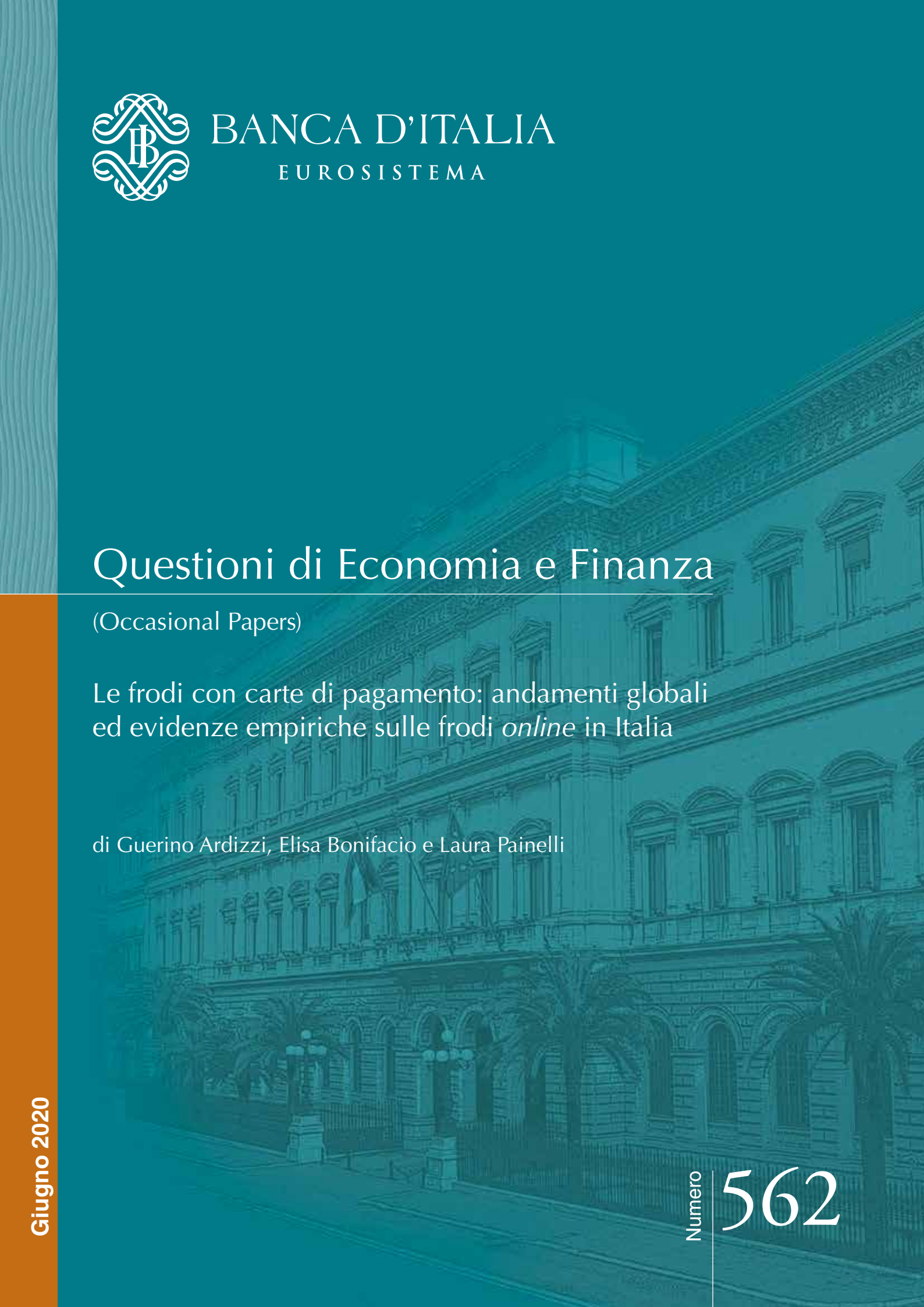
BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Le frodi con carte di pagamento: andamenti globali ed evidenze empiriche sulle frodi *online* in Italia

di Guerino Ardizzi, Elisa Bonifacio e Laura Painelli



Giugno 2020

Numero 562

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Le frodi con carte di pagamento: andamenti globali ed evidenze empiriche sulle frodi *online* in Italia

di Guerino Ardizzi, Elisa Bonifacio e Laura Painelli

Numero 562 – Giugno 2020

La serie Questioni di economia e finanza *ha la finalità di presentare studi e documentazione su aspetti rilevanti per i compiti istituzionali della Banca d'Italia e dell'Eurosistema. Le* Questioni di economia e finanza *si affiancano ai* Temi di discussione *volti a fornire contributi originali per la ricerca economica.*

La serie comprende lavori realizzati all'interno della Banca, talvolta in collaborazione con l'Eurosistema o con altre Istituzioni. I lavori pubblicati riflettono esclusivamente le opinioni degli autori, senza impegnare la responsabilità delle Istituzioni di appartenenza.

La serie è disponibile online sul sito www.bancaditalia.it .

ISSN 1972-6627 (stampa)
ISSN 1972-6643 (online)

Stampa a cura della Divisione Editoria e stampa della Banca d'Italia

LE FRODI CON CARTE DI PAGAMENTO: ANDAMENTI GLOBALI ED EVIDENZE EMPIRICHE SULLE FRODI *ONLINE* IN ITALIA

di Guerino Ardizzi*, Elisa Bonifacio* e Laura Painelli*

Sintesi

L'ampliamento del commercio al dettaglio a livello globale, favorito dalla diffusione delle transazioni via Internet (e-commerce), ha indotto il legislatore europeo a rafforzare i presidi di sicurezza nelle operazioni di pagamento online. Questo lavoro si pone l'obiettivo di valutare l'andamento delle frodi con carta di pagamento negli ultimi anni, tenuto conto dei più recenti interventi normativi. In Europa e in Italia si osserva che, dopo una lunga fase di crescita, a partire dal 2016 il tasso di frode online ha cominciato a ridursi. L'analisi empirica condotta per l'Italia su dati bancari mostra che la diminuzione è correlata ai miglioramenti dei presidi antifrode succedutisi negli ultimi anni. Nel lavoro sono anche illustrati i principali presidi anti-frode adottati dagli intermediari (es.: l'autenticazione forte e i modelli interni di mitigazione del rischio) nonché i meccanismi di tutela per il cliente in caso di frode (es.: diritto di rimborso entro la giornata successiva alla richiesta), che rendono più sicuri i pagamenti online.

Classificazione JEL: C22, C23, D12, E21.
Parole chiave: frodi, carte di pagamento, tasso di frode con carta, acquisti *online*, sicurezza, Internet.
DOI: 10.32057/0.QEF.2020.562

Sommario

* Banca d'Italia, Supervisione sui Mercati e sul Sistema dei Pagamenti.

1. Introduzione[1]

La fiducia nei mezzi di pagamento è un bene pubblico il cui perseguimento richiede, tra l'altro, investimenti in tecnologia. La prevenzione e la riduzione dei rischi nell'uso di strumenti elettronici sono punti cardine per l'integrazione e l'integrità dei sistemi di pagamento *retail* in Europa.

Le frodi con carta rappresentano un caso tipico di minaccia al buon funzionamento di uno dei circuiti di pagamento più utilizzati. In Europa, le transazioni fraudolente su operazioni con carta hanno raggiunto un valore di 1,8 miliardi di euro nel 2018 (BCE, 2020); a livello globale, nello stesso periodo, le frodi avrebbero raggiunto i 25 miliardi di dollari (HSN Consultants, 2019).

Ciò ha indotto il legislatore comunitario a introdurre nuovi presidi di sicurezza. L'intervento legislativo[2], tuttora in corso di recepimento nei diversi paesi europei, è stato in parte anticipato dal mercato grazie agli orientamenti dell'EBA sul tema della maggiore sicurezza nelle transazioni via Internet adottati tra il 2014 e il 2015.

L'analisi proposta in questo lavoro beneficia di una serie di informazioni contenute nelle segnalazioni periodiche diffuse da organismi nazionali e internazionali, sia privati che pubblici (BCE, MEF, Merchant Risk Council, HSN Consultants). Lo sforzo finora condotto dall'Eurosistema nella raccolta di statistiche armonizzate (BCE, *Report on Card Fraud*) consente di delineare alcuni interessanti andamenti riguardanti i fenomeni di frode con carta. Inoltre, in Italia le autorità (MEF, Banca d'Italia) raccolgono informazioni dagli intermediari vigilati sui principali utilizzi fraudolenti con carta, utili per un'analisi più approfondita del fenomeno su base nazionale.

Questo lavoro descrive la recente evoluzione delle frodi sulle carte di pagamento, fornendo un quadro aggiornato dei principali andamenti ed evidenziando gli ambiti più rischiosi. La sezione 2 fornisce una rassegna ragionata delle scelte del legislatore in materia di prevenzione delle frodi; la sezione 3 illustra i concetti fondamentali e i principali indicatori quantitativi utilizzati nel lavoro, la sezione 4 offre un quadro sintetico degli andamenti delle frodi con carta a livello globale, nell'area SEPA e in Italia; la sezione 5 presenta i risultati delle stime empiriche; la sezione 6 conclude. Il lavoro è corredato di un'Appendice e di un Glossario.

2. Le scelte del legislatore in materia di sicurezza nelle transazioni *online*

Nel 2012 la Commissione Europea ha pubblicato un Libro Verde (Commissione Europea, 2012), che sancisce il principio per cui è indispensabile che consumatori e commercianti possano servirsi di pagamenti elettronici sicuri, oltre che efficienti e competitivi, per poter beneficiare appieno del mercato unico. La sicurezza rappresenta quindi uno dei pilastri alla base dei provvedimenti succedutisi negli anni successivi per garantire la fiducia nell'ecosistema digitale e lo sviluppo dei pagamenti elettronici via Internet (commercio elettronico).

I requisiti di sicurezza riguardano soprattutto la prevenzione delle frodi. A livello europeo, la graduale sostituzione delle carte basate sulla banda magnetica per la lettura della carta con carte dotate di microprocessore e PIN (conformi allo standard EMV) ha

[1] Gli autori ringraziano Sonia Guida, Ravenio Parrini, Alberto Pozzolo, Francesca Provini e Maria Iride Vangelisti per i loro utili commenti.

[2] Direttiva UE 2015/2366, cd. PSD2 (Payment Service Directive2).

contribuito notevolmente a ridurre le frodi nei punti vendita fisici. Nell'ultimo decennio si è invece osservata una crescita delle attività fraudolente sul canale Internet. Nel Libro Verde la Commissione Europea sottolineava l'esigenza di diffondere sistemi di autenticazione "forte", ossia meccanismi di verifica dell'identità dell'utente a due fattori, basati sull'abbinamento di un'informazione che solo l'utente conosce (password) con un dispositivo che solo l'utente possiede (dispositivo con codice variabile).

In questo contesto, nel 2011 è stato costituito in ambito SEBC il *Secure Pay forum* (Forum sulla sicurezza dei pagamenti al dettaglio - SecurePay), un organismo di cooperazione tra autorità europee di Sorveglianza sul sistema dei pagamenti e di Vigilanza bancaria e finanziaria con l'obiettivo di sviluppare conoscenze e condividere iniziative in materia di sicurezza tecnica dei pagamenti elettronici. La Banca d'Italia ha contribuito a questa discussione pubblicando un allegato tecnico [3] al Provvedimento che disciplinava l'adozione di strumenti di più elevata qualità sotto il profilo della sicurezza; tale disciplina, applicabile su base volontaria, conteneva i principi fondanti il nuovo approccio sulla sicurezza nei pagamenti *online* (autenticazione con doppio fattore, sistemi antifrode, ecc.).

Nel 2013 il SecurePay ha emanato apposite Raccomandazioni e *best practices* per aumentare la sicurezza dei pagamenti in Internet (*Recommendations for the security of internet payments*). A dicembre 2014 i contenuti delle suddette Raccomandazioni sono stati ripresi dagli Orientamenti dell'European Banking Authority (EBA)[4]. Gli Orientamenti dell'EBA incoraggiano l'espletamento di una serie di attività da parte delle banche e degli altri prestatori di servizi di pagamento (PSPs) per ridurre le frodi *online*; in particolare:

a) il passaggio a sistemi di autenticazione "forte", ossia meccanismi di verifica dell'identità dell'utente a due fattori;
b) la realizzazione di un *assessment* specifico dei rischi connessi con l'offerta dei servizi di pagamento *online*, con indicazioni di carattere organizzativo e operativo;
c) l'adozione di procedure efficaci per l'autorizzazione e il monitoraggio delle transazioni per identificare comportamenti anomali e prevenire le frodi;
d) la promozione di iniziative di sensibilizzazione della clientela.

Con la PSD2 (Payment services directive 2) il legislatore comunitario, al fine di rafforzare e armonizzare pienamente gli standard di sicurezza in Europa, ha disciplinato i nuovi presidi antifrode assegnando all'EBA il mandato di sviluppare appositi *Regulatory Technical Standard* (RTS) e *Guidelines*. In particolare, il pacchetto normativo sulla sicurezza e la prevenzione delle frodi si compone di:

a) RTS in tema di autenticazione forte (Strong customer authentication - SCA) e comunicazione sicura;
b) *Guidelines* sui rischi operativi dei prestatori di servizi di pagamento, sul *reporting* degli incidenti di sicurezza e su quello delle frodi con gli strumenti di pagamento.

[3] Cfr. Allegato tecnico ("Tipologie di strumenti di più elevata qualità sotto il profilo della sicurezza") al Provvedimento di Banca d'Italia del maggio 2011 Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento.

[4] https://eba.europa.eu/documents/10180/1004450/EBA_2015_IT+Guidelines+on+Internet+Payments.pdf/b9c5dee9-78bd-47c5-a80c-4d2f3f8a1de2. Gli orientamenti dell'EBA recepiscono le raccomandazioni del SecurePay. L'EBA ha acquisito in quegli anni specifiche competenze regolamentari in materia di servizi di pagamento. Dal 2018 l'EBA, co-presiede il SecurePay insieme alla BCE.

Il *reporting* delle frodi consentirà in prospettiva alle autorità di raccogliere statistiche dettagliate sulle frodi per tipologia, canale e strumento di pagamento, sia a livello Paese che aggregate per area valutaria.

Per quanto riguarda gli RTS sulla SCA, la disciplina prevede che entro il 2019 tutti i pagamenti elettronici debbano essere autenticati con almeno due di tre fattori[5], con l'aggiunta, per i pagamenti su rete, di un codice dinamico associato indissolubilmente al pagamento. Quest'ultimo aspetto innova anche rispetto ai precedenti Orientamenti dell'EBA sulla sicurezza[6].

Inoltre, al fine di garantire equilibrio tra regole di sicurezza, velocità e facilità di utilizzo[7], gli stessi RTS consentono agli intermediari di essere esentati dall'applicazione generalizzata dell'autenticazione forte nei pagamenti via Internet sulla base di una specifica analisi del rischio associato alla transazione stessa (*transaction risk analysis*). Ulteriori esenzioni sono state poi previste per particolari tipologie di transazioni, quali i micro-pagamenti, le tariffe di trasporto, i pedaggi, i parcheggi.

Gli interventi della PSD2, tuttora in corso di attivazione nei diversi paesi europei, riprendono e rafforzano molti dei contenuti delle Raccomandazioni SecurePay/Orientamenti EBA adottati tra il 2014 e il 2015, in particolare quelli riguardanti l'autenticazione forte e i meccanismi tecnico-organizzativi di gestione dei rischi per gli intermediari (si veda il Box: *I presidi di sicurezza e i meccanismi di tutela del cliente in caso di frode nei pagamenti via Internet*). Questo ci consente di sviluppare una serie di considerazioni empiriche sui presidi antifrode nel commercio elettronico che saranno oggetto dei successivi paragrafi.

I presidi di sicurezza e i meccanismi di tutela del cliente in caso di frode nei pagamenti con carta via Internet

Le frodi con carta via Internet avvengono prevalentemente attraverso l'acquisizione da parte di un soggetto non autorizzato dei dati sensibili della carta, che vengono successivamente utilizzati per avviare un pagamento *online*. L'acquisizione dei dati sensibili può avvenire appropriandosi della carta fisica del titolare ovvero attraverso tecniche diverse quali: attacchi informatici, l'intercettazione dei dati sensibili della carta durante l'effettuazione di transazioni elettroniche, il *phishing*. Quest'ultima tecnica, in particolare, consiste nell'indurre il cliente a comunicare i propri dati sensibili attraverso l'invio di messaggi telefonici o e-mail che sembrano trasmesse da intermediari finanziari.

Gli orientamenti e *best practices* sulla sicurezza dei pagamenti via Internet richiamati nel precedente paragrafo hanno dato vita negli ultimi anni ad una serie di strumenti di pagamento supportati da una serie di **presidi** tecnico-gestionali rafforzati che ne accrescono l'affidabilità.

In primo luogo, le transazioni con carta di pagamento vanno presidiate dall'adozione di due fra tre fattori di autenticazione (cd. *strong customer authentication* – SCA): un fattore di "conoscenza" che solo l'utente conosce (es.: password), un fattore di "possesso", che solo l'utente possiede (es.: dispositivo *token*), un fattore di "inerenza" che solo l'utente è (es. impronta digitale). Inoltre, per i pagamenti online è prevista l'aggiunta di un codice dinamico

[5] La SCA introdotta dagli RTS è una procedura basata sull'uso di due o più dei seguenti elementi, classificati come conoscenza (una cosa che l'utente sa), proprietà (una cosa l'utente ha), e inerenza (una cosa che l'utente "è").

[6] Gli EBA RTS sull'autenticazione forte e la comunicazione sicura rappresentano il punto di arrivo di un lungo lavoro di analisi e disegno dei requisiti di sicurezza tecnica per gli strumenti *retail* sviluppato dalle autorità Europee insieme alle autorità nazionali di Vigilanza e Sorveglianza a partire dal 2011. Le GL sui rischi operativi e il reporting accrescono il set informativo a fini di controllo dei rischi a disposizione degli operatori e dell'autorità di controllo.

[7] Su questi aspetti, cfr. Ardizzi (2017).

associato indissolubilmente all'importo e al beneficiario del pagamento; ciò riduce ulteriormente il rischio di utilizzo improprio dei dati di pagamento perché ogni combinazione può essere utilizzata solo una volta. Sono gli intermediari che mettono a disposizione dei clienti i mezzi per l'autenticazione. Sono sempre gli intermediari che possono decidere di esonerare determinati tipi di operazioni, nei limiti previsti dalla normativa, dai requisiti di autenticazione (ad esempio, nel caso di transazioni di piccolo importo a basso rischio).

Inoltre, gli intermediari deve sviluppare al proprio interno un **processo di gestione e mitigazione dei rischi che si basa su meccanismi di riconoscimento della frode, gestione della stessa e approntamento di misure per evitare che essa si ripeta.** Nel caso in cui i suddetti presidi non riescano a evitare che si incorra in una frode, **i clienti sono tutelati** da specifiche previsioni di legge - contenute principalmente nella PSD2 - che riconoscono il diritto al rimborso degli importi indebitamente addebitati; il cliente ha, in via generale, **13 mesi** di tempo dall'addebito per chiedere il rimborso di un'operazione che non ritiene sia stata da lui autorizzata o correttamente eseguita dall'intermediario.

I clienti possono attivare diversi **meccanismi di tutela** per recuperare le somme: i) richiesta di rimborso rivolta direttamente all'intermediario emittente la carta, ii) ricorso ai sistemi stragiudiziali di risoluzione della controversia, iii) ricorso all'Autorità Giudiziaria. Inoltre, le regole interbancarie previste da un circuito di carte (regole di *chargeback*) spesso offrono una tutela aggiuntiva in caso di operazioni non autorizzate o contestate: queste regole consentono all'emittente di recuperare direttamente dall'acquirer le somme contestate, a beneficio del cliente titolare della carta.

Una volta ricevuta la richiesta di rimborso, **l'intermediario è tenuto a rimborsare** la somma entro la fine della giornata operativa successiva alla richiesta, a meno che non vi sia il sospetto che il frodatore sia lo stesso cliente che ha sporto denuncia. Spetta comunque all'intermediario dimostrare che l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subìto le conseguenze di guasti tecnici o altri inconvenienti. Se non è stata richiesta la SCA al momento del pagamento online, la banca **può rifiutare il rimborso solo se ritiene che il cliente abbia agito con frode**; negli altri casi la banca deve dimostrare che vi sia stato dolo o grave negligenza del cliente per rifiutare il rimborso.

Restano in capo ai clienti **gli obblighi di comportamento che attengono alla custodia** degli strumenti di pagamento e delle credenziali di autenticazione e alla comunicazione in tempi brevi di eventuali fatti anomali (smarrimento, furto, esecuzione di operazioni non autorizzate). Questi obblighi sono previsti da disposizioni di legge e sono esplicitati e specificati nel contratto che regola la prestazione del servizio di pagamento. Per incentivare la pronta notifica da parte del cliente alla banca emittente di eventuali furti o smarrimenti della carta, il legislatore ha stabilito comunque una franchigia di massimo 50 euro che il cliente può dover pagare per le operazioni non autorizzate effettuate fino al momento della comunicazione all'intermediario del furto o dello smarrimento della carta.

3. I concetti fondamentali per l'analisi economica della frode con carta

Per frode si intende l'operazione con carta (pagamento o prelievo) effettuata senza il consenso del legittimo titolare (transazioni non autorizzate o disconosciute). La perpetrazione della frode ha origine nel momento in cui la carta viene compromessa (dati intercettati o carta sottratta), ma si concretizza all'atto dell'utilizzo della carta stessa presso il punto vendita (POS fisico o e-commerce) o presso sportelli automatici (ATM): solo a partire da questo momento si registra la frode.

L'intermediario distingue tra frode lorda e frode netta. La frode lorda rappresenta il complesso delle transazioni (numero e importo) disconosciute dal titolare della carta o, in modo automatico, dai sistemi informatici post blocco/alert[8], a fronte di compromissione dello strumento e/o dei relativi dati a seguito di diverse cause (furto, smarrimento, clonazione, *phishing*, mancata ricezione, ecc.); la frode lorda rappresenta

[8] Per una definizione in chiaro delle sigle e dei termini tecnici utilizzati nel lavoro si veda il Glossario.

la perdita potenziale per un evento segnalato, indipendentemente dalle sue ricadute economico-patrimoniali. La frode netta[9], invece, è la perdita effettiva registrata in bilancio dall'*issuer* e/o dall'*acquirer* al verificarsi di una frode lorda. La differenza è data dalle frodi di cui l'intermediario non si è fatto carico. Il singolo intermediario è interessato soprattutto alla frode netta, che rappresenta per lui una perdita.

Il rapporto tra frode netta e frode lorda può essere minimizzato attraverso i meccanismi di *liability shift*[10]; questi ultimi consentono di traslare la responsabilità dell'operazione fraudolenta sull'intermediario controparte, se non ha attivato i necessari presidi di sicurezza ovvero sul cliente finale (consumatore o esercente) che abbia agito con dolo o negligenza grave[11]. Minore è il rapporto tra frode netta e frode lorda per il singolo intermediario, migliore è la sua *performance* in termini di minimizzazione della perdita economica.

L'*overseer* utilizza invece la definizione di frode lorda per misurare il grado di affidabilità di uno schema di carte o del sistema nel suo complesso, indipendentemente dal soggetto responsabile che sostiene effettivamente la perdita economica. Le statistiche disponibili utilizzate in questo lavoro si basano su questa definizione e misurano la frode lorda.

Nel nuovo *framework* regolamentare sulla sicurezza il tasso di frode, ossia il rapporto frode lorda e totale transazione, è divenuto un indicatore essenziale per valutare la possibilità, per il prestatore di servizi di pagamento, di essere esentato dall'applicare l'autenticazione forte del cliente (SCA; vedi *infra* al par. 5).

Fino ad oggi la scarsità dei dati disponibili ha reso difficile la misurazione del fenomeno, tuttavia, la PSD2 e la disciplina secondaria recentemente approvata (EBA *Guidelines on Fraud Reporting under PSD2*, in vigore dal 2019) consentiranno in prospettiva di raccogliere informazioni più estese e dettagliate sulle frodi (tipologia, canale e strumento), sia a livello paese che aggregate per area. In Italia, importanti evidenze sono disponibili a livello aggregato nei rapporti statistici sulle frodi con carte pubblicati dall'Ufficio Centrale Antifrode dei Mezzi di Pagamento (UCAMP - MEF). Inoltre, le informazioni per emittente carta contenute nelle segnalazioni alla Banca d'Italia degli intermediari vigilati (Matrice dei conti) consentono altresì di condurre analisi empiriche multivariate con particolare riguardo alle frodi su Internet.

4. L'analisi descrittiva

4.1 Le frodi su carte di pagamento nel mondo

Secondo le più recenti stime di HSN Consultants (2019), le frodi su carte di pagamento a livello globale per emittenti, esercenti e *acquirers*, utilizzate per acquisti o prelievi di contante, hanno raggiunto nel 2018 i 25 miliardi di dollari; tale valore, benché in crescita del 16,9% rispetto all'anno precedente, evidenzia una diminuzione del rischio

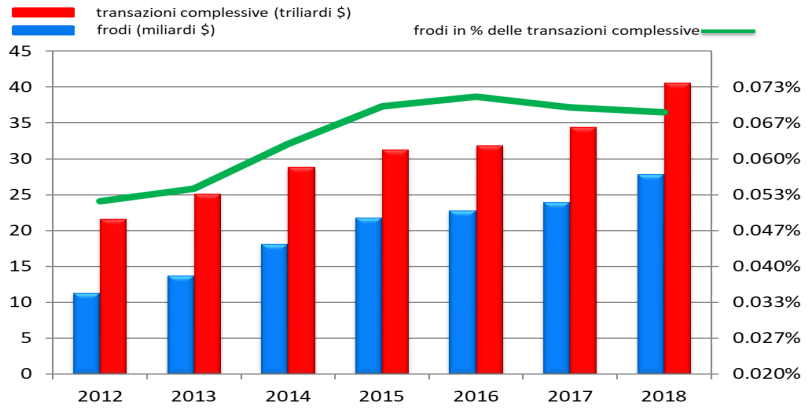
[9] Cfr. Giacomelli (2008).

[10] Le *liability shift rules* sono clausole interbancarie di trasferimento della responsabilità previste dalle *governance authority* dei circuiti di carte di pagamento, che consentono di traslare - in caso di contestazioni in senso lato - gli oneri da frode verso gli intermediari che non adottano le tecnologie più sicure (es.: autenticazione con il doppio fattore); questo meccanismo ha l'obiettivo di incentivare la migrazione di sistema verso standard di sicurezza più evoluti.

[11] In particolare, gli art. 69 e 74 della PSD2 che disciplinano gli obblighi e le responsabilità a carico dell'utente di servizi di pagamento.

frodi se rapportato al totale delle transazioni: nel 2018 il tasso di frode si è ulteriormente ridotto allo 0,069% (Fig. 1). I maggiori circuiti internazionali di carte (American Express, Diners Club/Discover, JCB, Mastercard, Visa e UnionPay), che rappresentano l'83% del transato totale, avrebbero registrato l'89% circa delle perdite complessive.

Fig. 1: Le frodi su carta di pagamento nel mondo



Fonte: HSN Consultants, 2018 e 2019.

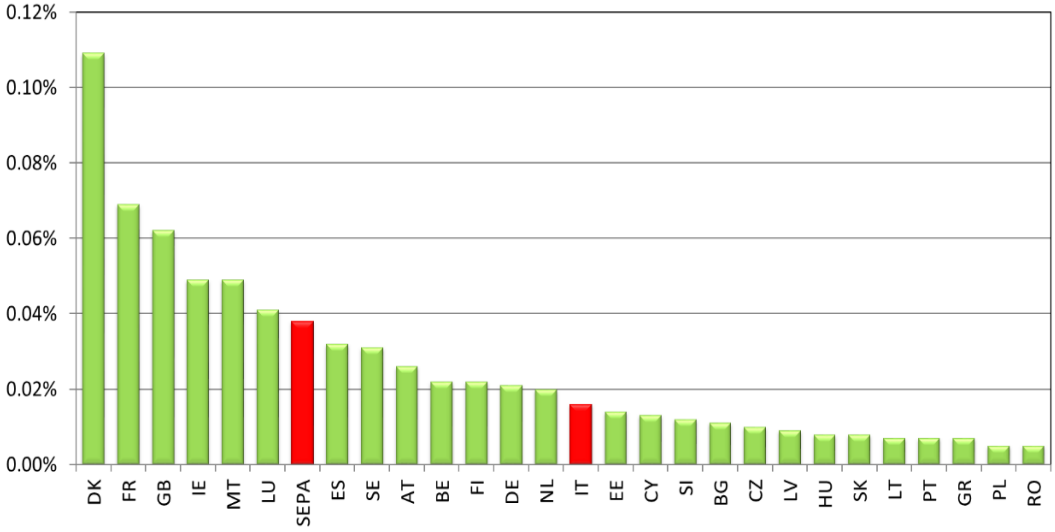
Con l'implementazione progressiva (2002-10) dello standard a microchip EMV (Europay Mastercard Visa)[12], che ha inteso contrastare in particolare la contraffazione delle carte di pagamento nel mondo fisico, i truffatori hanno spostato il loro focus soprattutto sulle transazioni disposte a distanza o in remoto (*card-not-present* (CNP))[13] che nel 2018 hanno raggiunto il 54% del valore complessivo frodato a livello globale. Le evidenze mostrano inoltre un generale abbassamento del valore medio per operazioni fraudolente.

4.2 Le frodi su carte di pagamento nell'area SEPA[14]

Nel periodo 2012-18, il valore in euro delle transazioni fraudolente per il totale dei paesi SEPA (Single Euro Payments Area) è cresciuto del 35,3% (+130,8% in numero). Anche il tasso di frode, espresso come percentuale tra importi delle operazioni fraudolente rispetto al valore totale delle transazioni, è cresciuto nella maggior parte dei paesi, facendo registrare, in quindici di questi, aumenti superiori alla media dell'area; nel 2018 il nostro paese ha mostrato un tasso di frode sul totale operazioni con carta ben al di sotto della media dell'area SEPA (0,016 rispetto allo 0,038% - Fig 2).

[12] Cfr. Ardizzi (2012).
[13] Le frodi CNP includono quelle relative alle transazioni effettuate su canale telefonico, via Internet e alla vendita per corrispondenza in cui il titolare della carta non presenta fisicamente la carta al commerciante. La maggior parte delle frodi CNP comporta l'uso dei dettagli della carta che sono stati ottenuti tramite *skimming*, *hacking*, campagne di *phishing*, e-mail, sollecitazioni telefoniche, ecc. I dettagli della carta vengono quindi utilizzati per effettuare transazioni fraudolente.
[14] I commenti in questo paragrafo si basano su nostre elaborazioni di dati dello Statistical Data Warehouse della BCE e della Matrice dei conti e potrebbero quindi differire rispetto quelli presentati in altre pubblicazioni.

Fig. 2: Tasso di frode in valore nell'area SEPA
(in percentuale delle transazioni complessive)

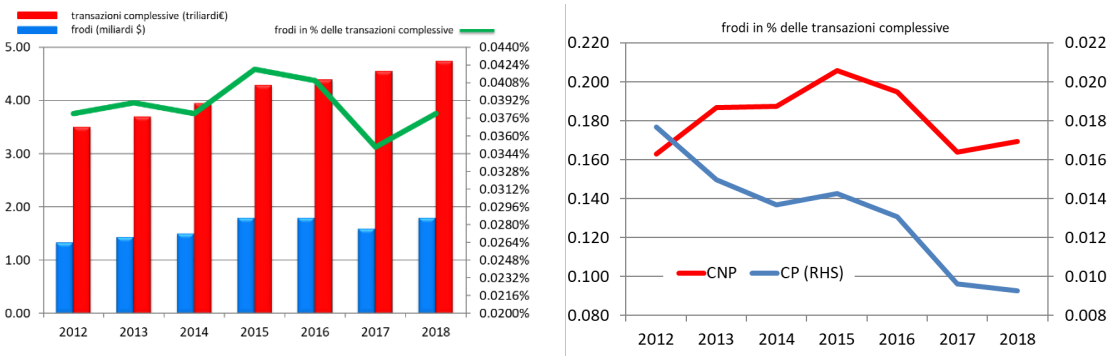


Fonte: nostre elaborazioni su dati BCE.

Il valore complessivo (in euro) delle frodi per transazioni condotte utilizzando carte emesse all'interno della SEPA e il tasso di frode in valore sono tornati a salire leggermente nel 2018 dopo il miglioramento osservato nell'anno precedente (Fig. 2); rimane comunque decrescente il trend rispetto al picco del 2015-2016: il tasso di frode sul valore delle operazioni passa infatti dallo 0,042% nel 2015 allo 0,038% nel 2018. Il numero di transazioni frodate è invece cresciuto in maniera più evidente nello stesso periodo, passando dallo 0,020% nel 2015 allo 0,023% nel 2018; ne consegue che le attività fraudolente si concentrano soprattutto sulle operazioni (più frequenti) di basso importo.

Nel periodo 2012-18 la quota maggiore di frodi è riconducibile ai pagamenti *card not present* (CNP): in base a stime preliminari della BCE, queste sono arrivate a rappresentare l'80% del totale frodato (sia in termine di valore che di numero) nel 2018; la restante parte sarebbe costituita dalle frodi da transazioni su POS fisici e ATM (*card present* – CP – Fig. 3).

Fig. 3: Le frodi su carta di pagamento nell'area SEPA



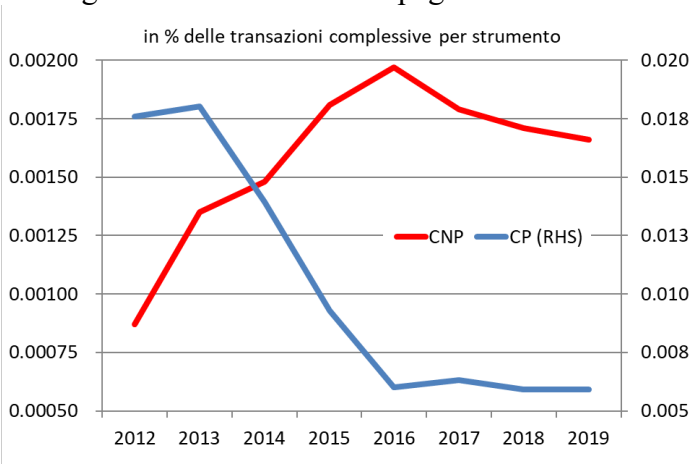
Fonte: nostre elaborazioni su dati BCE.

L'analisi combinata dei valori e dei numeri delle transazioni evidenzia come gli importi medi delle transazioni fraudolente per CP e CNP siano fortemente diminuiti nel 2018 rispetto all'anno precedente (a 82 e 87 euro da 95 e 101 euro, rispettivamente, nel 2017 – Fig. A1).

4.3 Le frodi su carte di pagamento in Italia

Le frodi in valore sulle transazioni condotte utilizzando carte emesse in Italia hanno ripreso a calare dal 2019 dopo gli incrementi osservati nel triennio precedente (Fig. 4); anche il tasso di frode è diminuito (allo 0,016%). Come osservato per il resto dell'Europa, alla crescita del numero delle transazioni frodate corrisponde una diminuzione dell'ammontare: il valore medio frodato avrebbe raggiunto nel 2019 gli 85 euro.

Fig. 4: Le frodi su carta di pagamento in Italia (1)



Fonte: nostre elaborazioni su dati della Matrice dei conti.
(1) Dati ponderati con il valore delle transazioni per ente segnalante.

Nel periodo 2012-19 le frodi sul canale CP si sono ridotte progressivamente, stabilizzandosi nell'ultimo triennio intorno allo 0,006%; di contro, le frodi sul canale CNP[15] sono cresciute del 73,3% circa in media d'anno fino a raggiungere nel 2019 una quota pari al 68% del valore totale frodato, anche per effetto di una crescita complessiva del segmento. Tuttavia, a partire dal 2016 si osserva una inversione dell'andamento: il tasso di frode CNP e passato dallo 0,197% nel 2016 allo 0,166% nel 2019, un dato inferiore all'ultimo disponibile per la SEPA (0,169% nel 2018).

Le frodi su canale CNP sono diminuite sia in termini di numero che – soprattutto – di valore rispetto alle transazioni totali. Le frodi su Internet sembrano assumere importi medi più contenuti rispetto al passato; ciò potrebbe essere imputabile anche ad asimmetrie nell'implementazione dei presidi di sicurezza[16] sia per soglie di importo, sia per tipologie di strumento utilizzato.

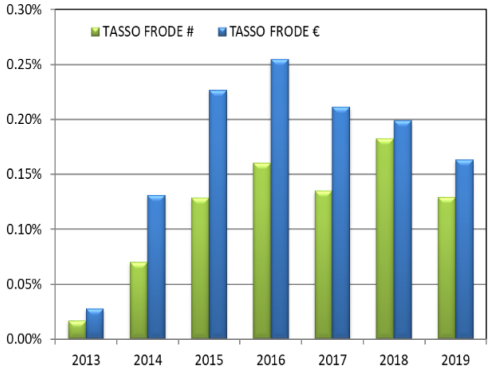
In particolare, il tasso di frode è diminuito gradualmente per le carte di credito a partire dal 2017, mentre per le prepagate, che rappresentano lo strumento elettivo per le

[15] Per il nostro Paese, le transazioni CNP si riferiscono al solo canale Internet ed escludono quindi i canali postali e telefonici che vengono attualmente rilevati solo parzialmente nella Matrice dei conti; si noti tuttavia che quest'ultimi canali rappresentano in genere una parte residuale del CNP (il 14% circa di quello dell'area SEPA).
[16] Cfr. Ardizzi (2017).

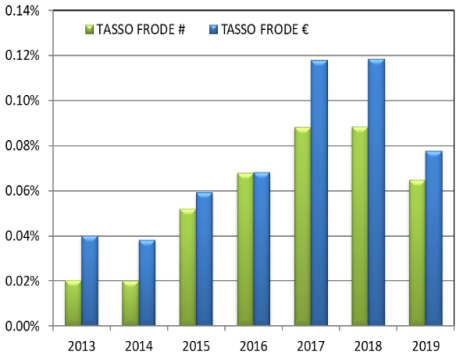
transazioni su Internet di basso importo, le transazioni frodate *online* hanno iniziato a ridursi soltanto a partire dal 2019 (Fig. 5).

Fig. 5: Frodi su carte di credito e prepagate, canale Internet
(% del totale Internet per tipologia di carta)

Carte di credito



Carte prepagate



Fonte: nostre elaborazioni su dati della Matrice dei conti.

5. Analisi esplorativa del tasso di frode *online* su dati panel

5.1 Il modello di analisi

Gli andamenti descritti trovano conferma nell'ultimo *Report on Card Fraud* della BCE (2018)[17]. I miglioramenti del tasso di frode potrebbero ricondursi ai presidi di sicurezza nel commercio elettronico che si sono succeduti negli ultimi anni; in particolare, gli Orientamenti sulla sicurezza dei pagamenti via Internet, emanati dall'EBA nel 2014, hanno raccomandato alle autorità competenti e agli intermediari di conformarsi entro il 2016 ai requisiti dell'autenticazione forte nelle transazioni *online*[18]. Gli stessi Orientamenti hanno promosso anche l'adozione da parte degli intermediari di modelli interni di mitigazione del rischio frode e di meccanismi di comunicazione volti a prevenire comportamenti fraudolenti. Questi presidi sono stati poi rafforzati dalle norme della PSD2 e dagli RTS emanati nel 2018 dall'EBA e resi definitivamente obbligatori dall'autunno del 2019[19].

Utilizzando un panel semestrale non bilanciato di 68 intermediari emittenti nel periodo 2012-2018 (dati estratti dalla Matrice dei conti) è possibile stimare la connessione tra la diffusione di nuovi standard di sicurezza *online* e la riduzione del tasso di frode nel nostro paese.

[17] "*Although there was an upward trend in card fraud between 2012 and 2015, it seems the trend is changing, given that fraud went down in 2016*".

[18] I gestori dei circuiti di carte e gli intermediari hanno nel frattempo investito nei nuovi standard di sicurezza per le transazioni sicure *online* (es. 3DS), stimolati anche dalle regole di incentivo indotte dalla *liability shift rules*, che trasferiscono le perdite da frode sugli operatori meno sicuri.

[19] In considerazione della complessità degli adeguamenti, l'EBA ha riconosciuto alle autorità nazionali la possibilità di concedere agli intermediari ulteriore tempo, rispetto al 14 settembre 2019, per consentire il completamento degli interventi e l'adozione dei nuovi strumenti di autenticazione da parte di tutti i clienti, con esclusivo riferimento ai pagamenti *online* con carta. La Banca d'Italia ha deciso di concedere una proroga di 18 mesi per adeguarsi, a condizione che gli intermediari presentino un dettagliato piano di migrazione che includa anche iniziative di comunicazione e di preparazione della clientela, sia lato esercenti, sia lato titolari di carte.

Definendo da una parte il tasso di frode y_{it} come variabile dipendente (*outcome*) per l'intermediario i nel periodo t e, dall'altra, la variabile esplicativa di tipo dicotomico (*dummy*) D^{EBA}_t *= 1 (anno > 2016)*, che assume valore 1 nel periodo 2017-2018 e 0 negli altri casi, l'impatto sul tasso di frode per intermediario prima e dopo l'entrata in vigore degli Orientamenti dell'EBA può essere spiegato attraverso l'equazione:

$$y_{it} = \beta D^{EBA}_t \quad [1]$$

L'equazione [1][20] può essere arricchita con altre variabili di controllo, per tenere conto delle caratteristiche evolutive del mercato e dei fattori specifici, non invarianti nel tempo, dei diversi intermediari, che possono incidere sul tasso di frode (y_{it}).

L'equazione completa del modello di analisi della frode è quindi la seguente:

$$y_{it} = \textit{online}\ \text{FRAUD rate} = \alpha_0 + \beta_1 D^{EBA}_t + \Sigma_j \beta_j Z_j \quad [2]$$

con j=1…n (variabili di controllo); e α_0 pari a un termine costante (l'intercetta).

Il termine $\Sigma_j \beta_j Z_j$ indica l'insieme di variabili di controllo (Zj) e dei relativi coefficienti che possono influire sull'indicatore di frode: la dimensione relativa dell'intermediario, il tipo di carte utilizzate (es. credito o prepagate), il tipo di attivazione e di controllo del processo di spedizione, il massimale di utilizzo accordato al cliente, i sistemi di autorizzazione e di allerta (es. *sms alert*), ecc. Tuttavia, nell'ottica di una indagine esplorativa e sulla base dei dati disponibili per intermediario, si possono considerare solo alcune delle variabili tra quelle elencate. Le variabili considerate (lato emittente carta) sono: la quota di mercato in termini di percentuale di transazioni *online* gestite dall'emittente (dimensione relativa dell'intermediario; Z_1 = QRETE) e la quota di operazioni *online* con carte prepagate sul totale carte (tipo di carte utilizzate; Z_2 = SHARE) al fine di catturare gli effetti della specializzazione di prodotto.

L'effetto atteso di QRETE sul tasso di frode è negativo: maggiore è la quota di transazioni all'interno del proprio network, maggiore è la probabilità di diversificare il rischio e maggiore sarebbe la capacità dell'intermediario di prevenire tempestivamente le frodi (Ardizzi, 2012; Giacomelli, 2008). L'effetto della variabile SHARE sul rischio frode è invece ambiguo in quanto dipende dal tipo di utilizzo e dal presidio di sicurezza disponibile per i diversi strumenti.

Dall'analisi grafica di cui al precedente paragrafo si evince che i tassi di frode *online* delle carte prepagate sono mediamente inferiori rispetto ai tassi di frode sulle carte di credito, ma registrano una dinamica meno virtuosa. L'analisi econometrica per dati panel che sfrutta l'informazione proveniente sia dalla variabilità cross-section sia da quella temporale dovrebbe aiutare ad approfondire meglio questo aspetto.

L'equazione finale del modello è dunque la seguente:

$$\textit{online}\ \text{FRAUD rate} = \alpha_0 + \beta_1 D^{EBA}_t + \beta_1\ \text{QRETE}_{it} + \beta_2\ \text{SHARE}_{it} + \varepsilon_{it} \quad [3]$$

Nei modelli panel[21] il termine ε_{it} dell'equazione può essere scomposto in un effetto specifico individuale, in un effetto temporale e in un disturbo stocastico. In particolare, l'effetto specifico individuale incorpora gli elementi di eterogeneità *firm specific* non osservabili[22], riducendo la distorsione da variabili omesse nelle stime. L'effetto

[20] Tra i controlli di robustezza si è condotta anche la stima dell'equazione [1], che ha confermato la stabilità dei risultati ottenuti con il modello completo.

[21] Per i quali generalmente la numerosità delle unità (intermediari) è elevata, mentre quella relativa alla dimensione temporale è piuttosto contenuta.

[22] Questi elementi possono essere ad esempio legati al sistema di controllo interno e gestione del rischio, alla tipologia di clientela, ecc., che nel modello panel a effetti fissi sono ipotizzati invarianti nel tempo,

temporale specifico può essere colto prevedendo, invece, una variabile temporale annuale (y=year), che cattura separatamente la presenza di un trend lineare, cui possiamo aggiungere (trattandosi di un panel semestrale) una variabile binaria, che individua il semestre di riferimento (h=semestre), in modo da controllare anche per eventuali effetti stagionali.

La variabile dipendente (*online* FRAUD) è pari al rapporto tra le operazioni (in numero o valore) disconosciute dal titolare (frode) e le transazioni totali CNP, ossia al tasso di frode lato emittente (*card fraud ratio*). Al crescere del tasso di frode aumenta la perdita potenziale e quindi la rischiosità sulle carte emesse dalla banca segnalante. Questa variabile è una percentuale e non assume una distribuzione dicotomica come nei modelli logistici, tuttavia si distribuisce in modo continuo nell'intervallo [0,1] con una massa concentrata su valori prossimi a zero.

La Fig. 6 mostra la distribuzione empirica della variabile *online* FRAUD calcolata sui dati segnalati dai PSPs italiani e combinati (*pooled*) per il periodo 2012-2018. La distribuzione è positivamente asimmetrica[23]: gli intermediari estremamente virtuosi, ovvero con tassi di frode prossimi allo zero, sono più numerosi di quelli estremamente rischiosi.

Inoltre, ai fini dell'esenzione SCA prevista dai nuovi RTS dell'EBA[24], la stessa distribuzione indica che circa il 60% degli emittenti si troverebbe al di sotto del tasso di soglia dello 0,13% e beneficerebbe pertanto dell'esenzione prevista per le transazioni fino ai 100€.

La Fig. 7 riporta invece la funzione di densità degli stessi dati trasformati in logaritmo, dalla quale si evince una distribuzione empirica meno asimmetrica ovvero più simile a una normale. Nella specificazione del modello di cui all'equazione [3], utilizzeremo quindi la variabile y in logaritmo**.**

Fig. 6: Distribuzione empirica tasso di frode in valore

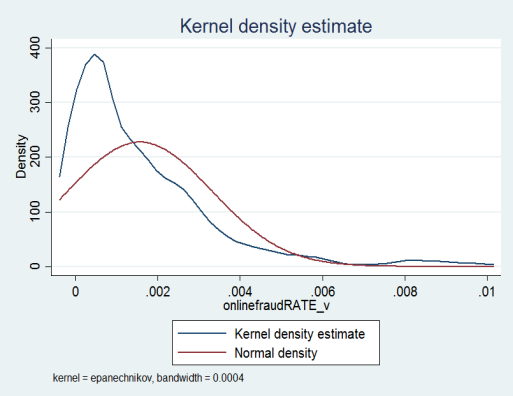
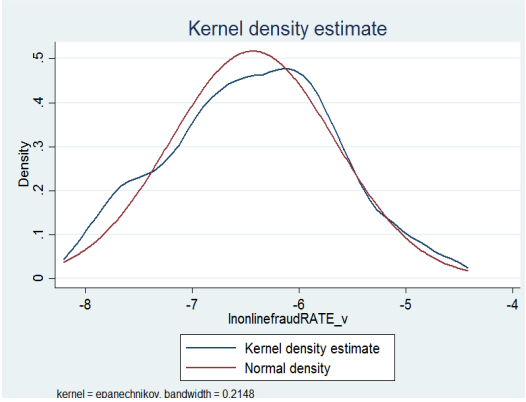


Fig. 7: Distribuzione empirica del logaritmo del tasso di frode in valore



Fonte: nostre elaborazioni su dati della Matrice dei conti.

mentre in quello a effetti casuali si suppone possano essere influenzati da un elevato numero di circostanze casuali e non osservabili.

[23] Le distribuzioni caratterizzate da asimmetria positiva e leptocurtosi (come nel caso in esame) sono peraltro comuni nel descrivere le caratteristiche di una distribuzione di perdita. Vedi, ad esempio, le distribuzioni empiriche dei tassi di *credit default* per le imprese ovvero la distribuzione di perdita per un portafoglio finanziario.

[24] Per le operazioni con carte di pagamento, l'esenzione può essere ottenuta per transazioni fino a 100, 250 e 500€ qualora i tassi di frode registrati dall'intermediario siano inferiori, rispettivamente, allo 0,13, 0,06 e 0,01% del valore transato (tabella allegata al Regolamento Delegato (Ue) 2018/389).

5.2 Stima del modello e risultati

I parametri dell'equazione [3] sono stati stimati utilizzando un panel non bilanciato di 72 intermediari osservati tra il 2012 e il 2019[25], per un totale di circa 600 osservazioni. La variabile dipendente (*online* FRAUD, calcolata per valori e numeri), è espressa in termini logaritmici, al fine di ridurne la dispersione e l'asimmetria. Le variabili esplicative, invece, sono espresse in termini percentuali e sono:

a. la quota percentuale di operazioni *online* (QRETE)
b. la percentuale di transazioni con carte prepagate (SHARE)
c. la variabile temporale annuale (year) e la componente binaria che identifica il semestre (h)
d. la variabile di controllo dicotomica per l'introduzione degli orientamenti EBA (D^{EBA})

Le tavole 1 e 2 mostrano rispettivamente le statistiche descrittive e la matrice di correlazione per le suddette variabili; da quest'ultima non sembra emergere la presenza di forte collinearità che potrebbero inficiare la consistenza delle stime.

Tav. 1: Statistiche descrittive

Variabili	Osservazioni	Media	Dev. Std.	Min	Max
QRETE	689	0.010	0.024	0.000	0.156
SHARE	583	0.443	0.379	0.000	1.000
D^{EBA}	689	0.369	0.483	0.000	1.000
ln *online* FRAUD_valori	583	-7.149	1.831	-15.327	5.650
ln *online* FRAUD_numeri	583	-7.586	1.682	-15.265	5.295

Tav. 2: Matrice di correlazione

	QRETE	SHARE	D^{EBA}	ln *online* FRAUD_valori
QRETE	1			
SHARE	-0.006	1		
D^{EBA}	0.010	0.096	1	
ln *online* FRAUD_valori	-0.127	-0.057	0.050	1
	QRETE	SHARE	D^{EBA}	ln *online* FRAUD_numeri
QRETE	1			
SHARE	-0.006	1		
D^{EBA}	0.010	0.096	1	
ln *online* FRAUD_numeri	-0.181	0.082	0.109	1

[25] Sono esclusi gli operatori che non segnalano perdite da frodi in uno o più dei periodi di riferimento poiché non è possibile discriminare tra valori *missing* e tasso di frode pari a 0 (ipotesi poco probabile); nell'analisi quindi sono considerati solo gli intermediari che segnalano livelli di frode positivi.

Per le stime, sono stati utilizzati tre modelli regressivi log-lineari[26] a confronto: una semplice regressione OLS sul data base *pooled*[27], un modello panel con effetti fissi (FE) e uno con effetti casuali (RE); i risultati delle stime sono riportati nella tavola 3.

Tav. 3: Stima panel del tasso di frode *on line* (online FRAUD rate)

	Valore			Numero		
VARIABLES	OLS online FRAUD rate	FE online FRAUD rate	RE online FRAUD rate	OLS online FRAUD rate	FE online FRAUD rate	RE online FRAUD rate
qrete	-9.402***	-26.59**	-13.51***	-12.21***	-38.15**	-18.57***
	(-2.996)	(-12.85)	(-4.897)	(-3.398)	(-15.27)	(-6.234)
shareem	-0.249	0.387	0.0139	0.372*	1.28	0.738*
	(-0.236)	(-1.998)	(-0.769)	(-0.201)	(-0.782)	(-0.442)
h	0.193	0.321***	0.257***	0.161	0.275***	0.220**
	(-0.147)	(-0.0886)	(-0.0777)	(-0.132)	(-0.098)	(-0.0903)
y	0.373***	0.477***	0.425***	0.379***	0.474***	0.427***
	(-0.0607)	(-0.0915)	(-0.0826)	(-0.0539)	(-0.0803)	(-0.0711)
EBA	-1.265***	-1.261***	-1.261***	-1.147***	-1.124***	-1.128***
	(-0.262)	(-0.263)	(-0.268)	(-0.252)	(-0.203)	(-0.198)
Constant	-758.0***	-969.2***	-863.2***	-771.3***	-963.3***	-869.2***
	(-122.4)	(-184.4)	(-166.5)	(-108.7)	(-161.9)	(-143.3)
Observations	583	583	583	583	583	583
R-squared	0.082	0.168		0.122	0.224	
Number of ente_segn		72	72		72	72

Robust standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Come previsto, il coefficiente relativo all'impatto degli orientamenti dell'EBA (D^{EBA}) presenta segno negativo e significativo in tutte le specificazioni. Risulta sempre significativo e coerente con le ipotesi sopra formulate anche il coefficiente negativo di QRETE, mentre quello relativo a SHARE è positivo e significativo solo nel modello OLS e RE per l'impatto sul tasso di frode nel numero. Quest'ultima evidenza, unita al fatto che la variabile D^{EBA} influenza negativamente più le frodi in valore (il coefficiente è maggiore) che quelle in numero, appare coerente con l'ipotesi che le operazioni di basso importo, più frequenti ed effettuate soprattutto con carte prepagate, possano presentare asimmetrie nei presidi di sicurezza[28]. I risultati sui coefficienti relativi all'impatto degli orientamenti dell'EBA sono robusti anche nel caso di stime condotte sul panel bilanciato, ossia con gli intermediari che segnalano tutte le variabili nell'intero periodo di riferimento (Tav. A1 in Appendice).

6. Conclusioni

Il tema delle frodi con carte di pagamento è da tempo oggetto di notevole attenzione in Europa. Dalla seconda metà del decennio appena concluso, si osserva una tendenziale riduzione delle frodi nel mondo fisico, soprattutto per effetto della migrazione al micro chip che ha ridotto il fenomeno della clonazione della carta. Nello stesso periodo, tuttavia, le attività fraudolente si sono in parte spostate sul canale Internet e sul commercio elettronico, dove è stato più difficoltoso adottare standard di sicurezza adeguati e armonizzati nei diversi paesi.

[26] I modelli log lineari sono in genere applicati in presenza di variabili esplicative di tipo dicotomico. In questo caso, le variabili indipendenti sono tutte continue, ma delimitate nell'intervallo [0-1] essendo espresse in termini percentuali.

[27] Il test di Hausman rifiuta infatti l'ipotesi di effetti casuali, così come il test di Breusch-Pagan rifiuta quella di *poolability* (modello cross-sezionale anziché panel). Tuttavia, preferiamo mantenere i diversi stimatori per verificare meglio la coerenza nei coefficienti stimati.

[28] Si rileva, tuttavia, che le transazioni con carte prepagate sono caratterizzate da importi contenuti anche per via dei vincoli di spesa legati alla provvista; questo consente anche di contenere le stesse perdite da frode.

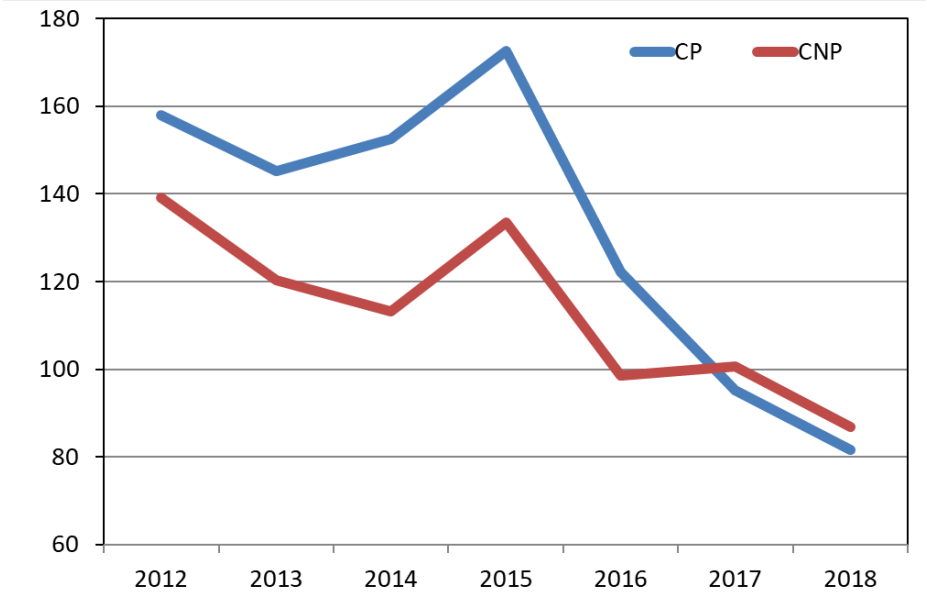
Ciò ha indotto il legislatore comunitario a introdurre nuovi presidi di sicurezza, soprattutto con riferimento alle transazioni *online* (Internet), attraverso le disposizioni sull'autenticazione forte contenute nella PSD2 e i requisiti tecnici (EBA) che promuovono, tra l'altro, l'utilizzo da parte degli intermediari di modelli di controllo interni di tipo preventivo. L'intervento legislativo, tuttora in corso di attuazione nei diversi paesi europei, è stato in parte anticipato dal mercato grazie agli orientamenti dell'EBA sul tema della maggiore sicurezza nelle transazioni via rete in vigore dal 2015.

In Italia nell'ultimo triennio si registra un abbassamento del tasso di frode *online*. La verifica empirica dei benefici indotti dai più recenti orientamenti EBA in materia di sicurezza delle transazioni *online* con carte di pagamento evidenzia che, a partire dal 2016, anno in cui si è registrato il picco delle frodi *online*, l'avvento dei nuovi presidi di sicurezza ha comportato minori perdite da frodi a livello di sistema. Sembrano permanere alcune asimmetrie nei presidi di sicurezza dato che i miglioramenti non sono omogenei per i diversi intermediari e sono più evidenti per le per operazione di importo elevato. In generale, l'Italia presenta comunque un tasso di frode totale con carta inferiore a quello medio registrato nell'area SEPA (ultimo dato disponibile al 2018).

La verifica empirica dei benefici indotti dai più recenti orientamenti EBA in materia di sicurezza delle transazioni *online* con carte di pagamento evidenzia che, a partire dal 2016, anno in cui si è registrato il picco delle frodi *online*, l'avvento dei nuovi presidi di sicurezza ha comportato minori perdite da frodi a livello di sistema. Sembrano permanere alcune asimmetrie nei presidi di sicurezza dato che i miglioramenti non sono omogenei per i diversi intermediari e sono più evidenti per le operazione di importo elevato.

Appendice

Fig. A1: Importo medio per operazione fraudolenta
(valori in €)



Fonte: nostre elaborazioni su dati BCE.

Tav. A1: Stima panel del tasso di frode on line (*balanced*)

	Valore			Numero		
VARIABLES	OLS online FRAUD rate	FE online FRAUD rate	RE online FRAUD rate	OLS online FRAUD rate	FE online FRAUD rate	RE online FRAUD
qrete	28.45***	20.03	20.33	-7.361	35.94	21.42**
	(-6.55)	(-23.11)	(-14.67)	(-5.128)	(-19.21)	(-9.161)
shareem	-4.191***	-2.178	-2.422**	-1.034**	0.341	0.052
	(-0.584)	(-1.202)	(-1.187)	(-0.411)	(-0.304)	(-0.516)
h	0.279	0.258**	0.262***	0.0684	-0.0445	-0.00993
	(-0.298)	(-0.0793)	(-0.066)	(-0.23)	(-0.113)	(-0.108)
y	0.207	0.264	0.259	0.245**	0.158	0.19
	(-0.135)	(-0.19)	(-0.182)	(-0.104)	(-0.17)	(-0.16)
EBA	-1.046*	-1.023*	-1.026**	-1.101***	-1.078***	-1.084***
	(-0.545)	(-0.478)	(-0.48)	(-0.391)	(-0.237)	(-0.232)
Constant	-424	-540.3	-530	-501.9**	-326.4	-391.5
	(-271.8)	(-383.3)	(-367.7)	(-210.5)	(-341.9)	(-322.1)
Osservazioni	96	96	96	96	96	96
R-squared	0.451	0.315		0.154	0.218	
Numero di enti segnalanti		6	6		6	6

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Glossario

ACQUIRER (soggetto convenzionatore): prestatore di servizi di pagamento che, sulla base di uno specifico contratto stipulato con il beneficiario (di solito un esercente), è responsabile della raccolta e della gestione dei flussi informativi relativi alle transazioni effettuate, nonché del trasferimento di fondi a favore del beneficiario.

ATM (Automatic teller machine): terminale che consente agli utenti autorizzati, generalmente attraverso l'utilizzo di carte, di effettuare operazioni di prelievo di contanti e/o accedere ad altri servizi, quali richieste di informazioni sul saldo, trasferimento di fondi o il versamento di contante e assegni. Un dispositivo che consente esclusivamente richieste di informazioni sul saldo non si qualifica come ATM.

BLOCCO/ALERT: misure utilizzate per prevenire le frodi. Consistono essenzialmente nel bloccare l'operatività della carta o nell'invio di un SMS per operazioni ritenute rilevanti, di importo superiore ad una certa soglia o comunque sospette perché, ad esempio, diverse da quelle tipicamente effettuate dal possessore dalla carta.

CARDHOLDER: titolare di una carta di pagamento sulla base di un contratto con il prestatore di servizi di pagamento *issuer*.

CARTE DI CREDITO: strumento di pagamento che consente ai titolari di effettuare acquisti di beni e servizi presso qualsiasi esercizio aderente al circuito e in alcuni casi, prelievi di contante, nei limiti di una linea di credito prestabilita e accordata dall'Istituto emittente. L'importo delle operazioni effettuate è addebitato totalmente o in parte ad una data specifica concordata tra le parti, senza o con interessi.

CARTE DI DEBITO: strumento di pagamento che abilita il titolare ad effettuare acquisti di beni e servizi presso esercenti aderenti al circuito, tramite il terminale POS, oppure prelievi e versamenti di contanti presso gli ATM; ogni transazione è regolata con valuta del giorno stesso tramite addebito sul conto di pagamento a esso collegato.

CARTE PREPAGATE: strumento di pagamento su cui è caricata moneta elettronica, quale definita all'articolo 2, punto 2, della Direttiva 2009/110/CE.

E-COMMERCE: definito generalmente come la vendita o l'acquisto di beni o servizi, tra imprese, famiglie, individui o organizzazioni private, attraverso transazioni elettroniche condotte via Internet o altre reti informatiche (comunicazione *online*).

EMV (Europay Mastercard Visa): standard globalmente riconosciuto per regolare i pagamenti elettronici con carte di pagamento dotati di microprocessore presso terminali POS e ATM.

FRODE PER CARTA NON RICEVUTA: una transazione fraudolenta che si verifica con l'utilizzo di una carta che il pagatore afferma di non aver ricevuto, nonostante il prestatore di servizi confermi di aver inviato.

FRODE PER CARTA CONTRAFFATTA: uso di una carta di pagamento alterata o riprodotta in maniera illegale (include quindi l'alterazione o la replica della banda magnetica e/o del chip).

FRODE CON CARTA SMARRITA/RUBATA: una transazione fraudolenta che si verifica con l'uso di una carta di pagamento smarrita o rubata senza l'effettiva, implicita o apparente autorizzazione del titolare della carta.

ISSUER (emittente): un'istituzione finanziaria che fornisce ai titolari le carte di pagamento, autorizza operazioni presso terminali POS e ATM e garantisce il pagamento all'*acquirer* per le operazioni che sono conformi alle regole del relativo schema di carte di pagamento.

MARCHIO DI PAGAMENTO: nome, termine, segno o combinazione di questi, in forma materiale o digitale, in grado di indicare lo schema di carte di pagamento nell'ambito del quale sono effettuate le operazioni di pagamento basate su carta.

MERCHANT (esercente): soggetto autorizzato a ricevere fondi in cambio della consegna di merci e/o servizi; stipula specifici contratti con il soggetto *acquirer* per l'accettazione di tali fondi.

OPERAZIONE CARD NOT PRESENT (CNP): operazione di pagamento iniziata tramite la rete Internet o tramite un dispositivo che può essere utilizzato per comunicare a distanza (smartphone, tablet, ecc.).

OPERAZIONE CARD PRESENT (CP): operazione di pagamento presso esercizi commerciali fisici o sportelli automatici in cui il titolare della carta e la carta stessa sono presenti contemporaneamente presso il terminale.

OPERAZIONE DI PAGAMENTO NAZIONALE: per le **operazioni basate su carta non a distanza** (CP), ci si riferisce alle operazioni in cui il prestatore di servizi di pagamento del pagatore, il prestatore di servizi di pagamento del beneficiario e il punto vendita (POS) o sportello automatico (ATM) utilizzati sono situati nello stesso Stato membro. Per le **operazioni di pagamento basate su carta a distanza** (CNP), ci si riferisce ad operazioni disposte da un pagatore (o da un beneficiario o per il suo tramite) quando il prestatore di servizi di pagamento del pagatore e quello del beneficiario sono situati nello stesso Stato.

OPERAZIONE DI PAGAMENTO TRANSFRONTALIERA (CROSS BORDER): per le **operazioni basate su carta non a distanza** (CP), ci si riferisce alle operazioni in cui il prestatore di servizi di pagamento del pagatore e quello del beneficiario si trovano in Stati diversi, oppure il prestatore di servizi di pagamento del pagatore è situato in uno stato membro diverso da quello del punto vendita (POS) o sportello automatico (ATM) utilizzato. Per le **operazioni di pagamento basate su carta a distanza** (CNP), ci si riferisce ad operazioni disposte da un pagatore (o da un beneficiario o per il suo tramite) quando il prestatore di servizi di pagamento del pagatore e quello del beneficiario sono situati in Stati diversi.

PHISING: attività illecita volta ad acquisire dati sensibili o riservati da soggetti (ad esempio: numero carta di credito, conto corrente, password, documenti di identità, ecc.), al fine di ottenere linee di credito o effettuare altre operazioni (ad esempio: acquisti) sotto falsa identità. Le informazioni vengono acquisite da organizzazioni illecite in genere via Internet, contattando i legittimi titolari anche attraverso la falsificazione e l'utilizzo di "marchi", "loghi" e indirizzi di posta elettronica di importanti istituzioni finanziarie.

POS (Point of sales): apparecchiatura automatica mediante la quale è possibile effettuare il pagamento di beni o servizi presso il fornitore degli stessi utilizzando carte di pagamento. L'apparecchiatura consente il trasferimento delle informazioni necessarie per l'autorizzazione e la registrazione, in tempo reale o differito, del pagamento.

PROCESSOR: soggetto, persona fisica o giuridica, incaricato del trattamento dell'operazione, in termini di azioni necessarie per l'esecuzione dell'ordine di pagamento tra il soggetto convenzionatore e l'emittente.

SCHEMA DI CARTE DI PAGAMENTO: insieme unico di norme, prassi, standard e/o linee guida di attuazione pe l'esecuzione di operazioni di pagamento basate su carta, separato da qualsiasi infrastruttura o sistema di pagamento che ne sostenga le operazioni, che includa

specifici organi decisionali, organizzazioni, o entità responsabili del funzionamento dello schema.

SCHEMA DI CARTE DI PAGAMENTO A QUATTRO PARTI: schema di carte in cui le operazioni di pagamento basate su carta sono effettuate dal conto di pagamento del pagatore verso il conto del beneficiario tramite l'intermediazione dello schema, dell'*issuer* e dell'*acquirer*.

SCHEMA DI CARTE DI PAGAMENTO A TRE PARTI: schema di carte in cui lo schema stesso fornisce servizi di convenzionamento e di emissione e le operazioni di pagamento basate su carta sono effettuate dal conto di pagamento del pagatore al conto del beneficiario nell'ambito dello schema stesso; lo schema di carte che concede ad altri la licenza di emissione di strumenti di pagamento, o di convenzionamento di operazioni basate su carte, o emette strumenti di pagamento basati su carta con un partner di carta multimarchio in *co-branding* o tramite agente è considerato uno schema a quattro parti.

TOKENIZZAZIONE: è il processo di sostituzione dei dati sensibili (ad es. numero di conto o carta) con identificatori univoci (*token*) che sostituiscono o mascherano gli attributi associati ai dati originali.

STRONG CUSTOMER AUTENTICATION (SCA): autenticazione del pagatore basata sull'uso di due o più elementi classificati come conoscenza (qualcosa che solo l'utente conosce), possesso (qualcosa che solo l'utente possiede) e inerenza (qualcosa che l'utente è) che sono indipendenti, per cui la violazione di uno non compromette l'affidabilità degli altri; è progettata in modo tale da proteggere la riservatezza dei dati di autenticazione.

Bibliografia

Ardizzi, G. (2012), *The Impact of Microchips on Payment Card Fraud*, Journal of Financial Market Infrastructures, Vol. 1, n. 2, December

Ardizzi, G. (2017), *Innovation in Customer Authentication Methods, Card-based Internet Payments and User Experience: Empirical Evidence from Italy*, Joint BCE-BI conference, Rome, 30 November-1 December

BCE (aa. vv.*), Report on Card Fraud*

Commissione Europea (2012), *Libro Verde - Verso un mercato europeo integrato dei pagamenti tramite carte, internet e telefono mobile,* Bruxelles.

Giacomelli A. (2008), "Non si gioca con le carte", in Internal Audit, May-August.

HSN Consultants (2018), *The Nilson Report*, November, #1142

HSN Consultants (2019), *The Nilson Report*, November, #1164