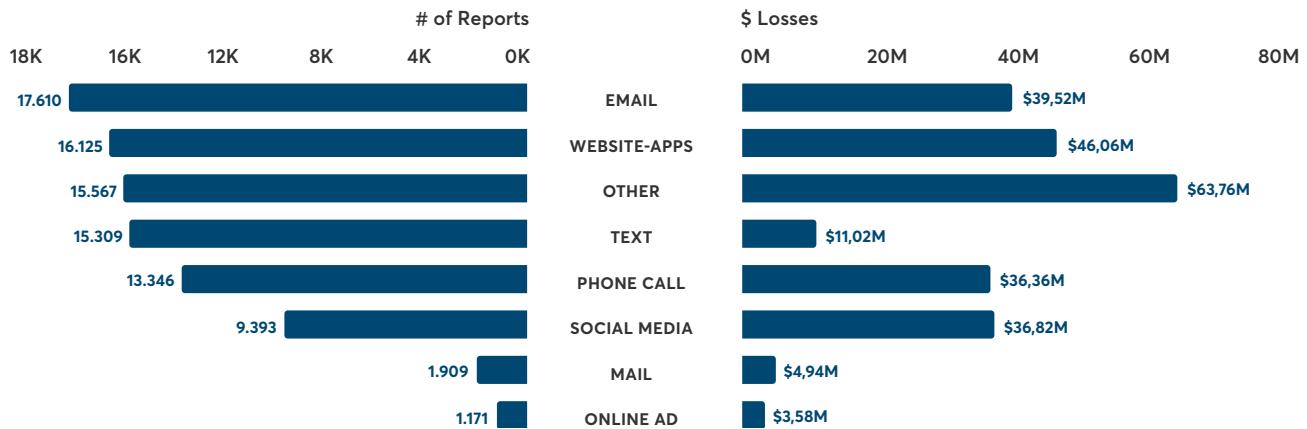
347.945 Total Fraud Reports

\$519.43 M Total Fraud Loss

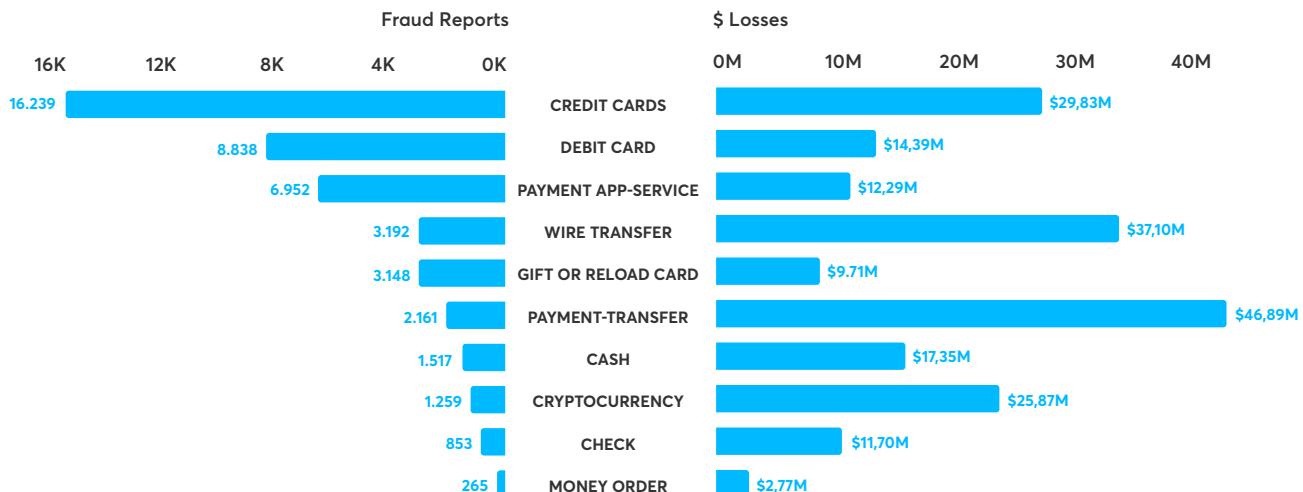
\$376 Median Fraud Loss

Grafico 3 - Fonte: FTC COVID-19 and Stimulus Reports

Contact Method



Payment Method



L'insieme di strumenti di contatto non riconducibili ai canali principali specificati nella ricerca e identificati con "Other" hanno generato i volumi di perdite più consistenti, raggiungendo nel periodo preso in esame un volume di 63,76 milioni di dollari.

Se si analizzano gli strumenti di pagamento, sono le carte di credito a raggiungere il numero più elevato di segnalazioni (16.239), ma in termini di

ammontare i bonifici con 46,89 milioni di dollari e le rimesse di denaro (*wire transfer*) con 37,10 milioni di dollari le superano abbondantemente. Interessante notare il valore medio delle truffe finalizzate con le crypto-valute che rispetto ai 1.837 dollari delle carte di credito sale a 20.548 dollari, anche se va considerata l'alta volatilità del controvalore di questi strumenti e dunque andrebbero approfondite le quotazioni prese in considerazione in fase di raccolta dei dati.

Il cyber-crime in Europa

Anche l'Unione europea sta aumentando gli sforzi in favore della lotta al cyber-crimine. La comunicazione congiunta al Parlamento e al Consiglio Europei "The EU's Cybersecurity Strategy for the Digital Decade" ha riconosciuto la cybersecurity come parte integrante della sicurezza dell'Unione: che si tratti di dispositivi connessi, banche, pubbliche amministrazioni o ospedali, tutta la popolazione ha il diritto di fruire di servizi con la sicurezza di essere protetta da eventuali minacce digitali.

Secondo l'Unione europea, economia, democrazia e società dipendono tutte da strumenti e connettività più sicuri e affidabili che sono anche essenziali per costruire un'Europa resiliente, eco-sostenibile e digitale.

"L'Europa è determinata a portare avanti una trasformazione digitale della nostra società ed economia, che dobbiamo quindi sostenere con livelli di investimento senza precedenti. La riuscita della trasformazione digitale, che sta accelerando, si basa sulla fiducia dei cittadini e delle imprese nella sicurezza dei prodotti e dei servizi connessi che utilizzano."



Margrethe Vestager, Vicepresidente esecutiva dell'Office per Un'Europa pronta per l'era digitale³

Dati pubblicati da GSMA⁴, l'organizzazione che rappresenta gli interessi di 750 operatori di rete mobile e 400 aziende del settore in tutto il mondo, confermano che entro il 2025 l'IoT (internet of

things) vedrà oltre 25 miliardi di dispositivi connessi che potranno generare un potenziale economico di oltre 1,1 trilioni di dollari, 242 miliardi dei quali solo per il mercato europeo. Numeri che rappresentano grandi opportunità per il settore dell'Ecommerce e, allo stesso tempo, anche per le organizzazioni criminali di tutto il mondo.

"La cyber-sicurezza è un elemento centrale dell'Unione della sicurezza. Non esistono più distinzioni tra minacce online e offline e la dimensione digitale è ormai indissolubilmente connessa alla dimensione reale."



Margaritis Schinas, Vicepresidente per la Promozione dello stile di vita europeo³

Nonostante gli sforzi di tutti gli organi istituzionali e delle aziende private del settore sicurezza nella lotta al crimine informatico, i cittadini europei mostrano ancora diffidenza nei confronti dell'ecosistema digitale, soprattutto in tema di gestione dei dati. È quanto emerge da "Crime, safety and victims' rights"⁵, uno studio pubblicato a febbraio 2021 dall'Agenzia europea per i diritti fondamentali (FRA) e basato su un sondaggio svolto nei 27 Paesi dell'Unione, Regno Unito e Macedonia del Nord, nel periodo gennaio – ottobre 2019 che ha coinvolto circa 35.000 rispondenti.

Nella ricerca, che include alcune domande relative alle frodi subite dai consumatori su carte di credito e online banking emergono, l'8% degli intervistati europei afferma di aver subito almeno una frode online negli ultimi 5 anni, dato che scende al 3% se si prendono come riferimento i 12 mesi precedenti all'intervista. I dati emersi in realtà sono molto variabili e vanno dall'1% al 19%, probabilmente

3 - Nuova strategia dell'UE per la cybersicurezza e nuove norme per rendere più resistenti i soggetti critici fisici e digitali, Commissione europea

4 - The Internet of Things by 2025, GSMA

5 - Crime, Safety and Victims' Rights, European Union Agency for Fundamental Rights

anche a causa della diversa penetrazione di questi servizi nei singoli Stati membri.

Uno scostamento rilevante emerge nel confronto tra persone con problemi di salute o disabilità e il resto della popolazione: il 14% della prima categoria afferma di aver subito una truffa di questo tipo nei 5 anni precedenti, contro il 6% del resto dei rispondenti.

Il 26% dei consumatori europei ha poi dichiarato di aver subito almeno una frode come consumatore su quantità, qualità, prezzo, spedizione di beni o erogazione di servizi nel quinquennio precedente all'indagine, dato che cala al 16% se si prende in considerazione solo l'ultimo anno antecedente all'inchiesta. Anche in questo caso le informazioni raccolte sono molto variabili a seconda del Paese di provenienza, infatti i risultati variano dall'8% al 46% a seconda della regione geografica.

Nel descrivere l'episodio più recente di frode subita, il 41% ha confermato di aver acquistato i beni o i servizi online, per telefono o per posta da un sito o azienda estera, dati che si sono rivelati molto più alti per alcuni Paesi come Lussemburgo (94%) e Malta (87%).

Reporting the most recent incident of three property crimes asked about in the survey (EU-27, %)



Grafico 4 - Fonte: Crime, Safety and Victims' Rights, European Union Agency for Fundamental Rights. Dati raccolti in collaborazione con CBS (NL), CTIE (LU) e Statistics Austria (AT)

Quasi tutti i cittadini europei coinvolti hanno denunciato agli ordini competenti le truffe legate all'utilizzo di servizi bancari online e frodi sulle carte di credito, chi alla Polizia (52%) chi ad altri canali (43%), mentre solo il 5% ha preferito astenersi. Il 50% delle frodi al consumatore sono state segnalate (il 7% alla Polizia e il 43% ad altri organi) mentre il restante 49% ha preferito non denunciare. Risulta molto variabile l'incidenza delle risposte relative alle frodi più recenti i cui valori registrati sono stati, ad esempio: Portogallo (69 %), Francia (65 %) e Germania (60 %) hanno avuto un peso più elevato rispetto a Grecia (25 %), Croazia (28 %), Slovenia (29 %) e Svezia (30 %).

Secondo le persone coinvolte, a fare da deterrente sono spesso i costi da sostenere per un eventuale contenzioso a causa della mancanza di procedimenti dei sistemi giudiziari economicamente sostenibili e di risorse economiche per la tutela dei consumatori. Non solo, le ragioni delle mancate denunce di frodi ai danni del consumatore sono state anche altre:

Il 49% ha ritenuto di scarsa importanza quanto subito;

Il 25% ha desistito, nella convinzione che la denuncia non sarebbe servita a nulla.

Mentre per quanto riguarda le truffe subite sulle carte di credito e debito o tramite online banking:

Il 22% ha ritenuto quasi irrilevante la gravità di quanto subito;

Il 22% ha dichiarato di non aver provveduto per mancanza di prove;

Il 21% non ha denunciato perché si è occupata personalmente di gestire l'accaduto;

Il 28% ha dichiarato altre motivazioni, rispetto a quelle previste nel sondaggio.

Dall'inchiesta dell'Agenzia europea per i diritti fondamentali emerge quindi un quadro di incertezza del cittadino, inoltre almeno un quarto delle persone coinvolte ritiene di scarsa utilità denunciare le attività illecite nell'ambito dei pagamenti e in qualità di consumatori, dimostrando di fatto poca fiducia negli strumenti messi a loro disposizione.

La situazione delle frodi online in Italia

Il tema delle frodi online è di estrema attualità in tutto il mondo, sia per gli impatti economici sia per quelli legati alla sicurezza nazionale. In Italia il 4 agosto 2021 è stata pubblicata in Gazzetta ufficiale la Legge n. 109, conversione con modificazioni del Decreto Legge n.82 del 14 giugno 2021 relativo alle disposizioni urgenti in materia di cyber-sicurezza e in particolare per l'istituzione di un'Agenzia di cyber-sicurezza nazionale, quale fattore necessario per assicurare lo sviluppo e la crescita dell'economia e dell'industria nazionale, ponendo la cyber-sicurezza a fondamento della trasformazione digitale.

Sul sito della Polizia di Stato è disponibile il Report 2020⁶ sulla situazione delle minacce e delle truffe sul web nel nostro Paese. Dai quanto pubblicato si evince che durante il primo anno di pandemia le truffe online sono aumentate, avvicinandosi a 100mila. La Polizia postale ha poi concluso 14 indagini anche sul dark web, sia in Italia sia all'estero, con un aumento del 132% dei casi trattati, del 93% di indagati, dell'86% di arresti e del 48% di perquisizioni, registrando anche un incremento del 69% di materiale sequestrato.

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) nel corso del 2020 ha identificato 507 minacce, in aumento del 113% rispetto alle 239 del 2019. L'aumento delle minacce informatiche ha certamente un legame con l'aumento, anche in Italia, delle aziende che hanno fatto ricorso allo smart working, di fatto aumentando le opportunità per i cracker. In questo ambito sono stati effettuati 21 arresti su 99 indagini, 3 delle quali iniziate nel 2019, con 79 denunce e oltre 79mila alert.

Con riferimento particolare ai crimini di tipo economico-finanziario, l'attività investigativa ha permesso di identificare ed indagare 3.741 truffatori. Oltre ad un aumento globale del 600% nel numero di e-mail di phishing che utilizzavano temi correlati al Coronavirus per colpire persone e aziende, per quanto concerne il contrasto al *cyber-crime* finanziario, la Polizia Postale ha identificato 48 imprese medio grandi frodate per 25 milioni di euro, 15 dei quali recuperati, e indagato 674 persone a cui sono seguiti 24 arresti.

Per contro, i dati italiani emersi nel report "Crime, safety and victims' rights", citato nel capitolo precedente, sono risultati molto sotto la media europea: rispettivamente il 3% per le frodi subite nei cinque anni precedenti all'intervista e l'1% nei 12 mesi precedenti. È bene considerare però che il 21% delle persone coinvolte ha dichiarato di non usare servizi di online banking o carte di credito e debito, rispetto ad una media europea dell'11%. Per avere un termine di paragone è possibile confrontare questi risultati con quelli del Regno Unito, in cui il 24% dice di aver subito una truffa nel quinquennio preso in esame e il 10% negli ultimi 12 mesi, mentre solo il 2% ha risposto di non utilizzare servizi bancari online o carte di pagamento.

Dalla ricerca emergono correlazioni tra le diverse generazioni dei rispondenti: all'aumentare dell'età diminuisce l'uso di servizi finanziari digitali e quindi anche l'incidenza delle frodi. Anche le condizioni fisiche dei rispondenti al sondaggio possono contribuire alla variabilità delle risposte, infatti le persone con problemi di salute o disabilità, tipicamente più propense all'uso di questi servizi, hanno subito più truffe di chi non si trovava nelle stesse condizioni.

Le tecniche utilizzate per le frodi online

Tra le difficoltà riscontrate da chi si occupa di contrastare il fenomeno delle frodi online c'è l'impegno crescente, di tutti gli attori coinvolti, per restare al passo con l'evoluzione continua degli strumenti utilizzati per perpetrare questi atti illeciti. Di seguito, abbiamo raccolto alcune delle tecniche più utilizzate, con analytics e approfondimenti di scenario.

Account Takeover

L'espressione [account takeover](#) (ATO) si riferisce alla pratica fraudolenta di furto dell'identità online di un soggetto per ottenerne profitto, facendo acquisti online o per altre attività criminose, ai danni di consumatori e aziende.

Secondo un'analisi elaborata da Sift⁷, società che si occupa di prevenzione frodi nei pagamenti, i tentativi di account takeover del suo network sono cresciuti del 282% tra il secondo trimestre del 2019 e lo stesso periodo del 2020.

A conferma della rilevanza di questi attacchi c'è anche un recente ricerca pubblicata da Arctic Wolf⁸, azienda che opera nel settore della sicurezza aziendale, che analizzando i dati nei primi sei mesi del 2020 ha riscontrato un aumento del 429% di credenziali esposte sul dark web e ha rilevato un aumento di casi di phishing e ransomware pari al 64% nel secondo trimestre, confrontando i due trimestri dello stesso anno.

Authorised Push Payments (APP)

Anche le attività fradudolente legate agli Authorised Push Payments (APP), ossia quei casi in cui il la vittima viene convinta ad inviare denaro al frodatore, generano volumi consistenti: nel 2020 solo nel Regno Unito, secondo l'associazione

bancaria UK Finance⁹, questi attacchi sono costati 479 milioni di sterline, rispettivamente 387,8 milioni ai danni di consumatori e 91,3 milioni spesi dalle aziende.

Secondo GBG¹⁰, azienda che opera nell'ambito della data intelligence e prevenzione frodi, queste attività sono particolarmente efficaci e potrebbero diventare la minaccia online più rilevante del 2021, inficiando ulteriormente sui bilanci aziendali.

Malware

I malware sono programmi tipicamente condivisi come allegati tramite e-mail o salvati su supporti di memoria (es. chiavette USB, hard disk portatili, ecc.) che una volta aperti danno accesso ai dispositivi dell'utente, al quale vengono cari dati riservati per poi essere utilizzati per scopi illeciti, come ad esempio pagamenti non autorizzati.

SONICWALL, azienda specializzata in soluzioni per la sicurezza informatica, ha realizzato una ricerca¹¹ sulle principali minacce online nella quale i malware risultano in calo. Gli attacchi registrati nel primo semestre 2021 sono stati pari a 2,5 miliardi, per la prima volta in dieci anni di monitoraggio il numero risulta in calo del 22% rispetto allo stesso periodo dell'anno precedente. Nel 2010 i volumi erano pari a 8 miliardi e nel 2018 hanno raggiunto un massimo di 10,5 miliardi di attacchi, per poi scendere a 5,6 miliardi nel 2020.

Nonostante la decrescita di minacce malware a livello globale, lo studio ha evidenziato un incremento del 23% in Asia. Nord America ed Europa hanno avuto un calo rispettivamente del 25% e del 13%, con l'eccezione della Germania che ha registrato nella prima parte dell'anno un incremento anomalo del 465%.

7 - Digital Trust & Safety Index: Account Takeover Fraud and the Growing Burden on Business, Sift

8 - Security Operations Annual Report, Arctic Wolf

9 - FRAUD – THE FACTS 2021, UK Finance and LexisNexis

10 - GBS Fraud Survey 2020, GBG

11 - 2021 MID-YEAR UPDATE CYBER THREAT REPORT, SONICWALL

Pharming

Con la parola *pharming*, neologismo creato dall'unione delle parole *phishing* (una tecnica per acquisire dati personali di cui parleremo in seguito) e *farming* (coltivare), ci si riferisce alle attività illecite poste in essere per accedere ad informazioni personali e riservate degli utenti che, inconsapevolmente, accedono a siti clone molto simili se non identici a quelli originali.

L'attività di *pharming* può avvenire grazie all'installazione di un virus sul dispositivo dell'utente o tramite l'accesso fraudolento ai server DNS del provider internet. In entrambi i casi l'utente, pur digitando correttamente l'indirizzo di un sito come quello della propria banca, atterra su un sito clone dal quale chi ha attuato la truffa può carpire, ad esempio, i dati di accesso ai servizi di internet banking o numeri e codici delle carte di pagamento.

Phishing

La tecnica del *phishing* consiste nell'invio di un'e-mail a nome di un'azienda – tipicamente una banca o un sito Ecommerce - i cui contenuti sembrano a tutti gli effetti riconducibili al mittente, nella quale vengono richiesti dati riservati che poi verranno utilizzati per: trasferimenti di denaro, acquisti online o attività illecite come la vendita nel deep web dei dati sottratti o la richiesta di un riscatto.

In alcuni casi l'e-mail contiene un link che atterra su una pagina clonata della società anch'essa vittima del raggio – ad esempio una banca - per rendere ancora più credibile la comunicazione e la legittimità della richiesta delle credenziali.

Il caso d'uso più conosciuto è quello in cui vengono rubati i dati di accesso a servizi bancari e finanziari grazie ai quali i criminali riescono a effettuare trasferimenti di denaro a proprio favore. In altri casi vengono carpiti le credenziali per accedere a un sito Ecommerce dal quale vengono poi effettuati acquisti con gli strumenti di pagamento salvati dall'utente, non prima di aver modificato destinatari e indirizzi di spedizione. I dati pubblicati a marzo 2021 da Trend Micro¹², multinazionale americana-giapponese di software per la sicurezza

informatica, mostrano che nel 2020 i loro servizi cloud-based hanno identificato e bloccato oltre 16,7 milioni di minacce via e-mail, pari ad oltre il 32% in più rispetto all'anno precedente. Di queste, 5.465.969 sono attacchi riconducibili ad attività di *phishing* che sono aumentati del 14% rispetto al 2019.

Credential phishing attacks

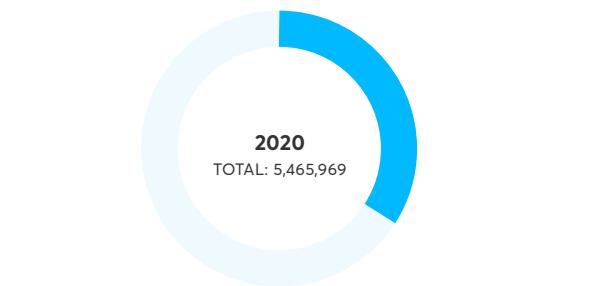
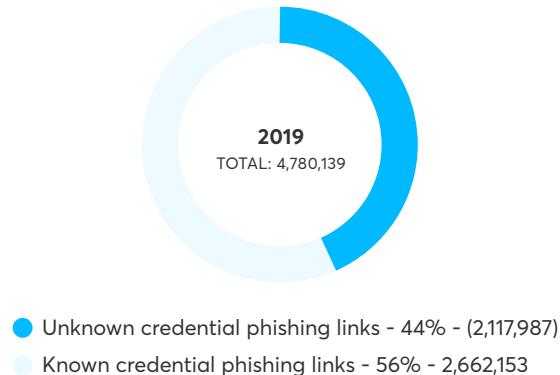


Grafico 5 - Fonte: Trend Micro Cloud App Security Threat Report 2020, Trend Micro

Anche a causa dell'impiego sempre più frequente dello smart working in molte aziende, tramite gli attacchi di *phishing* vengono eseguite altre tecniche fraudolente, come gli attacchi BEC (*Business Email Compromise*). Similmente a quanto accade nei casi di APP descritti in precedenza, in questi casi i cyber-criminali inviano e-mail a nome di manager o figure apicali dell'azienda verso altri dipendenti e, grazie alla capacità di rendere queste comunicazioni indistinguibili da quelle autentiche, li convincono ad effettuare pagamenti o trasferimenti di denaro a favore di conti correnti ipoteticamente intestati a fornitori, per citare un esempio, ma in realtà riconducibili o accessibili dai criminali stessi. Secondo un recente documento di Mimecast¹³,

12 - Trend Micro Cloud App Security Threat Report 2020, Trend Micro
13 - The State of Email Security Report, mimecast

società che opera nell'ambito della sicurezza informatica, nel 2020 le minacce via e-mail sono cresciute del 64%, incentivate anche dal picco di adozione dello smart-working, e i click su link non sicuri con l'avvento della pandemia sono arrivati al 300% rispetto al periodo precedente. Il dato richiede profonde riflessioni da parte di tutto l'ecosistema, soprattutto se si considera che il 13% delle aziende coinvolte nella ricerca non ha un sistema di sicurezza per le e-mail e che solo un quinto ha previsto corsi di approfondimento sul tema della cyber-sicurezza.

Ransomware

Un ransomware, parola composta da ransom (riscatto) e malware, è un software che una volta installato su un dispositivo, ne permette l'accesso solo a chi ha realizzato la truffa. In seguito, alla vittima viene richiesto un riscatto per poter entrare nuovamente in possesso dei suoi dati.

Anche questo fenomeno è in costante crescita: secondo un report pubblicato da Cybersecurity Ventures¹⁴, dal 2021 al 2031 l'incremento di queste attività sarà pari al 30% anno su anno, arrivando a far registrare entro 10 anni un ransomware ogni 2 secondi con un costo per aziende e consumatori di 265 miliardi di dollari.

L'Internet Crime Complaint Center solo nel 2020 ha registrato 2.474 denunce per un totale di oltre 29 milioni di dollari di perdite.¹⁴ Va considerato poi che molte delle persone coinvolte da questo tipo di truffa non denunciano sia per scarsa fiducia nell'esito delle eventuali indagini sia perché diffidenti nel rilasciare dati personali, essenziali per circoscrivere l'accaduto.

SIM Swapping

Il SIM swapping, anche detto SIM swap, consiste nell'ottenere l'accesso al numero di telefono di uno o più utenti per finalità illecite, in particolare l'intento di prassi è quello di poter effettuare autenticazioni 2FA (autenticazione a due fattori) e

quindi accedere a servizi o effettuare pagamenti al posto del legittimo proprietario dell'utenza.

Chi realizza questo tipo di attacchi raccoglie quanti più dati possibile della persona in target, per esempio tramite attività di social engineering, per poi chiedere all'operatore telefonico la sostituzione della SIM per smarrimento impersonando la vittima.

L'ufficio di polizia europeo (Europol) ha dichiarato recentemente che il fenomeno del SIM swap è in crescita¹⁵, anche a fronte del fatto che l'autenticazione a due fattori è sempre più richiesta dalle piattaforme online, come i social network e le piattaforme di crypto exchange. Anche i volumi riconducibili a questi eventi, relativamente recenti, sono difficili da quantificare a livello globale ma per avere un quadro indicativo è possibile fare riferimento ai comunicati dell'ufficio di polizia europeo. A febbraio 2021, proprio Europol ha dichiarato di aver contribuito all'arresto di dieci hacker sospettati di aver sottratto cryptovalute per un controvalore indicativo di 100 milioni di dollari attraverso l'uso di questa tecnica.¹⁶

Poco meno di un anno prima, a marzo 2020 per la precisione, la stessa agenzia in collaborazione con gli organi di polizia spagnoli, rumeni e austriaci, aveva comunicato l'arresto di decine di membri di diversi gruppi di persone che hanno generato profitti illeciti per oltre 3 milioni di euro.¹⁷

SMSishing

Lo SMSishing si differenzia dal phishing per il canale di comunicazione. Nel primo caso si tratta sempre di e-mail mentre in questo frangente i malintenzionati utilizzano gli SMS. Se si considera che in Italia, negli ultimi 3 anni, l'uso di SMS è cresciuto del 35%¹⁸, nonostante l'utilizzo ormai consolidato di piattaforme di messaggistica alternative come Whatsapp, Telegram o Signal solo per citarne alcune, è facile capire quale sia il potenziale per chi ha intenzioni criminali.

14 - Global Ransomware Damage Costs, Cybersecurity Ventures

15 - COVID-19 sparks upward trend in cybercrime, Europol

16 - Europol: 10 held for alleged \$100m cryptocurrency theft from celebs, others, Reuters

17 - The SIM highjackers: how criminals are stealing millions by highjacking phone numbers, Europol

18 - Mobile Messaging Adoption Report 2021, Esenex e PricewaterhouseCoopers (PwC)

Ciò che rende questo canale particolarmente appetibile per i truffatori è il tasso di apertura dei messaggi di testo che supera il 93%, numeri ben al di sopra di quelli delle e-mail che, sebbene molto variabili a seconda di diversi fattori come la qualità del database, l'orario di invio o l'efficacia dell'oggetto, sono ben al di sotto degli sms. È bene tenere in considerazione poi che l'sms è lo strumento di comunicazione istantanea più comune per un pubblico che ha meno cultura digitale e quindi più appetibile proprio per i criminali del digitale.

Vishing

È la pratica che consiste in una chiamata telefonica da parte di chi, fingendosi un operatore di un'azienda, spesso una banca, chiede alle vittime alcuni dati personali utili per finalizzare una truffa, tipicamente un bonifico in uscita dal conto corrente della vittima. Alla telefonata spesso può seguire l'invio di un'e-mail di phishing, in molti casi giustificata da chi sta chiamando per vincere l'insicurezza del malcapitato che preferisce non fornire dati personali al telefono. Anche questa tecnica si presta non solo al raggiro di consumatori ma anche a quello di dipendenti aziendali. Non sono infrequentati casi in cui tramite telefonate apparentemente provenienti da un ufficio interno – tipicamente l'help desk – è stato chiesto a ignari dipendenti di installare un nuovo software aziendale che poi si è rivelato essere un malware. Solo nel 2020, le attività registrate da IC3¹⁹ riconducibili a pharming, phishing, smishing e vishing hanno generato una perdita superiore a 54 milioni di dollari. Ci sono però anche nuovi media e strumenti che stanno guadagnando posizioni nella classifica delle minacce più frequenti, sfruttando piattaforme sempre più utilizzate dagli utenti online.

APP malevole

Quando si tratta di ottimizzare l'accesso ai propri servizi tramite dispositivi mobili spesso la scelta delle aziende ricade sullo sviluppo di un'app. Al proliferare di applicazioni legittime purtroppo si

affianca quello di app malevole che possono essere cloni di altre app o semplicemente applicazioni con finalità crimonose; in entrambi i casi il loro scopo è unicamente quello di carpire i dati personali dell'utente che le utilizza.

Secondo l'ultimo report trimestrale di Outseer²⁰, società di RSA che si occupa di sicurezza a livello globale, il 63% di tutte le transazioni fraudolente sono state generate da mobile e di queste il 47% è avvenuto tramite app. Non solo, all'aumento delle transazioni è corrisposto anche un incremento medio del valore di questi pagamenti pari al 17%, segno che le attività illecite poste in essere hanno aumentato la loro efficacia.

Fraud transaction distribution by channel

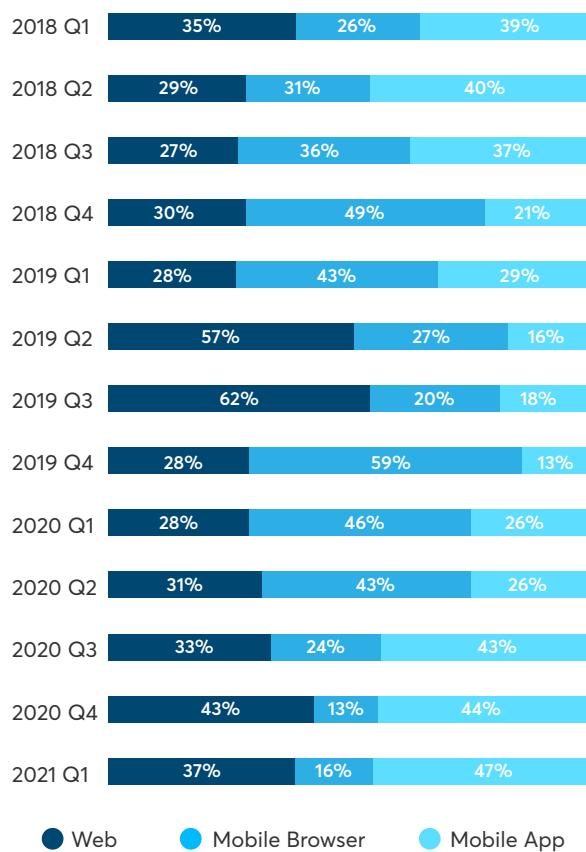


Grafico 6 - Fonte: Q2 2021 Outseer™ Fraud & Payments Report, Outseer (RSA)

Social Media

I social media sono le piattaforme digitali sulle quali gli utenti online spendono più tempo: 145 minuti al giorno a livello globale. Anche per questo

19 - Internet Crime Report 2020, Internet Crime Complaint Center (FBI)
20 - Q2 2021 OutseerTM Fraud & Payments Report, Outseer (RSA)

sono fonte inesauribile di informazioni che possono essere utilizzate per perpetrare truffe online; essendo piattaforme la cui natura stessa stimola la condivisione di informazioni, spesso anche molto personali, il rischio è che queste possano essere utilizzate per attività illecite legate al furto di identità tramite le tecniche di *social engineering*, ossia la raccolta e l'analisi di dati degli utenti per studiarne il comportamento e, in alcuni casi, compiere atti illeciti a loro danno o in loro nome.

Secondo il report di RSA citato in precedenza²⁰, i casi di Brand Abuse, ossia l'insieme di attività fraudolente che sfruttano il nome di un Brand a sua insaputa, solo nel primo trimestre del 2021 sono stati oltre 28.000 (il 56% di tutti gli attacchi identificati da Outseer, contro il 27% del 2020). Secondo RSA, l'incremento di queste minacce è da ricondurre principalmente all'uso intensivo dei social media nei periodi in cui la pandemia si è dimostrata più acuta.

Un sondaggio di PwC²¹ che ha coinvolto 3.249 dirigenti negli ambiti business e IT di società internazionali, ci permette di chiudere questo capitolo con alcuni dati sul futuro della cybersecurity in ambito aziendale.

21 - 2021 Global Digital Trust Insights, PwC

Circa il 96% delle aziende coinvolte ha dichiarato di dover cambiare la strategia in materia di sicurezza informatica a causa della pandemia e il 50% ha confermato di considerare gli aspetti legati alla cyber-security in ogni decisione di business. In molti casi è aumentata la sensibilità sul tema della sicurezza:

- il 44% degli intervistati ha identificato nuovi processi di budgeting per la spesa in sicurezza e di quantificazione dei rischi e il 43% ha incrementato i confronti tra CISO e CEO e i test di resilienza, per ottenere una probabilità più bassa di subire eventi di grande impatto.
- Il 55% dei rispondenti ha previsto un aumento del budget dedicato per il 2021;
- L'8% ha programmato un aumento di spesa anche superiore al 10%;
- Il 22% ha messo a budget costi che si attesteranno tra il 6% e il 10%;
- Il 25% spenderà fino al 5% in più.
- Il 13% delle aziende interessate dal sondaggio manterrà invariato il budget dedicato alla cyber-sicurezza mentre il 27% ridurrà gli investimenti in questo ambito. Solo il 5% non ha ancora preso decisioni in merito a quanto allocare per questo settore.

Gli ambiti di spesa dichiarati dagli executive interpellati sono vari e si possono riassumere come segue:

- Persone e hard skill
- Capacità e processi
- Tecnologie
- Architettura
- Automazione

Particolare importanza viene data al passaggio in cloud di operations (75% degli intervistati) e sicurezza (76% degli intervistati), sia per ridurre le frizioni interne sia per semplificare l'accesso dei loro clienti a prodotti e servizi.

I dati che emergono dalla ricerca di PwC sono in linea con quanto emerso da un'indagine di

Gartner²² che a settembre del 2020 ha coinvolto alcune aziende sul tema della sicurezza informatica. Dal sondaggio è emerso che il 67% delle società interessate ha intenzione di aumentare di circa il 7% quanto preventivamente allocato per tutelare i loro sistemi da attacchi online, puntando in particolare sull'intelligenza artificiale.

In definitiva il tema della sicurezza online è centrale e sempre più parte integrante delle strategie di tutte le aziende a livello globale, a prescindere da dimensioni e settori merceologici in cui operano. Nonostante sensibilità e investimenti su questi temi siano in costante crescita, quanto e come si ripercuotono sui conti economici degli Ecommerce i danni provocati dalle frodi online?

Le frodi Ecommerce: quanto costano all'intero sistema e come prevenirle

Il settore dell'Ecommerce a livello globale nell'ultimo anno e mezzo è cresciuto, con alcune eccezioni dovute alle restrizioni imposte da molti governi per far fronte alla pandemia, come i settori del turismo e della ristorazione in presenza, per esempio. Tra le molte fonti che confermano il trend tendenzialmente positivo delle vendite online si è aggiunto di recente il sondaggio "June 2021 Global Consumer Insights Pulse"²³ condotto da PwC che, a marzo e poi a giugno di quest'anno, ha intervistato 8.600 consumatori provenienti da 22 Paesi.

Canali di vendita preferiti

	MARZO '21	GIUGNO '21	SCOSTAMENTO
Store fisici	42%	46%	9,50%
Computer	30%	34%	13,33%
Tablet	33%	38%	15,15%
Smartphone	39%	44%	12,82%
Assist. vocali	37%	42%	13,51%

Tabella 1 - Fonte: June 2021 Global Consumer Insights Pulse Survey, PwC

Nel report sono state raccolte le preferenze relative ai canali di acquisto degli intervistati ed è emerso che, per quanto concerne le spese online, tablet e assistenti vocali sono stati oggetto di un'accelerazione maggiore rispetto a computer e smartphone.

Oltre il 50% delle persone coinvolte ha dichiarato di considerarsi un acquirente più "digitale" rispetto alle rilevazioni degli anni passati di PwC e dunque anche per questo diventa strategico investire

sulla sicurezza, consolidando i risultati ottenuti nell'ultimo periodo dal settore e fidelizzando la clientela che si è trovata, costretta dal momento contingente, ad affidarsi a strumenti di acquisto e pagamento considerati fino a quel momento poco sicuri, anche solo per semplice diffidenza.

L'insicurezza dei consumatori, lo abbiamo visto, in realtà non si può ricondurre esclusivamente a pregiudizi o mancanza di conoscenza. Infatti, nonostante l'aumento della sicurezza sia un punto focale delle strategie di tutte le aziende che operano online, come vedremo in seguito, i costi relativi alla prevenzione e le perdite generate da attività illecite online continuano a crescere, gravando sia sui merchant sia sui loro clienti.

Quanto costano quindi le frodi online ai danni degli esercenti?

È difficile quantificare con precisione le perdite subite dagli esercenti a livello globale e i motivi sono molteplici. Innanzitutto, non esiste un database condiviso dai merchant o dagli acquirer, inoltre l'offerta di sistemi di pagamento disponibili al mondo è molto frammentata e tenere traccia di tutti gli eventi illeciti registrati dai singoli strumenti e da tutti i PSP oggi non è una strada percorribile. È possibile però analizzare alcune ricerche effettuate proprio nell'ambito dei pagamenti online per tracciare dei perimetri, anche se solo indicativi, e disegnare un quadro generale da cui partire per impostare scelte di business consapevoli in materia di sicurezza e prevenzione.

FIS, player internazionale nell'ambito dei sistemi di pagamento, ha da poco pubblicato gli esiti di

23 - The global consumer: Changed for good, PwC

un sondaggio commissionato a Forrester su un bacino di quasi 700 manager di grandi Ecommerce provenienti da 11 Paesi nel mondo²⁴. Dalla ricerca è emerso che quasi il 90% delle aziende coinvolte ha subito delle perdite a causa delle frodi sui pagamenti online e circa il 50% ha speso in prevenzione, solo nel 2020, dall'1% al 5% dei profitti.

Nel 38% dei casi, sempre secondo il sondaggio di FIS, le perdite corrispondono almeno al 6% dei ricavi al quale si devono comunque aggiungere i costi per implementazione di soluzioni legate a prevenzione e adeguamenti normativi (la normativa PSD2 per esempio).

Come evidenziato nel grafico 7, le sfide che hanno richiesto maggiore effort sono stati i costi legati agli aggiornamenti e proprio le integrazioni lato sicurezza come tokenizzazione e la gestione dei protocolli 3DS2.

What are the top payment challenges that your team faced in the last 12 months?

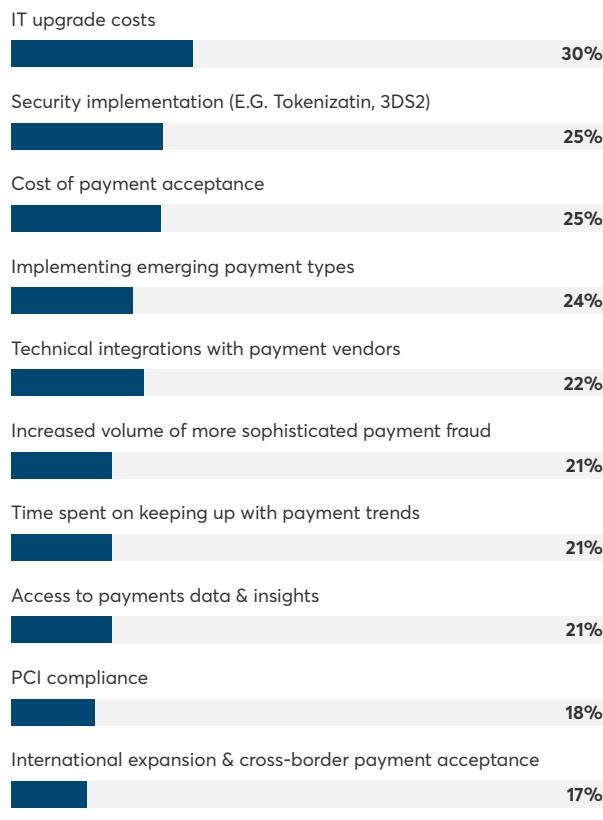


Grafico 7 - Fonte: Global Payment Risk Mitigation, FIS e Forrester

Un merchant su quattro ha ritenuto particolare sfidante l'integrazione di soluzioni di prevenzione frodi oltre sforzi profusi negli ambiti dell'accesso ai dati di pagamento e della conformità alle nuove normative introdotte.

In cima alla lista dei punti di attenzione che hanno contraddistinto il 2020 delle aziende europee intervistate, ci sono PSD2 e tokenizzazione (28% dei rispondenti). Il 27% dei manager nordamericani ha identificato tra le sfide più importanti del 2020 l'integrazione di sistemi di sicurezza, dato che sale al 30% per il mercato sudamericano.

How challenging are the following to your business today?

	PAYMENT FRAUD	CUSTOMER DATA SECURITY
Critical challenge	22%	20%
Very challenging	33%	31%
Not challenging	4%	5%

Grafico 8 - Fonte: Global Payment Risk Mitigation, FIS e Forrester

In ogni caso Fraud Prevention e Sicurezza dei dati dei clienti sono stati i due fattori più impegnativi per la maggior parte degli intervistati, rispetto ad esempio alla complessità di integrare e gestire soluzioni di pagamento multiple, fattore critico solo per il 18% degli intervistati. Il 55% degli esercenti coinvolti ritiene particolarmente gravoso il tema della prevenzione frodi e oltre il 50% ha risposto allo stesso modo in materia di sicurezza dei dati dei clienti.

Tra gli effetti negativi della pandemia da COVID-19 rientrano anche le frodi ai danni degli Ecommerce. L'aumento delle vendite online, verificatosi in molti settori anche se non tutti come abbiamo già approfondito nel nostro articolo dedicato al [futuro del retail](#), si è dimostrato essere terreno fertile per i cyber criminali. A confermarlo anche le interviste di FIS: oltre l'80% dei rispondenti ha dichiarato di aver subito un numero pari o superiore di frodi rispetto al 2019, e il 59% ha riscontrato un aumento nelle truffe sui pagamenti card-not-present.

Has your company detected less, more or an equal amount of the following types of payment fraud in 2020 versus 2019?

	SIGNIFICANTLY MORE	SLIGHTLY MORE	SAME	SLIGHTLY LESS	SIGNIFICANTLY LESS
Card-not-present fraud	21%	38%	25%	12%	3%
Synthetic identity fraud	21%	34%	28%	11%	5%
Chargeback fraud	20%	35%	30%	11%	3%
Card testing	20%	33%	32%	12%	3%
Identity theft/new account fraud	20%	32%	30%	13%	5%
Friendly fraud	22%	29%	31%	13%	5%
Account takeover fraud	20%	30%	31%	13%	5%

Grafico 9 - Fonte: Global Payment Risk Mitigation, FIS e Forrester

La maggioranza degli intervistati ha segnalato anche un incremento delle cosiddette *friendly fraud* e il 20% ha riscontrato un costante aumento delle dispute di anno in anno.

Nel grafico 9 sono evidenziate le principali tipologie di frodi subite dalle aziende coinvolte dal sondaggio. Le frodi sulle transazioni *card-not-present*, come quelle Ecommerce e M.O.T.O., e i furti di identità combinata (*Synthtic Identity Fraud* per il mondo anglosassone) sono le truffe aumentate in modo più significativo.

Analizzando i dati per area geografica emerge una maggiore rilevanza delle truffe sui pagamenti *card-not present* in Europa (59%) e Nord America (67%) e di furti di identità combinata per l'area Asia-Pacifico (61%). In America del Sud, i pagamenti *card-not-present*, i chargeback e le transazioni *card testing*, ossia i micro-pagamenti per testare la validità di una carta, tipicamente clonata o rubata, hanno fatto registrare l'incremento maggiore.

Queste attività hanno avuto un impatto diretto e significativo su molte aree di business. Il 60% degli intervistati ha dichiarato di aver subito perdite economiche e di produttività, il 58% ha avuto ripercussioni dirette sul tasso di abbandono dei clienti, su costi di back office e sui chargeback. Oltre il 50% ha specificato altre conseguenze

rilevanti, come ad esempio l'aumento dei costi legati a cause legali e all'ambito reputazionale oltre all'incremento degli storni e delle spese per mediazioni e sanzioni.

Le perdite economiche dovute a frodi online in alcuni casi raggiungono anche cifre considerevoli: il 4% del campione ha dichiarato di aver perso anche oltre l'11% del fatturato solo nel 2020. Il 34% sostiene di aver subito perdite tra il 6% e il 10% del fatturato, il 51% ha perso tra l'1% e il 5% e solo l'11% ha affermato di non aver subito perdite.

What risk management strategies does your company use to mitigate card payment fraud?



Grafico 10 - Fonte: Global Payment Risk Mitigation, FIS e Forrester

% Distribution of Fraud Losses by Domestic / International Transactions

	2019		2020	
	DOMESTIC TRX	INTERNATIONAL TRX	DOMESTIC TRX	INTERNATIONAL TRX
DIGITAL GOODS				
SMEs	85%	15%	73%	27%
Mid/Large	86%	14%	78%	22%
PHYSICAL GOODS				
Mid/Large	74%	26%	69%	31%

Tabella 2 - Fonte: 2020 True Cost of Fraud™ Study E-commerce/Retail Report, LexisNexis

Tutte le aziende coinvolte naturalmente affrontano da tempo il tema e hanno adottato diverse soluzioni, singolarmente o in combinazione tra loro. Il 55% si avvale della verifica del dispositivo dal quale viene effettuato l'acquisto, il 51% gestisce i protocolli 3D – è bene considerare che la ricerca si riferisce al 2020, anno precedente all'attuazione di PSD2 e SCA – mentre il 48% applica analisi comportamentali.

Alle principali tecniche di prevenzione si aggiungono poi autenticazioni knowledge-based (es. 2FA), biometria, scoring interno e soluzioni basate sullo scambio di dati di settore. L'uso di tecnologie basate su intelligenza artificiale e machine learning viene considerato un fattore strategico molto importante dal 72% dei manager coinvolti, dato superato solo da: autenticazione a due fattori, analisi multicanale (web, app, ecc.) e analisi predittive, tutte considerate importanti dal 74% dei rispondenti.

Anche in questo caso, l'analisi per regione di provenienza delle aziende interessate dal sondaggio evidenzia alcune peculiarità. C-level e manager dell'area Asia-Pacifico (APAC) hanno sottolineato l'importanza di uno stack tecnologico facile da integrare, di insight in real-time e dell'autenticazione a due fattori come strumenti più utili per il rilevamento delle frodi.

Per il 73% dei merchant europei i fattori chiave identificati sono: l'applicabilità di soluzioni multichannel, l'autenticazione a due fattori (71% delle risposte) e i protocolli 3D Secure (70% delle risposte). Anche in Nord America le soluzioni

multicanale hanno ricevuto la maggioranza di risposte (76%), seguite dall'autenticazione a due fattori (73%) e gli insight azionabili in tempo reale (73%).

In Sud America la risposta più frequente è stata relativa alle analisi predittive, con l'84% dei rispondenti, al pari degli strumenti di intelligenza artificiale e machine learning, mentre l'autenticazione a due fattori è stata considerata strategica dall'80% delle aziende.

LexisNexis, società statunitense specializzata nell'analisi di dati e nell'offerta di soluzioni tecnologiche aziendali, ha effettuato un sondaggio coinvolgendo oltre 800 tra Ecommerce e Retailer statunitensi²⁵. I risultati hanno indicato un aumento dei costi legati alle frodi del 7,3% per retailer ed esercenti statunitensi. Nel 2019, quindi nel periodo pre-pandemia, ogni dollaro di frode ha maturato costi pari a 2,87 dollari in Canada e 3,13 dollari negli Stati Uniti.

Non solo, ad aumentare è stata anche la media di tentativi di frode andati a buon fine ai danni di medie e grandi imprese che, sempre in USA, sono cresciute del 43%-48%. I tentativi di frode mensili sventati dagli Ecommerce coinvolti invece, sempre secondo quanto emerso dal sondaggio, sono diminuiti del 68% circa.

Analizzando le risposte degli Ecommerce medio/grandi statunitensi che vendono beni digitali, il costo delle frodi per ogni dollaro è passato da 3,50 dollari nel 2019 a 3,73 dollari nel 2020 (+6,5%) mentre nel caso di beni fisici l'aumento è stato dell'8,7% (da 3,11 dollari a 3,38 dollari).

25 - LexisNexis® Risk Solutions 2020 True Cost of Fraud™ Study E-commerce/Retail Report US & Canada Edition July 2020

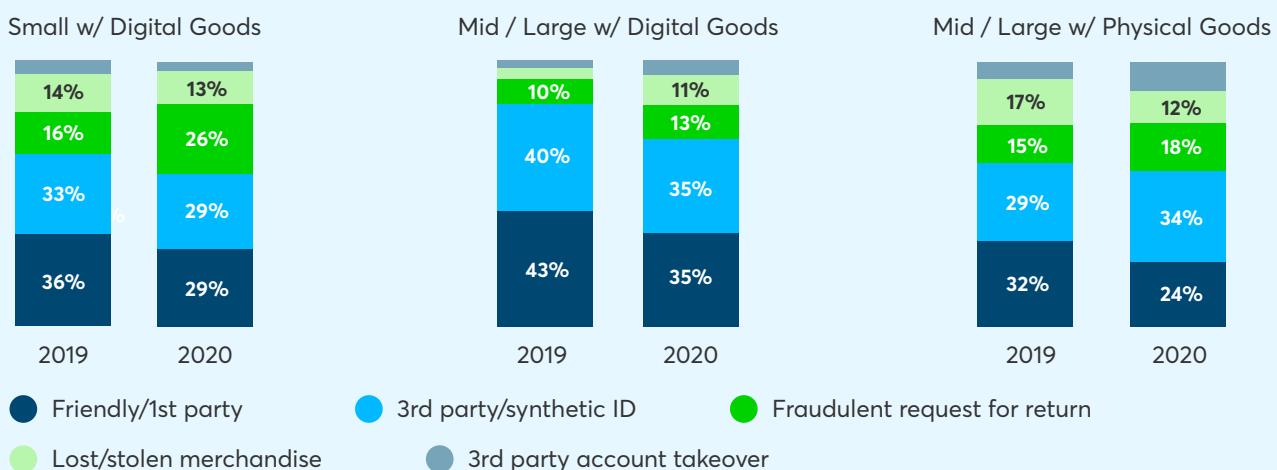
L'aumento delle perdite si è verificato in particolare per gli Ecommerce americani che vendono anche a clientela internazionale tramite il canale mobile. Come si evince dalla tabella 2, i costi maggiori sono legati alle transazioni domestiche ma va considerato che dal report emerge che molti attacchi sono avvenuti tramite l'uso di bot sofisticati, che possono ingannare i sistemi anche modificando l'origine geografica dell'acquisto.

Nei 12 mesi precedenti al sondaggio i merchant online statunitensi hanno subito principalmente friendly fraud e frodi di terze parti poste in essere con l'utilizzo di *synthetic ID*, ossia identità false e non riconducibili a persone esistenti ma create da

combinazioni di dati reali (es. numero di previdenza sociale) e altri inventati (es. indirizzo di residenza).

Un confronto tra 2019 e 2020 evidenzia l'uso ancora massiccio di tecniche legate ad account takeover o alla creazione di identità false. Solo nel caso delle piccole e medie imprese che operano nel campo dei beni digitali questa tipologia di frode riguarda poco meno del 50% dei casi (48%), mentre per le aziende medio-grandi i dati evidenziano tassi superiori al 60%, a prescindere dalla tipologia di beni venduti. Per quanto riguarda la distribuzione delle perdite da frode per metodo di pagamento, sono le carte di credito e debito a far registrare i dati più consistenti, con il 57% sul totale. Rispetto al 2019,

% Distribution of Losses by Fraud Type 2020 VS 2019



Identity Related Fraud: % Distribution by Activity

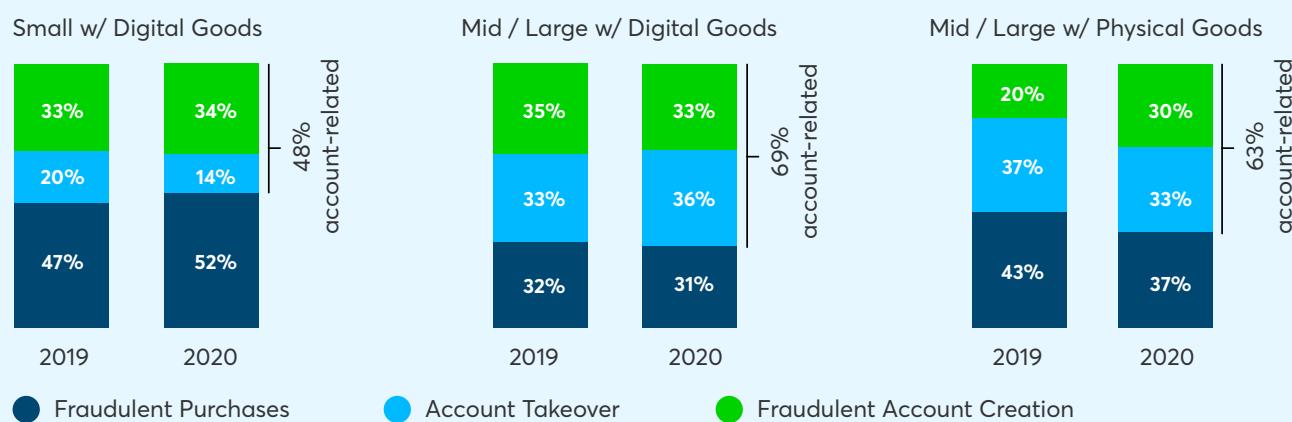


Grafico 11 e 12 - Fonte: Risk Solutions 2020 True Cost of Fraud™ Study E-commerce/Retail Report US & Canada Edition July 2020, LexisNexis®

gli Ecommerce statunitensi di piccole dimensioni coinvolti hanno riscontrato in particolare un aumento sulle transazioni card not-present fraudolente, che sono passate dal 41% al 55% del totale delle frodi con carta di credito su acquisti di beni digitali. Le perdite degli acquisti con carte rubate sono rimaste costanti nel tempo (27%), mentre per i pagamenti con carte contraffatte e fake o alterate sono diminuite, rispettivamente dal 15% al 10% e dal 14% al 7%.

Anche le aziende di media e grande dimensione che vendono beni digitali hanno visto accrescere i volumi sulle transazioni card-not-present, passate dal 45% del 2019 al 51% del 2020. Sono rimasti costanti le perdite derivanti dalle carte rubate (23%) e in leggera diminuzione le altre categorie. Per i beni fisici i dati sono invece tutti in aumento anche se non di molto. I pagamenti card-not-present nel 2020 hanno generato volumi saliti dal 43% al 44% mentre quelli con carte rubate sono passati dal 32% al 33%. È passato dal 15% al 19% invece il dato riconducibile alle operazioni con strumenti contraffatti e dall'11% al 12% quello con carte false.

Non sono solo le carte gli strumenti con le quali i merchant hanno subito attività illecite. Alla lista degli strumenti più utilizzati si aggiungono infatti i pagamenti alternativi come PayPal, BillMeLater e eCheck, per citare alcuni esempi, e tendenzialmente tutti gli altri metodi che hanno rappresentato il 20% del totale delle perdite nel 2019.

Frodi Ecommerce in Europa e Stati Uniti: il punto di vista di merchant e consumatori

Riskified, azienda internazionale la cui mission è consentire alle aziende di realizzare il pieno potenziale dell'Ecommerce rendendolo sicuro, accessibile e frictionless, ha pubblicato una ricerca²⁶ che ha coinvolto 4.000 consumatori e 400 retailer di Stati Uniti, Regno Unito, Francia e Germania, nella quale sono stati approfonditi

ulteriormente gli impatti delle frodi online mettendo a confronto il punto di vista di consumatori e merchant.

Dalla ricerca è emerso che i consumatori si aspettano di più dagli esercenti in termini di prevenzione, arrivando a ritenerli responsabili di quanto subito e, per questo, a non comprare più dai siti sui quali è stata perpetrata una frode ai loro danni. I merchant quindi si trovano a dover contrastare un fenomeno che genera ripercussioni economiche sotto molti punti di vista, inclusa la perdita di vendite potenziali.

"It's no surprise that the rapid growth of Ecommerce has also led to a rise in Ecommerce fraud, and as our research shows, the impact is significant for both merchants and consumers."



Peter Elmgren, Chief Revenue Officer di Riskified²⁷

Secondo il sondaggio di Riskified il 55% degli esercenti ritiene di essere in grado di prevenire le frodi online ma solo il 34% dei consumatori intervistati ha dichiarato di fidarsi delle capacità degli Ecommerce di impedire attività illecite. Il 26% dei retailer online coinvolti ha anche affermato che le frodi stanno danneggiando significativamente i profitti e il 34% ha quantificato perdite tra il 5% e il 10% del fatturato.

Si evince quindi una divergenza tra esercenti e acquirenti in termini di percezione della capacità di prevenire le truffe da parte del comparto delle vendite online. Per misurare le aspettative delle due categorie, Riskified ha creato l'indice eConfidence misurato in centesimi dove a 100 corrisponde il grado di fiducia medio dei rispondenti.

Per quanto riguarda i merchant, sono Stati Uniti e Regno Unito ad aver dimostrato un grado di sicurezza maggiore, con un punteggio rispettivamente di 111 e 112. Le risposte degli

26 - A Crisis of Confidence: Findings from the eConfidence Survey, Riskified

27 - The impact of eCommerce fraud on retailers and shoppers, HELPNETSECURITY

esercenti tedeschi hanno fatto registrare un risultato di 96 mentre la Francia è il mercato con i dati più bassi, 77 su 100.

Anche l'opinione dei consumatori statunitensi è superiore alla media, con 107 centesimi, mentre in UK la fiducia scende a 99. I consumatori tedeschi si attestano sul dato medio, 100 centesimi, mentre i francesi fanno registrare un punteggio pari a 94.

Consumer econfidence gap - By country

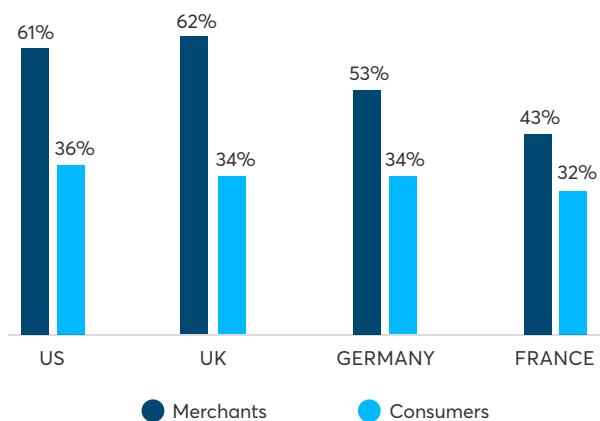


Grafico 13 - Fonte: A Crisis of Confidence: Findings from the eCofidence Survey, Riskified

L'analisi di Riskified mostra inoltre una differenza marcata tra esercenti e acquirenti, più consistente negli Stati Uniti e nel Regno Unito. In Francia invece la distanza si assottiglia, ma va tenuto conto del fatto che gli stessi esercenti hanno dimostrato una fiducia significativamente più bassa rispetto al resto dei Paesi coinvolti.

È molto importante inoltre tenere in considerazione che l'aumento delle vendite online dell'ultimo anno e mezzo è stato influenzato dalle restrizioni istituite dai diversi Paesi per contrastare il diffondersi della pandemia. Probabilmente quindi nel prossimo futuro si vedrà un ribilanciamento tra acquisti online e in-store, se non ai livelli pre-COVID comunque con un ridimensionamento di quelli Ecommerce.

Va considerato infatti che tra i motivi principali per i quali i cittadini europei non acquistavano

online nel 2019, secondo dati Eurostat²⁸, c'era proprio l'insicurezza nei confronti dei pagamenti, motivazione fornita da oltre il 20% del campione e seconda sola alla preferenza di molti per l'esperienza di acquisto in negozio (quasi l'80% dei rispondenti). Percezione che, con il continuo aumento delle minacce digitali di cui abbiamo parlato nei capitoli precedenti, non è inverosimile pensare che nell'ultimo periodo possa essere anche aumentata.

PSD2 e Strong Customer Authentication al fianco di tutto l'ecosistema Ecommerce

Lo abbiamo già scritto: la prevenzione frodi contribuisce positivamente a tutto l'ecosistema dei pagamenti online. Ne è consapevole anche l'Unione europea che ha introdotto la nuova normativa su pagamenti [PSD2](#) (Payments Service Directive 2) con il duplice obiettivo di aumentare la competizione nell'ambito dei pagamenti a livello pan-Europeo e migliorare la protezione sulla sicurezza dei consumatori, soprattutto per gli acquisti online, contribuendo a rafforzare la loro fiducia nei confronti di tutto l'ecosistema.

La nuova regolamentazione, la cui attuazione nell'ambito dell'Ecommerce è partita a gennaio del 2021, è ancora in una fase di assestamento in tutta Europa e vede l'Italia agli ultimi posti in termini di autenticazioni delle transazioni. L'introduzione del concetto di Strong Customer Authentication (SCA), ossia la necessità da parte dell'acquirente di autenticarsi per finalizzare un pagamento, ha di fatto aumentato la sicurezza dei pagamenti online ma, allo stesso tempo, ha aggiunto un passaggio ulteriore nel percorso di acquisto inficiando sul tasso di conversione dei carrelli.

Soprattutto i pagamenti con carte di credito e debito, utilizzati nella quasi totalità degli Ecommerce italiani come evidenziato anche nel grafico 14, non vengono sempre finalizzati proprio a causa della SCA.

Troppò spesso infatti l'autenticazione a due fattori

del pagamento può essere causa di una riduzione del tasso di conversione, come approfondito nel nostro whitepaper ["Strong Customer Authentication rate in Europa nel 2021"](#).

Share of the top 250 Italian online stores with at least one payment method belonging to the following categories

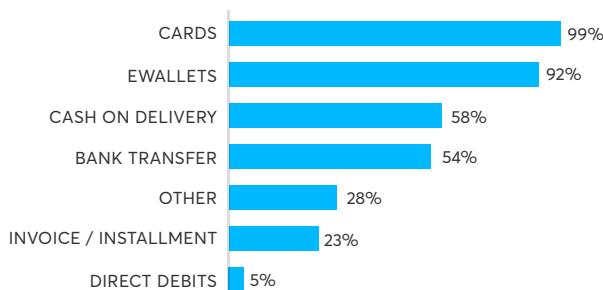


Grafico 14 - Fonte: Statista, Payments Analytics

Nel documento vengono presi in esame dati pubblicati da Mastercard che mostrano l'impatto della nuova normativa europea sui carrelli di tutti gli Ecommerce europei. L'autenticazione a due fattori introdotta dalla PSD2 ha sì l'obiettivo di ridurre l'impatto delle frodi ma, come emerge chiaramente dall'analisi dei dati, inficia sulla conversione dei carrelli, diminuendo di fatto i benefici legati alla potenziale decrescita delle perdite dovute alle attività illecite.

La Strong Customer Authentication infatti è a conti fatti una barriera all'ingresso che, in molti casi, non viene superata dal buyer. Secondo quanto osservato da Mastercard, durante il primo trimestre 2021 in Europa solo il 74,5% delle autenticazioni è andato a buon fine, con una distribuzione molto eterogena dei risultati. È il Regno Unito a confermarsi benchmark di riferimento, con l'89,5% delle autenticazioni finalizzate correttamente, mentre l'Italia si posiziona agli ultimi posti con un risultato che supera di poco il 60%, superando solo il Belgio che fa registrare il 56% circa di SCA superate con successo.

Non solo, in Italia sono le performance delle autenticazioni frictionless, cresciute soprattutto grazie alla capacità di 7 issuer di fare leva sulle

esenzioni, a far registrare il risultato meno soddisfacente: 12,7% contro una media europea del 29,6%. Il dato è particolarmente significativo soprattutto se si considerano i risultati di Paesi come la Spagna, nazione che nonostante sia stata tra le ultime a adottare il flusso 2.0 ha fatto segnare il 38,6% di autenticazioni frictionless andate a buon fine nel mese di aprile. Nonostante la nuova normativa PSD2 abbia l'obiettivo di aumentare la competizione nell'ambito dei pagamenti a livello pan-Europeo, migliorando la protezione sulla sicurezza dei consumatori, soprattutto per gli acquisti online, e offrendo loro nuove opportunità in materia di servizi finanziari, risulta evidente la necessità da parte di tutti gli stakeholder coinvolti di ottimizzarne l'attuazione nei processi di pagamento.

Occorre quindi che gli issuer introducano soluzioni in grado di migliorare la user experience dei consumatori in fase di autenticazione e che i merchant contribuiscano migliorando il processo di analisi del rischio dei pagamenti e mantenendo alto il livello di sicurezza senza inficiare sulle conversioni. L'adozione di soluzioni efficaci non solo in termini di prevenzione ma anche nell'identificazione di falsi positivi, ossia quei pagamenti genuini che potrebbero essere scambiati per fraudolenti da sistemi di prevenzione poco performanti, potrebbe essere la chiave di volta, sia per gli esercenti sia per i loro clienti.

Analisi del rischio e intelligenza artificiale: la risposta di Axerve alle frodi

Intelligenza artificiale e machine learning sono strumenti che possono contribuire attivamente al contrasto delle minacce sempre più sofisticate descritte nei capitoli precedenti. Il 27% delle aziende medio-grandi che operano nell'ambito dei beni digitali coinvolte dal sondaggio di LexisNexis²⁵ ha dichiarato di aver integrato questi strumenti, così come il 6% della stessa categoria di società che vendono prodotti fisici.

L'uso di soluzioni di prevenzione frodi però rischia di inficiare sulla customer experience del buyer, occorre dunque un'integrazione completa che allo stesso tempo sia in grado ridurre al minimo le frizioni in fase di pagamento. Solo il 34% dei merchant ritiene di aver raggiunto un equilibrio ottimale in questo senso, il 48% si considera mediamente soddisfatto e il 16% si dice insoddisfatto o non è in grado di rispondere con certezza.

Axerve Guaranteed Payments: l'intelligenza artificiale al servizio della prevenzione frodi

Partendo da queste premesse Axerve ha introdotto nella sua offerta una soluzione di prevenzione frodi basata su intelligenza artificiale e machine learning che si integra completamente con il gateway online. Riduzione dei punti di frizione del processo di pagamento, diminuzione dei chargeback e incremento del conversion rate sono solo alcuni dei punti di forza della piattaforma.

Il processo di elaborazione delle transazioni prevede una serie di passaggi che permettono di analizzare il rischio della transazione con estrema precisione, non solo raccogliendo dati direttamente dal merchant ma arricchendo gli ordini di acquisto grazie ad una serie di strumenti.



Axerve Guaranteed Payment raccoglie i dettagli dell'ordine dall'esercente.



Ogni ordine è collegato a tutti gli altri ordini nel database principale.



Gli ordini vengono valutati e quindi approvati, rifiutati e rielaborati per ulteriori informazioni.



La piattaforma arricchisce i dati provenienti da fonti interne ed esterne.



I modelli di machine learning rivedono le transazioni e restituiscono una decisione in una frazione di secondo.



Vengono esaminate le transazioni per verificarne l'accuratezza e osservare i trend più rilevanti per individuare eventuali anomalie.

I commercianti inviano i dettagli selezionati degli ordini da valutare, come le informazioni di contatto, i dettagli di spedizione e di fatturazione. Axerve Guaranteed Payment integra queste informazioni arricchendole tramite fonti esterne in grado di fornire, per esempio, la data di creazione dell'e-mail e i profili social media dell'acquirente.

Dopo aver raccolto dati esterni, ne vengono aggiunti altri elaborati internamente dalla piattaforma che, tramite un beacon, tiene traccia delle informazioni sugli acquirenti di tutti i siti che utilizzano lo stesso servizio di prevenzione frodi, inclusi il tipo di dispositivo, il comportamento sul sito e l'utilizzo di proxy.

La piattaforma viene perfezionata costantemente anche grazie ad analisti specializzati che contribuiscono all'evoluzione dei modelli. In definitiva, Axerve Guaranteed Payment è in grado di aumentare la conversione del carrello e, allo stesso tempo, di garantire il rimborso totale delle eventuali frodi non identificate.

Axerve Advice: come migliorare il conversion rate sulle autenticazioni

La soluzione per le esenzioni 3DS2 di Axerve offre ai merchant la possibilità di processare transazioni direttamente in autorizzativo, spostando la liability sull'esercente. Integrando anche il servizio di prevenzione frodi Axerve Guaranteed Payment, l'eventuale frode non riconosciuta verrebbe sostenuta al 100% da Axerve.

La TRA (Transaction Risk Analysis) consiste nella valutazione in tempo reale del rischio della transazione e permette l'eventuale esenzione dalla SCA delle transazioni inferiori a 500 euro. Le transazioni che presentano livelli di rischio di frode bassi possono essere elaborate senza autenticazione: inviandole con una richiesta di esenzione, le probabilità che vengano autorizzate aumentano ma la responsabilità di un'eventuale frode resta sul merchant.

Grazie alla soluzione di Axerve, descritta approfonditamente nel [whitepaper dedicato al rapporto tra SCA e conversion rate](#), le transazioni processate sono poi sottoposte ad alcune verifiche e, nel caso di superamento di questa fase, inviate direttamente all'autorizzativo, evitando l'autenticazione a 2 fattori. In fase di elaborazione dei pagamenti, vengono fatti alcuni controlli: La transazione deve essere all'interno della soglia prevista, in base all'acquirer; Se il rischio della transazione è basso, il pagamento viene inviato in esenzione altrimenti è necessario procedere con l'autenticazione.

La soluzione Axerve Advice ha quindi l'obiettivo di intervenire sull'analisi del rischio, migliorandone l'efficacia e contribuendo all'aumento del numero potenziale di transazioni finalizzate senza l'ausilio dei protocolli 3DS che, per loro stessa natura, possono inficiare sulle conversioni.

Axerve Advice (TRA)

Axerve Advice esegue un'analisi dei rischi in tempo reale, consentendo di richiedere **un'esenzione TRA** ogniqualvolta sia possibile.

Authentication

Authorization

Axerve Guaranteed

Dopo l'autorizzazione, viene eseguito un **secondo controllo antifrode** con Axerve Guaranteed Payments al fine di rimuovere qualsiasi rischio correlato alla frode da parte dell'utente.

Ecommerce e la rivoluzione dei Payment Orchestrator

Come abbiamo scritto all'inizio, la crescita costante di nuovi clienti Ecommerce ha anche un risvolto negativo, ossia l'aumento delle frodi online ai danni di consumatori e aziende, nonostante siano aumentate le iniziative e le soluzioni per contrastarle.

L'evoluzione delle soluzioni di pagamento per ovviare alle minacce digitali però non dipende solo dall'innovazione delle piattaforme di prevenzione frodi, dall'integrazione di strumenti compliant alle nuove normative introdotte come la PSD2 o dalla maggiore consapevolezza degli acquirenti, ma anche dall'introduzione di strumenti in grado di gestire i pagamenti in un sistema sofisticato di gestione delle piattaforme e, allo stesso tempo, di agevolare il coordinamento di tutti gli incassi. Proprio con questa finalità è nato recentemente il concetto di [payment orchestration](#) che identifica un contesto in cui un solo elemento è in grado di governare un insieme, anche complesso, di flussi di incasso provenienti da diverse fonti e metodi di pagamento, proprio come farebbe un direttore d'orchestra con i suoi strumentisti musicali.

Grazie alle piattaforme di orchestrazione dei pagamenti, ogni integrazione collabora all'interno del sistema in modo da consentire il percorso più efficiente per una transazione rapida e sicura. Ciò semplifica il processo, consentendo al merchant di risparmiare su ulteriori integrazioni, offrendo al contempo un'esperienza di check-out *frictionless* per i clienti.

Aumento del conversion rate, scalabilità, riconciliazione automatica sono solo alcuni dei vantaggi offerti da queste piattaforme e non ultima una prevenzione frodi più efficace, soprattutto

in contesti multi-acquirer. Grazie alla payment orchestration infatti è possibile gestire i singoli pagamenti veicolandoli su diversi PSP, acquirenti e piattaforme di prevenzione frodi, a seconda delle esigenze del merchant.

Un esempio evidente delle potenzialità di questo approccio riguarda la possibilità di veicolare specifici pagamenti su diversi acquirenti per gestire al meglio le esenzioni previste dalla normativa europea PSD2, come approfondito nel nostro [articolo su SCA e 3DS2](#). La nuova regolamentazione europea sui pagamenti infatti permette di gestire in esenzione, senza richiedere la SCA, le transazioni cosiddette low value il cui importo però può variare a seconda del tasso medio di frodi dell'acquirer che gestisce il pagamento.

In pratica, grazie all'intervento di regole predefinite o nei casi più evoluti tramite motori di intelligenza artificiale, la payment orchestration può indirizzare i pagamenti verso l'acquirer ideale per quella specifica transazione oppure su una piattaforma di prevenzione frodi specifica, non necessariamente offerta dal PSP o dai PSP ai quali ci si affida abitualmente.

Non solo, lo stesso approccio può essere adottato per impostare re-indirizzamenti legati al pricing applicato dal fornitore di servizi. Dunque, per esempio, i pagamenti possono essere smistati per singolo mercato (es. carte americane su acquirenti o PSP statunitense) o per tipologia del metodo di pagamento (es. carte corporate, consumer, digital wallet, ecc.).

Prevenzione frodi e Payment Orchestration

Una recente ricerca di Global Market Estimates (GME)²⁹, finalizzata per identificare il valore di mercato delle piattaforme di orchestrazione dei pagamenti per tipo di mercato, applicazione e settore verticale a livello globale nel periodo 2021-2026, ha identificato una crescita costante della domanda di questi servizi.

Secondo GME entro la fine del 2026 il mercato delle piattaforme di payment orchestration raggiungerà quasi 1,5 miliardi di dollari di ricavi grazie al fatto che continuerà a crescere la domanda di strumenti in grado di gestire più metodi di pagamento, in un contesto globale sempre più regolamentato.

In uno scenario in continuo mutamento e frammentato, le payment orchestration platform colmeranno un vuoto creato dalla mancanza di standard globali per i pagamenti cross-border e di provider in grado di fornire una visione omogenea e chiara dei dati di incasso, gestiti con un numero sempre maggiore di piattaforme e metodi di pagamento.

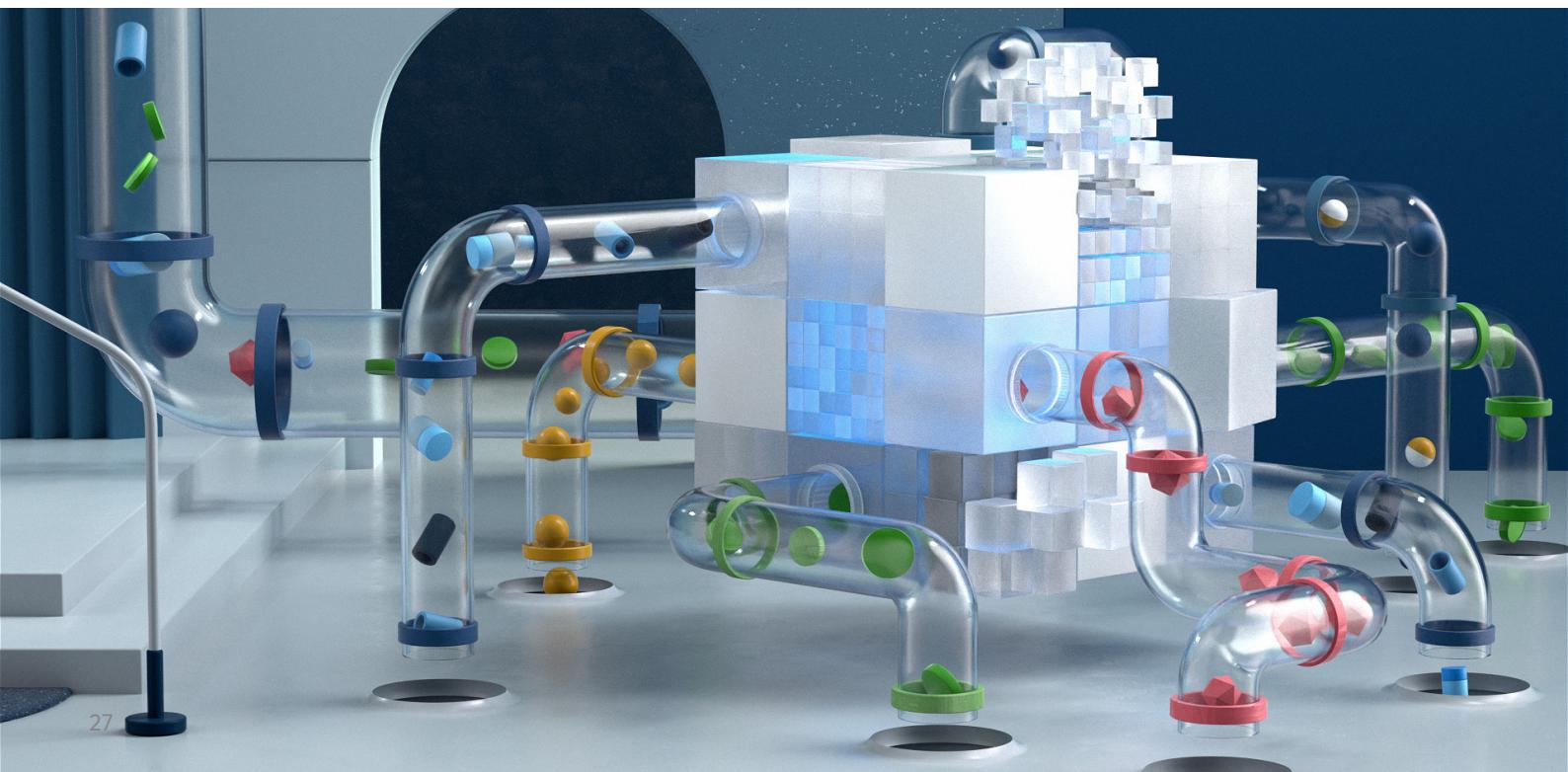
Tra i punti di forza di queste piattaforme ci sono proprio la raccolta e l'analisi dei dati, provenienti

da più fonti, e strumenti di real time analytics, componenti strategiche per ottimizzare anche internamente le attività di prevenzione frodi. La raccolta di dati da più canali richiede tempo e risorse e, spesso, non tutte le soluzioni offrono dashboard in grado di offrire una visione completa dell'andamento del transato.

Una vista omogenea e completa delle transazioni non solo rende più agevoli riconciliazione e rendicontazione ma permette di analizzare più efficacemente i pagamenti, offrendo l'opportunità di analizzarli per contribuire alle attività di prevenzione frodi, riducendo il numero di frodi subite e il numero di falsi positivi, aumentando il tasso di conversione dei carrelli.

Le opportunità offerte dalle piattaforme di payment orchestration sono molteplici e in questo documento abbiamo solo accennato ai loro vantaggi in termini di analisi delle transazioni per rendere più efficace la prevenzione frodi. Sul sito Axerve puoi approfondire tutte le potenzialità della [Payment Orchestra™](#) anche rivolgendoti ad un nostro commerciale, in più nei prossimi mesi pubblicheremo nuovi contenuti sul tema all'interno della [sezione approfondimenti](#).

29 - Global payment orchestration market - Forecasts to 2026, Global Market Estimates



Fonti e riferimenti

1. [econsumer.gov International Fraud Report](#)
2. [FTC COVID-19 and Stimulus Report](#)
3. [Nuova strategia dell'UE per la cybersicurezza e nuove norme per rendere più resistenti i soggetti critici fisici e digitali, Commissione europea](#)
4. [The Internet of Things by 2025, GSMA](#)
5. [Crime, Safety and Victims' Rights, European Union Agency for Fundamental Rights](#)
6. [Resoconto della Polizia postale nel 2020, Polizia di Stato](#)
7. [Digital Trust & Safety Index: Account Takeover Fraud and the Growing Burden on Business, Sift](#)
8. [Security Operations Annual Report, Arctic Wolf](#)
9. [FRAUD – THE FACTS 2021, UK Finance and LexisNexis](#)
10. [GBS Fraud Survey 2020, GBG](#)
11. [2021 MID-YEAR UPDATE CYBER THREAT REPORT, SONICWALL](#)
12. [Trend Micro Cloud App Security Threat Report 2020, Trend Micro](#)
13. [The State of Email Security Report, mimecast](#)
14. [Global Ransomware Damage Costs, Cybersecurity Ventures](#)
15. [COVID-19 sparks upward trend in cybercrime, Europol](#)
16. [Europol: 10 held for alleged \\$100m cryptocurrency theft from celebs, others, Reuters](#)
17. [The SIM highjackers: how criminals are stealing millions by highjacking phone numbers, Europol](#)
18. [Mobile Messaging Adoption Report 2021, Esendex e PricewaterhouseCoopers \(PwC\)](#)
19. [Internet Crime Report 2020, Internet Crime Complaint Center \(FBI\)](#)
20. [Q2 2021 OutseerTM Fraud & Payments Report, Outseer \(RSA\)](#)
21. [2021 Global Digital Trust Insights, PwC](#)
22. [2021 Gartner Board of Directors Survey, Gartner](#)
23. [The global consumer: Changed for good, PwC](#)
24. [Global Payment Risk Mitigation, FIS e Forrester](#)
25. [LexisNexis® Risk Solutions 2020 True Cost of Fraud™ Study E-commerce/Retail Report US & Canada Edition July 2020](#)
26. [A Crisis of Confidence: Findings from the eConfidence Survey, Riskified](#)
27. [The impact of eCommerce fraud on retailers and shoppers, HELPNETSECURITY](#)
28. [E-commerce statistics for individuals, Eurostat](#)
29. Global payment orchestration market - Forecasts to 2026, Global Market Estimates



Your Payment Partner to Grow

www.axerve.com

