



BANCA POPOLARE[®]
del FRUSINATE

**POLICY SULLA GESTIONE DEI
DISCONOSCIMENTI DI OPERAZIONI DI
PAGAMENTO**

CRONOLOGIA DELLE MODIFICHE APPORTATE

Data Approvazione Consiglio di Amministrazione	Note
XX/05/2025	Prima stesura della Policy sulla gestione dei disconoscimenti delle operazioni di pagamento

INDICE

CRONOLOGIA DELLE MODIFICHE APPORTATE.....	1
1. PREMESSA	3
2. GLOSSARIO	3
3. AMBITO DI APPLICAZIONE	5
4. RIFERIMENTI NORMATIVI	6
5. RUOLI E RESPONSABILITA'	6
6. PERIMETRO DELLE OPERAZIONI DI PAGAMENTO	7
7. LINEE GUIDA PER IL PROCESSO DI GESTIONE DEI DISCONOSCIMENTI	8
7.1 TRASPARENZA NELLE COMUNICAZIONI CON LA CLIENTELA	9
7.2 FORMAZIONE E SENSIBILIZZAZIONE DEL PERSONALE E DEI CLIENTI.....	9
7.3 STRUMENTI A DISPOSIZIONE DEL CLIENTE PER COMUNICARE IL DISCONOSCIMENTO	10
7.4 GESTIONE DEI DISCONOSCIMENTI	11
8. LA SOSPENSIONE DEL RIMBORSO E LA GESTIONE DELLE SEGNALAZIONI A BANCA D'ITALIA.....	20
8. GIURISPRUDENZA ABF RILEVANTE.....	21
9. APPROVAZIONE, MODIFICHE E AGGIORNAMENTI	21

1. PREMESSA

La presente Politica (di seguito anche la “Policy”), adottata dalla Banca Popolare del Frusinate (di seguito anche la “Banca”) definisce le linee guida da attuarsi nel processo di gestione dei disconoscimenti delle operazioni di pagamento (di seguito anche i “Disconoscimenti”), al fine di garantire ai clienti l’esercizio dei propri diritti e favorire nel contempo il rispetto degli obblighi normativi a carico della Banca.

Le regole della Banca definite nella presente Policy mirano ad assicurare che, in ogni fase delle attività di trattazione e gestione delle richieste di Disconoscimento trasmesse dai clienti, sia prestata costante e specifica attenzione: i) alle circostanze fattuali dell’evento; ii) ai comportamenti tenuti dai soggetti coinvolti nell’esecuzione di una operazione di pagamento, al fine di garantire una efficiente e corretta gestione delle richieste ricevute dalla Banca in conformità con la normativa di riferimento.

Il documento definisce inoltre ruoli e responsabilità anche con riferimento alla segnalazione delle frodi.

2. GLOSSARIO

Nella presente Policy i seguenti termini hanno il significato (c.d. “Definizioni”) sottoindicato:

Addebito diretto	Servizio di pagamento nazionale o transfrontaliero per l’addebito di un conto di pagamento del pagatore in cui un’operazione di pagamento è iniziata dal beneficiario in base al consenso del pagatore.
Autenticazione	Si tratta di una procedura che consente al prestatore di servizi di pagamento di verificare l’identità di un utente di servizi di pagamento o la validità dell’uso di uno specifico strumento di pagamento, incluse le relative credenziali di sicurezza personalizzate fornite dal prestatore.
Autenticazione forte del cliente	Si tratta di un’autenticazione basata sull’uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l’utente conosce), del possesso (qualcosa che solo l’utente possiede) e dell’inerenza (qualcosa che caratterizza l’utente), che sono indipendenti, in quanto la violazione di uno non compromette l’affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione.
Beneficiario	Il soggetto previsto quale destinatario e beneficiario dei fondi oggetto dell’operazione di pagamento.
Cliente	Persona fisica (consumatore e non), persona giuridica ed altro ente con cui la Banca intrattiene rapporti di durata (a tempo determinato o indeterminato) inerenti servizi di pagamento, sulla

	base di specifica disciplina contrattuale (contratto quadro).
Contratto quadro	Il contratto che disciplina la futura esecuzione di operazioni di pagamento singole e ricorrenti e che può dettare gli obblighi e le condizioni che le parti devono rispettare per l'apertura e la gestione di un conto di pagamento.
Disconoscimento	Attività attraverso cui si può richiedere (se si è titolare di un conto corrente o di una carta di pagamento – es. carta di credito, carta di debito, carta prepagata anche con IBAN) il rimborso e/o la rettifica di una operazione che non è stata autorizzata o non è stata correttamente eseguita.
Frode	Azione deliberatamente volta ad ingannare o truffare qualcuno al fine di ottenere un vantaggio personale illegittimo. In genere comporta l'uso di mezzi illeciti, come la falsificazione di documenti, la manipolazione di dati o l'inganno di persone al fine di ottenere denaro, beni, servizi o qualsiasi altra forma di vantaggio materiale.
ID Caller Spoofing	Caso di frode che consiste in una telefonata nel corso della quale un sedicente operatore del prestatore di servizi di pagamento induce la vittima nella falsa rappresentazione di dover fornire dati e credenziali al fine di bloccare un'operatività fraudolenta, ovvero di stornare operazioni non autorizzate.
Operazione di pagamento	Attività, posta in essere dal pagatore o dal beneficiario, di versare, trasferire o prelevare fondi, indipendentemente da eventuali obblighi sottostanti tra pagatore e beneficiario.
Operazione di pagamento non autorizzata	Operazione di pagamento in assenza di consenso del cliente nell'esecuzione dell'operazione.
Operazione di pagamento non correttamente eseguita	L'esecuzione dell'operazione non è conforme all'ordine o alle istruzioni impartite (es. l'importo dell'operazione non è corretto).
Pagatore	Il soggetto titolare di un conto di pagamento a valere sul quale viene impartito un ordine di pagamento ovvero, in mancanza di un conto di pagamento, il soggetto che impartisce un ordine di pagamento.
Phishing	Caso di frode che solitamente consiste nell'invio di una e-mail o il rinvio ad un sito web "civetta" che simulano i canali istituzionali del prestatore di servizi di pagamento, ma che in realtà sono stati inviati o costruiti con l'unico scopo di aggirare gli utenti e carpire loro le credenziali di sicurezza personalizzate.
Prestatore di servizi di pagamento (o "PSP")	Soggetto che funge da intermediario nei pagamenti. Lo sono, ad esempio: istituti di moneta elettronica e istituti di pagamento nonché,

	quando prestano servizi di pagamento, banche, Poste Italiane s.p.a., la Banca centrale europea e le banche centrali nazionali se non agiscono in veste di autorità monetarie, altre autorità pubbliche, le pubbliche amministrazioni statali, regionali e locali se non agiscono in veste di autorità pubbliche.
Reclamo	Ogni atto con cui un cliente chiaramente identificabile contesta in forma scritta (ad esempio lettera, fax, e-mail) alla Banca un suo comportamento o un'omissione.
Spoofing	Caso di frode che consiste nel falsificare l'origine della connessione (indirizzo mittente della mail / numero di telefono) in modo da indurre a ritenere che il contatto provenga dal prestatore di servizi di pagamento. L'obiettivo è raccogliere informazioni personali o dati sensibili come le credenziali bancarie dell'utente.
Strumento di pagamento	Qualsiasi dispositivo personalizzato e/o insieme di procedure concordate tra l'utente e il prestatore di servizi di pagamento e di cui l'utente di servizi di pagamento si avvale per impartire un ordine di pagamento.
Smishing	Caso di frode che consiste nell'invio di messaggi di testo per indurre in errore i clienti, invitandoli ad aprire link dannosi con lo scopo di sottrarre loro i dati personali o indurli a comunicare le proprie credenziali/informazioni personali
Ufficio Reclami	Struttura cui compete la trattazione dei reclami ricevuti dalla Banca.
Vishing o Voice Phishing	Caso di frode che consiste in una truffa telefonica con cui il frodatore cerca di indurre la vittima a fornire dati personali, fingendosi un dipendente / incaricato della banca o del prestatore di servizi di pagamento. Per concretizzare tale tecnica, il terzo frodatore utilizza tecniche di persuasione, di inganno ed in grado di ledere la capacità cognitiva e di giudizio della vittima.

3. AMBITO DI APPLICAZIONE

La Direttiva PSD2 (di seguito anche la "PSD2") si applica a tutti i servizi di pagamento prestati nell'UE, tra cui bonifici, addebiti diretti, carte di credito, debito e prepagate, portafogli elettronici e altri pagamenti via internet. La PSD2 prevede inoltre lo sviluppo dell'Open Banking, che consente ai clienti di autorizzare terze parti ad accedere ai propri dati bancari per l'offerta di nuovi servizi.

Le principali finalità della Direttiva sono contrastare le frodi e accrescere la fiducia dei consumatori nei pagamenti digitali modernizzando il quadro normativo che regola i servizi digitali innovativi.

4. RIFERIMENTI NORMATIVI

- D.lgs. del 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218, che ha recepito la direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13 gennaio 2018;
- Regolamento UE 2022/2554 (DORA - Digital Operational Resilience Act);
- Norme generali in tema di adempimento delle obbligazioni e sulla diligenza del mandatario (art. 1710 c.c.) e della Banca nell' *"Esecuzione d'incarichi"* (art. 1856 c.c.)

Con riferimento alla normativa interna:

- Policy Metodologia di gestione del rischio ICT e di sicurezza;
- Regolamento trasparenza;

5. RUOLI E RESPONSABILITA'

Il presente paragrafo descrive ruoli e responsabilità delle strutture organizzative della Banca coinvolte nel processo di gestione dei Disconoscimenti.

- **Consiglio di Amministrazione:** approva la Policy ed eventuali modifiche e/o integrazioni sostanziali al documento;
- **Amministratore Delegato/Direttore Generale:** attua gli indirizzi deliberati dal Consiglio di Amministrazione con riferimento alla sicurezza informatica della Banca.
- **L'Ufficio IT:** è l'Ufficio che è stato designato a seguire i disconoscimenti. In coerenza con le strategie e gli obiettivi definiti dal Consiglio di Amministrazione ottimizza i processi aziendali per poter rispondere ai nuovi rischi e alle evoluzioni del panorama delle minacce informatiche; garantisce che i processi aziendali e le politiche interne siano conformi alle leggi e regolamenti relativi alla sicurezza informatica (come GDPR, NIS Directive, DORA, ecc.); sviluppa, in collaborazione con altre funzioni, piani per rispondere ad eventi (come cyber attacchi o guasti tecnici) che potrebbero compromettere i sistemi informatici della Banca; rivede inoltre con cadenza periodica e comunque in occasione di aggiornamenti della normativa di riferimento, la presente Policy al fine di verificare l'adeguatezza e l'efficacia, in modo tale da porre rimedio alle carenze eventualmente riscontrate nonché approvare le azioni di rimedio individuate nella gestione dei disconoscimenti;
- **L'Ufficio Monetica:** gestisce i processi operativi in materia di disconoscimenti di operazioni di pagamento e di segnalazioni di frodi relative a tali operazioni;
- **L'Ufficio Contabilità:** garantisce la predisposizione e l'inoltro a Banca d'Italia delle segnalazioni di vigilanza riferite ai dati riguardanti le frodi connesse ai diversi mezzi di pagamento;
- **L'Ufficio Reclami:** prende in carico il reclamo inerenti i sistemi di pagamento valutandone la legittimità della richiesta.

- **Funzione di Compliance:** monitora l'evoluzione della normativa in tema di disconoscimenti, ivi compresi gli orientamenti dell'ABF, provvedendo ad informare la struttura in merito alle novità afferenti a principi, prassi operative e metodologie, e promuovendo l'adozione di best practice da adottare in sede di gestione della richiesta di disconoscimento;
- **L'Ufficio Risk Management:** deputata al monitoraggio del complesso dei rischi e in particolare allo svolgimento dell'attività di controllo dei rischi ICT e di sicurezza;
- **L'Ufficio Legale:** nello svolgimento delle attività di prevenzione e gestione dei rischi legali, fornisce consulenza e assistenza legale alle strutture organizzative, valuta il rischio di contenzioso derivante dalle richieste di Disconoscimento, fornendo assistenza operativa, presidiando e gestendo i procedimenti civili, penali, sanzionatori in cui la Banca è coinvolta;
- **L'Ufficio Organizzazione:** monitora l'adeguata strutturazione delle funzioni coinvolte nel processo descritto dalla presente Policy ed eroga al personale coinvolto una formazione specifica ed adeguata rispetto ai compiti svolti;

La presente Policy non disciplina le richieste dei clienti relative a c.d. "*dispute commerciali*", disciplinate invece nel Regolamento Trasparenza - Paragrafo dedicato ai Reclami.

6. PERIMETRO DELLE OPERAZIONI DI PAGAMENTO

Le operazioni di pagamento che rientrano nel perimetro della normativa PSD sono le operazioni disposte tramite:

1. canali virtuali;
2. bonifici SCT (Sepa Credit Transfers); SCT Inst (Sepa Instant Credit Transfers) effettuati anche tramite home banking, ATM/CSA e PISP;
3. addebito diretto Sepa Direct Debit (SDD);
4. carta di pagamento emessa dalla Banca (e non);
5. carte prepagate.

La presente Policy, dunque, definisce le modalità con cui la Banca gestisce i Disconoscimenti derivanti da:

- operazioni di pagamento non autorizzate ovvero non correttamente eseguite: bonifico, pagamenti con carta di pagamento (debito/credito/prepagata), SDD Core e SDD B2B - Sepa Direct Debit, altre operazioni di pagamento (ad esempio pagamento bollettini, MAV, ecc.);
- operazioni di pagamento formalmente autorizzate ma disconosciute in un secondo momento: bonifico, pagamenti con carta di pagamento (debito/credito/prepagata), SDD Core e SDD B2B - Sepa Direct Debit, altre operazioni di pagamento (ad esempio pagamento bollettini, MAV, ecc.);
- operazioni di pagamento autorizzate disposte su iniziativa del beneficiario o per il suo tramite;
- operazioni di pagamento disposte tramite SDD Core, qualora la comunicazione del disconoscimento sia ricevuta dalla Banca entro 8 settimane dalla data di addebito.

La Banca esegue una operazione di pagamento, o una serie di operazioni di pagamento, sulla base del consenso rilasciato dal cliente, prestato nella forma e secondo la procedura convenuta tra quest'ultimo e la Banca nel contratto quadro o nel contratto relativo a singole operazioni di pagamento. Il consenso del cliente può essere prestato alla Banca direttamente, o tramite il beneficiario del pagamento, o tramite un prestatore di servizi di disposizione di un ordine di pagamento (PISP).

Un'operazione, dunque, è considerata non autorizzata se:

- è eseguita in mancanza del consenso del cliente;
- è effettuata sulla base di un consenso poi revocato dal cliente, a condizione che la revoca avvenga prima che l'ordine di pagamento diventi irrevocabile.

Ai fini della presente Policy è considerata non autorizzata, in caso di Disconoscimento, qualunque operazione di pagamento disposta senza l'adozione della Strong Customer Authentication (SCA) prevista dalla Banca e contrattualizzata con il cliente per la quale non è applicabile un'esenzione della SCA.

La gestione dei Disconoscimenti e la segnalazione delle frodi relative a strumenti di pagamento (carte di credito / debito / prepagate) emesse e gestite da terzi emittenti e solo distribuite dalla Banca sono direttamente in capo all'emittente dello strumento di pagamento ⁽¹⁾, secondo le modalità descritte nella presente Policy, previamente concordate dalla Banca con il soggetto emittente lo strumento di pagamento.

7. LINEE GUIDA PER IL PROCESSO DI GESTIONE DEI DISCONOSCIMENTI

In coerenza con le previsioni normative, l'utente che riceve uno strumento di pagamento, adotta tutte le misure idonee a proteggere le credenziali di sicurezza personalizzate e, secondo le modalità previste nel contratto quadro, comunica senza indugio alla Banca lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento non appena ne viene a conoscenza.

La Banca, qualora l'utente neghi di aver autorizzato un'operazione di pagamento già eseguita, ha l'onere di provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

Inoltre, in aggiunta alla prova di autenticazione dell'utente, la Banca, ove intenda invocare una responsabilità esclusiva dell'utente deve fornire la prova della frode, del dolo o della colpa grave dell'utente.

1) Si rappresenta che con riferimento alle operazioni di pagamento eseguite dai clienti con gli strumenti di pagamento (carte di credito / debito / prepagate), dato che il rapporto contrattuale è sottoscritto tra il cliente e l'emittente lo strumento di pagamento, le richieste di Disconoscimento saranno avanzate direttamente all'emittente della carta, secondo le modalità indicate nel predetto contratto.

7.1 Trasparenza nelle comunicazioni con la clientela

Nella fase precontrattuale, la normativa impone una serie di obblighi di trasparenza e di informazione riguardo alle operazioni di pagamento non autorizzate. L'obiettivo è garantire che il cliente sia correttamente informato sui suoi diritti e sulle procedure da seguire nel caso in cui si verifichino transazioni non autorizzate.

Innanzitutto, la Banca fornisce al cliente la documentazione di trasparenza contenente un'informativa adeguata volta ad assicurare la piena consapevolezza della clientela in merito al riconoscimento dei propri diritti e alle modalità di adempimento dei propri doveri.

La Banca informa il cliente che è obbligato a segnalare tempestivamente eventuali operazioni non autorizzate; la segnalazione deve essere effettuata entro 13 mesi dalla data di addebito, nel caso del pagatore, o di accredito, nel caso del beneficiario. Tale termine non opera se l'utente ha ommesso di fornire o non ha messo a disposizione le informazioni relative all'operazione di pagamento sulla tempistica della segnalazione.

Nel caso di operazioni di pagamento autorizzate disposte dal beneficiario o per il suo tramite il pagatore può chiedere il rimborso entro otto settimane dalla data in cui i fondi sono stati addebitati.

Il cliente, tramite l'informativa predisposta dalla Banca, viene informato sulle modalità e i tempi di rimborso nel caso di disconoscimento di transazioni non autorizzate. La normativa prevede che il rimborso dell'operazione debba essere effettuato immediatamente e, in ogni caso, entro la fine della giornata operativa successiva a quella in cui la Banca prende atto dell'operazione o riceve una comunicazione di Disconoscimento in merito.

Nel corso della giornata operativa, la Banca verifica l'esistenza o meno dell'autorizzazione dell'utente rilasciata nella forma e secondo la procedura concordata nel contratto quadro PSD.

Nella documentazione contrattuale la Banca fornisce una chiara spiegazione sui meccanismi di sicurezza utilizzati per autorizzare i pagamenti, come la autenticazione forte del cliente (c.d. SCA), che richiede l'uso di almeno due fattori di autenticazione (ad esempio, una combinazione di password, biometria e codice OTP). Il cliente deve essere reso consapevole che eventuali operazioni non autorizzate potrebbero derivare da un uso improprio di tali credenziali di accesso.

La Banca informa il cliente su come disconoscere operazioni non autorizzate e a chi rivolgersi in caso di disaccordo. Il cliente è informato del suo diritto di ricorrere alla risoluzione alternativa delle controversie (ADR) o all'Autorità competente ovvero di presentare esposto alla Banca d'Italia.

7.2 Formazione e sensibilizzazione del personale e dei clienti

La Banca definisce percorsi formativi a tutto il personale coinvolto nel rapporto con la clientela e nel processo delle operazioni di pagamento affinché sia adeguatamente informato sulla normativa vigente, come la direttiva europea sui servizi di pagamento (PSD2).

I percorsi formativi sono strutturati in modo che i dipendenti conoscano e attuino le politiche e le procedure interne della Banca in relazione alla gestione dei Disconoscimenti, nonché le scadenze e i tempi di risposta previsti dalla legge. In particolare, il personale viene istruito su come esaminare le richieste di disconoscimento valutando e verificando (mediante l'analisi dei File di Log) se le operazioni disconosciute sono state correttamente autenticate, registrate e contabilizzate secondo la procedura SCA adottata dalla Banca, verificando eventuali anomalie nelle transazioni, e considerando la possibilità di errore o frode ovvero la sussistenza di profili idonei ad identificare il dolo o la colpa grave del cliente.

Inoltre, la Banca promuove campagne di sensibilizzazione dei clienti sui tipi comuni di frode, come la clonazione delle carte, le truffe via e-mail o telefoniche, e altre tecniche utilizzate dai truffatori per ottenere accesso ai loro dati bancari. La Banca, quindi, informa i clienti sui rischi di phishing, truffe online e altre tecniche fraudolente che potrebbero portare a operazioni non autorizzate, illustrando gli elementi tipizzanti e caratterizzanti le più comuni tipologie di truffa/frode (e come si presentano) al fine di consentire ai clienti / utenti di avvertirne la pericolosità e i rischi, raccomandando ai clienti adeguate precauzioni e/o accorgimenti per evitare di incorrere in tali situazioni, avvertendo in particolare il cliente che la Banca non richiede mai di comunicare dati/credenziali personalizzate relative all'utilizzo di uno strumento di pagamento per le vie brevi ovvero mediante l'invio di sms e/o email contenenti link da cliccare.

7.3 Strumenti a disposizione del cliente per comunicare il disconoscimento

La Banca mette a disposizione dei clienti una varietà di canali, sia digitali che tradizionali, per comunicare il Disconoscimento di un pagamento.

Le modalità di comunicazione di una richiesta di Disconoscimento e i connessi diritti sono definiti e illustrati alla clientela sulla pagina dedicata del sito internet della Banca. La richiesta di Disconoscimento e la successiva interazione della Banca con il cliente non è sottoposta ad alcun costo od onere ed i canali messi a disposizione dei clienti devono essere idonei a consentire a questi ultimi di effettuare tale richiesta in modo agevole e senza ostacoli.

Prima di procedere alla comunicazione di Disconoscimento di operazioni di pagamento, è opportuno che il cliente, qualora si renda conto di non aver autorizzato un'operazione, blocchi la carta o l'Internet banking o l'app seguendo le indicazioni riportate sul sito della Banca. Tale operatività, tuttavia, non è requisito procedurale preliminare all'inoltro di una richiesta di Disconoscimento da parte del cliente.

La Banca, al fine di tutelare il cliente, ha previsto l'utilizzo della c.d. *SCA – Strong Customer Authentication*, salvo i casi previsti per legge per cui è prevista un'esenzione della SCA.

La Banca inoltre prevede l'abilitazione di notifiche o SMS o e-mail per ogni transazione nonché *alert* informativi relativi ad ogni accesso effettuato alle piattaforme di Home banking e/o in relazione alle fasi di installazione ed attivazione dell'APP Mobile/Token software della Banca necessari per l'utilizzo dei servizi di banca telematica, attraverso cui i clienti possono identificare rapidamente un'operazione sospetta.

Al fine di supportare il cliente, la Banca dà informativa sul proprio sito internet dei numeri di telefono da contattare per segnalare transazioni disconosciute, permettendo ai clienti di effettuare la segnalazione in qualsiasi momento.

È prevista la possibilità di inviare un Disconoscimento (al pari di un reclamo) tramite e-mail, posta elettronica certificata ovvero per posta ordinaria raccomandata.

Il cliente, inoltre, considerato che potrebbe essere sprovvisto dell'Internet banking, ha in ogni caso la possibilità di recarsi presso una filiale della Banca dove l'operatore raccoglie tutte le informazioni necessarie e assiste il cliente nel completamento delle formalità del Disconoscimento.

La formalizzazione per iscritto che precedono non costituiscono, tuttavia, requisito necessario per la gestione della richiesta di Disconoscimento.

Nella eventualità in cui il cliente proceda ad informare la Banca di un Disconoscimento presentando direttamente un reclamo/esposto a Banca d'Italia, l'Ufficio Reclami della Banca provvede tempestivamente a segnalare la circostanza alla Filiale di riferimento ovvero alle Strutture competenti, le quali si attivano tempestivamente per raccogliere (anche attraverso le altre Funzioni interessate della Banca, eventuali informazioni necessarie per la gestione della richiesta e avvia le attività di valutazione e rimborso nei tempi previsti dalla normativa esterna ed interna (come declinati nei paragrafi che seguono della presente Policy).

Tra le informazioni/documentazione richieste/a ai fini della gestione di un Disconoscimento la Banca non richiede al cliente copia della denuncia /querela presentata all'Autorità di Pubblica Sicurezza o altra documentazione aggiuntiva (quali ed esempio, copia di e-mail, sms, registro delle telefonate) quale presupposto per avviare la pratica di Disconoscimento e procede (ove dovuto) con il conseguente rimborso. Resta in ogni caso ferma la facoltà per la Banca di richiedere ed acquisire tale documentazione dal cliente in un momento successivo ai fini della istruttoria.

La Banca informa il cliente, con specifica comunicazione, dell'apertura della pratica di Disconoscimento e di ogni suo aggiornamento, sia positivo che negativo; il linguaggio utilizzato nelle comunicazioni con il cliente deve essere chiaro e comprensibile.

In particolare, nel caso di rigetto del rimborso, la Banca motiva chiaramente al cliente le ragioni sottostanti il diniego affinché il cliente possa comprenderle e rappresenta (sempre) al cliente la possibilità di far valere i propri diritti nelle sedi competenti (quali Arbitro Bancario Finanziario o altri ADR; Autorità giudiziaria ordinaria) ovvero del suo diritto di proporre esposto alla Banca d'Italia.

7.4 Gestione dei disconoscimenti

A. Processo di gestione dei Disconoscimenti di operazioni di pagamento non autorizzate tramite SCA ovvero non correttamente eseguite, diverse da SDD

A.1. Verifica dei presupposti

Nel caso di operazioni di pagamento non autorizzate tramite SCA o non correttamente eseguite, il cliente ha diritto a richiedere la rettifica dell'operazione entro e non oltre 13 (tredici) mesi dalla data di addebito (nel caso di pagatore) ovvero di accredito (nel caso di beneficiario).

Ricevuta la richiesta di Disconoscimento di una operazione di pagamento da parte del cliente, le strutture competenti della Banca sono tenute a verificare (in via preliminare) il rispetto del suddetto termine di 13 (tredici) mesi, oltre il quale il cliente non ha più il diritto ad ottenere alcuna rettifica nel caso di operazioni di pagamento non autorizzate o non correttamente eseguite.

Con preciso riferimento alle operazioni non autorizzate, il mancato rispetto del termine di 13 (tredici) mesi preclude al cliente ogni possibilità di ottenere il rimborso. Resta impregiudicato il diritto del cliente di adire le competenti sedi stragiudiziali e/o giudiziarie.

Nei casi sopra esposti la Banca per il tramite dell'Ufficio IT evade la richiesta del cliente fornendo compiuto e chiaro riscontro al cliente.

Il termine di 13 (tredici) mesi non opera se la Banca ha omesso di fornire o mettere a disposizione del cliente le informazioni relative all'operazione di pagamento oggetto di Disconoscimento.

A.2. – Processo di valutazione e gestione

In caso di Disconoscimento di operazioni di pagamento non autorizzate con SCA, le Strutture competenti della Banca, prima di procedere con il rimborso, valutano le richieste di Disconoscimento allo scopo di accertare che:

- i) l'operazione oggetto di Disconoscimento non sia stata effettivamente autorizzata,
- ii) il Disconoscimento dell'operazione di pagamento non autorizzata non sia connesso ad una frode perpetrata dal cliente stesso a danno della Banca.

Tali verifiche e valutazioni devono essere completate tempestivamente al fine di consentire alla Banca di procedere con l'eventuale rimborso entro e non oltre la fine della giornata operativa successiva a quella in cui ha preso atto dell'operazione o ha ricevuto la comunicazione di Disconoscimento da parte del cliente.

Tale istruttoria, funzionale a pervenire ad una decisione circa il rimborso (o meno), è basata sugli elementi forniti dal cliente in sede di Disconoscimento ovvero sugli altri elementi acquisibili e valutabili da parte della Banca (ad esempio la presenza e/o l'assenza della SCA) entro il predetto termine.

Nei casi di particolare rilevanza, le Strutture competenti alla gestione dei Disconoscimenti, pur dovendo sempre rispettare il suddetto termine di rimborso, possono richiedere supporto operativo alle altre Funzioni della Banca, al fine di concludere la valutazione della singola casistica.

L'eventuale valutazione circa la messa in atto di una frode da parte del cliente nei confronti della Banca deve basarsi su elementi di fatto robusti e oggettivi, utili a dimostrare - in maniera univoca ed inconfutabile - il dolo del cliente. Per tali valutazioni, è valutata attentamente la condotta del cliente, anche alla luce delle circostanze di fatto (ad esempio livello di sofisticazione/notorietà

della truffa, tempistiche di effettuazione delle operazioni disconosciute in caso di asserito furto degli strumenti di pagamento ecc..) nonché degli elementi informativi tecnici desunti dai sistemi informatici di sicurezza della Banca preposti alla prevenzione di frodi e/o all'erogazione del servizio di pagamento interessato.

Le evidenze ed attestazioni delle verifiche svolte sul singolo caso sono archiviate e conservate per un periodo pari a 10 (dieci) anni dalla data di esecuzione dell'operazione oggetto di Disconoscimento.

Laddove al rifiuto del rimborso da parte della Banca segue una richiesta di chiarimenti, la proposizione di un reclamo e/o di un esposto alla Banca d'Italia ovvero la presentazione di un ricorso dinanzi all'Arbitro Bancario Finanziario/Autorità giudiziaria ordinaria da parte del Cliente, le Strutture della Banca che hanno gestito il Disconoscimento forniscono alle Funzioni competenti alla gestione di reclami/ricorsi ABF/contenzioso una relazione scritta contenente tutti gli elementi oggettivi e robusti idonei a dimostrare (in maniera inconfutabile) il comportamento doloso del cliente.

A.2.1. Tempi di rimborso

Terminato il processo di valutazione di cui sopra, la Banca – tramite la Filiale di riferimento – entro e non oltre la fine della giornata operativa successiva a quella in cui ha preso atto dell'operazione o ha ricevuto la comunicazione di Disconoscimento da parte del cliente:

- esegue a favore del cliente un **rimborso definitivo**, di importo pari all'operazione disconosciuta, nel caso in cui i) non sia stata richiesta l'autenticazione forte per autorizzare l'operazione; ii) non sia possibile dimostrare e provare che l'operazione è stata autorizzata con SCA e iii) sia accertata, sulla base delle informazioni/documenti analizzati, l'assenza di dolo o colpa grave del cliente;
- esegue a favore del cliente un **rimborso salvo buon fine**, di importo pari all'operazione disconosciuta, allorquando, entro il predetto termine, abbia avuto modo di verificare che l'operazione è stata autorizzata tramite SCA ma non abbia concluso la valutazione sul comportamento/condotta del cliente ovvero non abbia a disposizione tutte le informazioni/documenti per concludere l'analisi;
- **non procede** con il rimborso a favore del cliente, allorquando l'operazione di pagamento risulta autorizzata a mezzo SCA e sia provata (sulla scorta di documenti ed elementi soggettivi ed oggettivi specifici per il caso di specie) la colpa grave ovvero il dolo del cliente.

La Banca, dunque, per il tramite dell'Ufficio IT, comunica tempestivamente (e in ogni caso entro e non oltre la fine della giornata operativa successiva a quella in cui ha preso atto dell'operazione o ha ricevuto la comunicazione di Disconoscimento da parte del cliente) al cliente, in forma scritta tramite posta elettronica certificata o posta raccomandata agli indirizzi indicati dal cliente nella richiesta di rimborso o diversamente agli indirizzi presenti nell'anagrafica della banca:.

- i) l'esecuzione del rimborso definitivo;

ii) l'esecuzione di un rimborso salvo buon fine e la prosecuzione delle relative attività di valutazione, avendo cura di specificare che l'eventuale esito negativo di tali valutazioni/istruttoria verrà prontamente comunicato al cliente, comportando il riaddebito del rimborso previamente eseguito;

iii) i motivi del mancato rimborso, con indicazione al cliente della facoltà di poter adire le sedi competenti (sia ADR sia ordinari).

A seguito dell'esecuzione di un rimborso salvo buon fine, la Filiale di riferimento della Banca e/o le Strutture competenti:

- richiede al cliente la trasmissione della documentazione necessaria (ad esempio la denuncia) entro 15 giorni di calendario dalla data in cui il cliente ha trasmesso il Disconoscimento;

- completa tutte le valutazioni entro 60 giorni (sessanta) di calendario dalla data in cui il cliente ha trasmesso (e la Banca ha ricevuto) il Disconoscimento, richiedendo alle altre Funzioni della Banca il supporto necessario per i profili di propria competenza funzionali a dirimere la specifica fattispecie;

- se entro il termine indicato nel punto che precede, sono riscontrate l'autorizzazione dell'operazione disconosciuta e la colpa grave e/o il dolo del cliente, la Banca ha il diritto di chiedere al cliente ed ottenere dal cliente la restituzione della somma inizialmente rimborsata, comunicando al cliente (per iscritto e secondo le modalità sopra esposte e concordate con questi) i motivi dell'addebito e la possibilità di far valere (in ogni caso) i propri diritti nelle sedi competenti ritenute più opportune;

- se entro il predetto termine accerta i) la mancata autorizzazione dell'operazione di pagamento e/o ii) l'assenza del dolo/colpa grave del cliente, mantiene fermo il rimborso in precedenza effettuato, comunicando al cliente l'esito dell'istruttoria e delle valutazioni condotte.

Ai fini della valutazione della colpa grave/dolo del cliente, la Banca adotta apposite griglie granulari (come disciplinata al paragrafo 8 della presente Policy), in cui sono valorizzati non solo i c.d. profili oggettivi, ma altresì i c.d. profili soggettivi. Le istruttorie sulle richieste di Disconoscimenti sono pertanto condotte tenuto conto dei criteri di ripartizione della responsabilità tra la Banca e il cliente, come previsti dalla normativa di settore, e dell'orientamento della giurisprudenza e dell'Arbitro Bancario Finanziario.

In ogni caso, pur a fronte delle griglie granulari, deve sempre essere assicurata una adeguata valutazione del comportamento nel concreto tenuto dal cliente in relazione a ciascuna fattispecie oggetto di Disconoscimento ed esame.

Fermo restando il rispetto del termine della giornata operativa successiva per garantire il rimborso di un'operazione NON autorizzata, la Banca (per il tramite delle Strutture competenti) adotta tutte le misure necessarie (ad es. la "recall") per ottenere il recupero della somma oggetto di operazione non autorizzata, restituendo la somma al cliente qualora sia stata recuperata prima dell'avvenuto rimborso oppure compensandola con il rimborso già effettuato al cliente.

A.2.3. - Data valuta

La Banca, nel disporre il rimborso dell'operazione di pagamento non autorizzata, riporta il conto addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito del rimborso non sia successiva a quella dell'addebito dell'importo, nonché il rimborso di eventuali interessi, spese e/o commissioni addebitate in relazione a tale operatività.

B. Processo di gestione dei Disconoscimenti di operazioni di pagamento autorizzate, diverse da SDD

Nel caso in cui il cliente – per esempio a seguito di una frode subita – disconosca una operazione di pagamento autorizzata (ossia una operazione eseguita in presenza del consenso del cliente prestato secondo la forma, le modalità e la procedura concordata nel contratto quadro o relativo a singole operazioni), la Banca verifica la sussistenza dei presupposti e procede con la valutazione della richiesta secondo quanto indicato nel paragrafo A.1. e nel paragrafo A.2. che precedono della presente Policy.

La Banca non esegue il rimborso nel termine previsto e sopra indicato (*cfr.* paragrafi A.2.1. e A.2.3. che precedono della presente Policy) solo nel caso in cui sia stato accertato che tale operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata (ossia che l'operazione è stata eseguita con la SCA).

Nel caso in cui l'operazione non risulti essere stata disposta/eseguita tramite SCA, la Banca esegue il rimborso al cliente in via definitiva.

La Banca, per il tramite dell'Ufficio IT:

- procede con l'accoglimento o il rigetto del rimborso secondo le modalità e nelle forme descritte nel precedente paragrafo A.2.1. e A.2.3 della presente Policy;
- prosegue con una istruttoria più approfondita della pratica, secondo le modalità descritte nel precedente paragrafo A.2.1. della presente Policy;

Nel caso in cui vi sia il motivato sospetto che l'operazione derivi da un comportamento fraudolento posto in essere dal cliente a danno della Banca, trova altresì applicazione quanto già descritto nel precedente paragrafo A.2.1. e nel successivo paragrafo 7 della presente Policy.

La Banca archivia e conserva le evidenze e le attestazioni delle verifiche svolte sul singolo caso di specie per un periodo pari a 10 (dieci) anni dalla data di esecuzione dell'operazione oggetto di disconoscimento.

C. Processo di gestione dei Disconoscimenti di operazioni di pagamento autorizzate disposte su iniziativa del beneficiario o per il suo tramite

C.1. - Verifica dei presupposti

Nel caso di Disconoscimenti di operazioni di pagamento disposte su iniziativa del beneficiario o per il suo tramite, la Banca verifica, in via preliminare, che la comunicazione di

Disconoscimento dell'operazione di pagamento sia stata ricevuta dalla Banca entro il termine delle 8 (otto) settimane dalla data in cui i fondi sono stati addebitati sul conto del cliente.

C.2. - Processo di valutazione e gestione

La Banca rimborsa l'intero importo dell'operazione di pagamento nel caso in cui ha verificato la sussistenza di entrambe le seguenti condizioni:

- al momento del rilascio, l'autorizzazione non specificava l'importo dell'operazione di pagamento;
- l'importo dell'operazione di pagamento supera quello che il cliente avrebbe potuto ragionevolmente aspettarsi avuto presenti il suo precedente modello di spesa, le condizioni del contratto quadro e le circostanze del caso specifico.

La Banca effettua tali valutazioni sulla base di documenti e di ogni altro elemento utili/e fornito dal cliente.

Nella dimostrazione del significativo discostamento del predetto importo rispetto al modello di spesa del cliente, il cliente non può far valere questioni legate al cambio, se è stato applicato il tasso di cambio concordato con la Banca.

Il diritto al rimborso è escluso se il cliente ha dato l'autorizzazione di pagamento direttamente alla Banca e, ove possibile, le informazioni sulla futura operazione di pagamento, limitatamente al caso in cui l'autorizzazione del pagatore è stata data prima della esecuzione dell'operazione di pagamento, sono state fornite o messe a disposizione del cliente pagatore dalla Banca o dal beneficiario almeno 4 (quattro) settimane prima dell'esecuzione dell'operazione

C.3. - Termini di rimborso

La Banca fornisce una giustificazione per il rifiuto del rimborso, entro 10 (dieci) giornate lavorative dalla ricezione della richiesta in forma scritta all'indirizzo di posta elettronica ordinaria registrato/certificato del cliente. In tal caso, la Banca comunica al cliente il suo diritto di presentare un esposto alla Banca d'Italia oppure di ricorrere ai sistemi stragiudiziali di cui all'art. 128-*bis* del TUB, ove non condivida la motivazione fornita dalla Banca.

Diversamente, qualora fosse confermato il rimborso, la Banca rimborsa l'intero importo dell'operazione di pagamento.

C.4. - Data valuta

La Banca, nel disporre il rimborso dell'operazione di pagamento, riporta in conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo, nonché il rimborso di eventuali interessi, spese e/o commissioni addebitate.

D. Processo di gestione dei Disconoscimenti di SDD Core ricevuti entro 8 settimane dalla data di addebito

D.1. - Verifica dei presupposti

Come previsto al paragrafo C.1. che precede della presente Policy, la Banca verifica (in via preliminare) anche per gli SDD Core che la comunicazione di Disconoscimento sia stata ricevuta dalla Banca entro 8 (otto) settimane dalla data in cui fondi sono stati addebitati sul conto del cliente.

D.2. - Processo di valutazione e gestione

Considerato che nel caso di Disconoscimenti di SDD Core il Cliente ha diritto incondizionato ad ottenere il rimborso dell'operazione, la Banca rimborsa l'intero importo dell'operazione di pagamento disconosciuta, indipendentemente da ogni valutazione.

Il Disconoscimento di un singolo addebito non è da intendersi come disconoscimento di tutti gli addebiti effettuati in forza del mandato autorizzativo, salvo diversa esplicita volontà del cliente. In quest'ultima casistica, la Banca rimborsa l'intero importo delle operazioni di pagamento addebitate nel periodo, che sono state oggetto di Disconoscimento entro il termine di 8 (otto) settimane dalla data di addebito.

D.3. - Tempi di rimborso

La Banca, in base allo schema SDD, garantisce al Cliente la disponibilità delle somme oggetto di disconoscimento al più tardi entro 10 (dieci) giornate lavorative dalla ricezione della richiesta, ferma l'opportunità, in ottica di ragionevolezza, di rimborsare immediatamente dopo il ricevimento della comunicazione del Disconoscimento.

D.4. - Data valuta

La Banca, nel disporre il rimborso, riporta il conto di pagamento addebitato nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo, nonché il rimborso di eventuali interessi, spese e/o commissioni addebitate con riferimento a tale operatività.

E. Processo di gestione dei Disconoscimenti di operazioni di pagamento non autorizzate disposte su iniziativa del beneficiario o per il suo tramite, SDD Core e SDD B2B

Con riferimento alla casistica in oggetto si rimanda, fermo quanto puntualmente specificato nei paragrafi che seguono, a quanto descritto nel paragrafo A.2. che precede della Presente Policy.

E.1. - Verifica dei presupposti e gestione

Ricevuta la richiesta da parte del cliente di Disconoscimento di SDD Core e SDD B2B non autorizzati, la Banca verifica preliminarmente che la comunicazione di Disconoscimento di singoli addebiti non autorizzati sia stata ricevuta entro i seguenti termini.

- operazioni di pagamento su iniziativa del beneficiario o per il suo tramite: entro 13 (tredici) mesi dalla data di addebito dei fondi sul conto del cliente, fermo quanto previsto dal paragrafo C che precede della presente Policy;
- SDD Core: oltre le 8 (otto) settimane dalla data di addebito dei fondi ed entro 13 (tredici) mesi dalla data di addebito sul conto del cliente;
- SDD B2B: entro 13 (tredici) mesi dalla data di addebito dei fondi sul conto del cliente.

Il Disconoscimento di un singolo addebito non è da intendersi come Disconoscimento di tutti gli addebiti effettuati in forza del mandato autorizzativo, salvo diversa esplicita volontà del cliente. In quest'ultima ipotesi, la Banca considera i soli addebiti effettuati in forza del mandato autorizzativo nei 13 (tredici) mesi precedenti alla data dell'ultimo addebito.

La Banca esegue tutte le analisi e conseguenti attività già puntualmente descritte nel paragrafo A.2. che precede della presente Policy, tenuto conto delle caratteristiche delle operazioni di pagamenti di cui al presente paragrafo.

In particolare, con specifico riferimento a SDD Core e SDD B2B, la Banca:

- nella stessa giornata operativa in cui riceve la richiesta di Disconoscimento dal cliente, effettua la richiesta della copia del mandato alla banca del creditore attraverso i messaggi interbancari, in cui sono indicate tutte le informazioni utili alla controparte e anche l'indirizzo PEC al fine di facilitare la comunicazione;
- entro la fine della giornata operativa successiva a quella in cui ha preso atto dell'operazione o ha ricevuto la comunicazione di Disconoscimento da parte del cliente, effettua il rimborso nel caso in cui non riceva copia del mandato dalla banca del creditore.

F. Processo di gestione dei Disconoscimenti di operazioni di pagamento eseguite mediante carte di pagamento emesse e gestite da soggetti terzi rispetto alla Banca e da questa solo collocate

Con specifico riferimento ai Disconoscimenti di addebiti derivanti da operazioni di pagamento eseguite tramite strumenti di pagamento (carte di credito / debito /prepagate) emesse e gestite da soggetti terzi rispetto alla Banca e da quest'ultima solo collocate sarà l'emittente lo strumento di pagamento a gestire tali richieste avanzate dalla clientela alla Banca, nel contesto del più generale affidamento di attività e servizi, anche di verifica, finalizzati a garantire la funzionalità dello strumento di pagamento, anche al fine di garantire una tempestiva analisi della richiesta di Disconoscimento e riscontro al cliente.

Di seguito, dunque, si riporta una descrizione del processo adottato dall'emittente lo strumento di pagamento (previamente condiviso con la Banca) per le richieste di Disconoscimento trasmesse dalla clientela della Banca:

- la pratica di Disconoscimento è tempestivamente aperta nel momento in cui il cliente contatta l'emittente lo strumento di pagamento per disconoscere un'operazione e non è subordinata alla richiesta al cliente di documenti/informazioni aggiuntive, proprio come

previsto per i casi di richieste di Disconoscimenti ricevuti direttamente dalla Banca. L'emittente lo strumento di pagamento dispone di un canale di contatto per consentire al cliente l'immediata apertura del Disconoscimento ed il blocco della carta, attivo sette giorni su sette e per 365 giorni all'anno;

- l'emittente lo strumento di pagamento, entro e non oltre la fine della giornata operativa successiva a quella in cui ha preso atto dell'operazione o ha ricevuto la comunicazione di Disconoscimento da parte del cliente, esegue il rimborso definitivo in tutti i casi in cui le operazioni siano state disposte in assenza di SCA;
- per le operazioni di pagamento che risultano autenticate con SCA, affinché l'istruttoria assicuri una adeguata valutazione del comportamento del cliente (dolo/colpa grave), l'emittente lo strumento di pagamento: i) garantisce il rimborso salvo buon fine entro e non oltre la fine della giornata operativa successiva a quella in cui ha preso atto dell'operazione o ha ricevuto la comunicazione di Disconoscimento da parte del cliente; ii) richiede al cliente, ove necessaria ai fini dell'istruttoria e delle valutazioni, documentazione addizionale; iii) sulla base delle valutazioni svolte in fase di istruttoria e sulla scorta di criteri interni definiti a priori valuta la pratica e, se dimostrato il dolo o la colpa grave del cliente, procede nell'esercitare il proprio diritto di chiedere al cliente ed ottenere dal cliente la restituzione della somma inizialmente rimborsata, comunicando al cliente (per iscritto e secondo le modalità con questi concordate nel contratto) i motivi dell'addebito e la possibilità di far valere (in ogni caso) i propri diritti nelle sedi competenti ritenute più opportune. Diversamente l'emittente conferma il rimborso al cliente.

Nell'eventualità in cui il cliente contatti la Banca per una richiesta di Disconoscimento relativa ad un'operazione di pagamento effettuata mediante carte di pagamento emesse da un soggetto terzo rispetto alla Banca, la Banca mette prontamente in contatto il cliente direttamente con il servizio competente dell'emittente preposto alla gestione e trattazione di tali richieste, indicandogli i contatti tempo per tempo condivisi dall'emittente stesso.

L'emittente dello strumento di pagamento sarà tenuto a trasmettere alla Banca, secondo una periodicità pattuita, le richieste di Disconoscimento che ha ritenuto di non accogliere, anche solo parzialmente, e per cui non ha provveduto al rimborso, ove le stesse presentino degli elementi di peculiarità ovvero criticità predefinite dalla Banca.

In tali casi, la Banca provvede ad analizzare la decisione, effettuando - se del caso - approfondimenti secondo quanto previsto nella presente Procedura e comunicando tempestivamente al cliente tale ulteriore attività.

Ad esito dell'analisi la Banca procede, ove ne ravvisi gli estremi anche previo confronto con altre strutture competenti per profili legali, di sicurezza e di conformità, tempestivamente al rimborso, in considerazione delle necessità operative sottese, in coerenza con quanto previsto dai paragrafi precedenti della presente Procedura.

8. La sospensione del rimborso e la gestione delle segnalazioni a Banca d'Italia

La Banca ha l'obbligo di rimborsare immediatamente all'utente l'importo dell'operazione non autorizzata secondo le modalità dettagliate nella presente Policy.

Tuttavia, resta ferma la possibilità di dimostrare, anche in un momento successivo al rimborso, che l'operazione di pagamento era stata autorizzata. In tal caso, la normativa prevede che la Banca ha il diritto di chiedere al cliente ed il diritto di ottenere dall'utente la restituzione dell'importo inizialmente rimborsato secondo le regole previste nella presente Policy.

Un'eccezione all'obbligo di rimborso opera nel caso in cui l'Ufficio IT abbia il motivato sospetto che l'operazione non autorizzata derivi da un comportamento fraudolento posto in essere dall'utente stesso. In proposito, la Banca ritiene che il comportamento fraudolento si caratterizzi per elementi specifici che denotano l'intenzione dell'utente di raggirare la Banca e pertanto, che lo stesso non possa consistere nella mera inosservanza dolosa o colposa degli obblighi di comunicazione e di custodia gravanti sull'utente medesimo.

Nel caso in cui l'Ufficio IT sospenda il rimborso, deve darne immediata comunicazione per iscritto alla Banca d'Italia ⁽²⁾ per il tramite dell'Ufficio Contabilità.

Al fine di promuovere la trasmissione delle segnalazioni secondo modalità standardizzate che ne facilitino sia l'invio da parte della Banca, sia la raccolta e gestione da parte della Banca d'Italia, quest'ultima invita ad effettuare la comunicazione attraverso uno specifico template ⁽³⁾, che deve essere inviato dalla Banca all'indirizzo vic@pec.bancaditalia.it, indicando nell'oggetto le seguenti informazioni: codice ABI, mese/anno di riferimento della notifica dell'operazione non autorizzata e la dicitura “*segnalazione ai sensi dell'art. 11, co. 2, d.lgs. n. 11/10*”. Tale comunicazione deve essere eseguita immediatamente e comunque entro e non oltre la fine della giornata operativa successiva a quella in cui ha preso atto dell'operazione o ha ricevuto la comunicazione di Disconoscimento da parte del cliente. Inoltre, l'Ufficio *Contabilità* deve comunicare, con cadenza mensile (il giorno 10 (dieci) di ciascun mese, con riferimento al mese precedente) e solo in caso di segnalazione positiva, ogni rimborso sospeso e indicare i motivi del sospetto di frode, la tipologia dell'utente (persona fisica/consumatore; persona fisica/non consumatore; etc.) e le caratteristiche delle operazioni di pagamento disconosciute (data e importo dell'operazione), senza fornire dati o informazioni del cliente aventi carattere personale (ad es. il nome).

Infine si precisa che l'Ufficio IT renderà trimestralmente all'Ufficio Risk Management e alla Funzione Compliance l'elenco delle richieste di disconoscimento pervenute, le caratteristiche (data, strumento di pagamento utilizzato, importo ecc....) e il loro esito.

2) Al riguardo, la Banca d'Italia ha pubblicato una specifica comunicazione con cui sono state fornite precisazioni sui presupposti della sospensione del rimborso delle operazioni non autorizzate da parte dei PSP e sulle modalità con cui comunicare tale sospensione, rendendo disponibile un template che tutti i PSP operanti sul territorio della Repubblica Italiana e destinatari dell'obbligo segnaletico possono utilizzare per attivare il flusso segnaletico (<https://www.bancaditalia.it/compiti/tutela-educazione/avvisi-comunicazioni/2023.10.30/index.html>).

3) <https://www.bancaditalia.it/compiti/tutela-educazione/avvisi-comunicazioni/2023.10.30/index.html?dotcache=refresh>

8. GIURISPRUDENZA ABF RILEVANTE

Al fine di recepire le indicazioni formulate dalla giurisprudenza e dall'Arbitro Bancario Finanziario sul tema è stata predisposta una griglia granulare (all.1) che supporta le funzioni coinvolte nella gestione dei Disconoscimenti (e dei reclami) nella valutazione dell'eventuale dolo o colpa grave del cliente, considerando anche le casistiche già gestite dalla Banca e coerenti con l'attività da questa svolta ⁽⁴⁾.

9. APPROVAZIONE, MODIFICHE E AGGIORNAMENTI

La presente Policy è stata approvata dal Consiglio di Amministrazione della Banca *Popolare del Frusinate* nella seduta del XX/XX/XX25.

Con il medesimo *iter* sono approvate eventuali modifiche e/o integrazioni sostanziali al documento. La presente Policy viene aggiornata periodicamente dalla Funzione Organizzazione ogni qualvolta si verifichi un cambiamento rilevante della normativa.

4) La valutazione circa la sussistenza di una colpa grave dell'utente deve essere infatti condotta tenendo in considerazione una pluralità di elementi, tra cui la specifica realtà fattuale, le caratteristiche di sicurezza dello strumento di pagamento utilizzato, l'esistenza di eventuali sistemi di allerting per il cliente tempo per tempo previsti, le caratteristiche soggettive ed il comportamento tenuto dall'utente stesso, il grado di riconoscibilità delle ipotesi specifiche di frode e di indebito utilizzo, la tempestività con cui il cliente ha comunicato quanto occorso alla Banca. Nella predisposizione e aggiornamento delle griglie devono essere valorizzate le plurime variabili di carattere oggettivo fattuale e soggettivo comportamentale, al fine di individuare le situazioni sintomatiche dalle quali può emergere – sempre in funzione del caso concreto – una violazione con colpa grave da parte del cliente degli obblighi previsti dalla normativa in capo allo stesso (e.g. obbligo di diligente custodia dello strumento di pagamento ovvero dei dispositivi personalizzati o dei codici di sicurezza, di tempestiva comunicazione in caso di smarrimento, furto, appropriazione indebita o uso non autorizzato).