



Banca Popolare Pugliese

MODULO “OPERAZIONI DI PAGAMENTO OGGETTO DI DISCONOSCIMENTO”

Il seguente Modulo è utilizzabile dai Clienti per comunicare alla Banca il disconoscimento di operazioni di pagamento intervenute sui propri Conti di Pagamento.

Seguire queste istruzioni:

1. *Compilare in ogni parte la sezione introduttiva con i Suoi dati identificativi e con i riferimenti del rapporto su cui sono state addebitate le operazioni oggetto del disconoscimento;*
2. *Compilare in ogni parte la sezione “OPERAZIONI DI PAGAMENTO OGGETTO DI DISCONOSCIMENTO”, avendo cura di riportare tutti i dati rilevanti sulle operazioni di pagamento segnalate;*
3. *Compilare la sezione “RIEPILOGO DEGLI EVENTI INTERCORSI”, avendo cura di esporre in modo chiaro e completo tutti gli elementi utili sui fatti intervenuti;*
4. *Procedere ad apporre la propria “Firma” (analogica o digitale) nell’apposito spazio in calce al modulo;*
5. *Allegare al Modulo copia della denuncia presso le autorità competenti, laddove già sporta, nonché tutta la documentazione disponibile in Suo possesso relativa all’operazione di pagamento non autorizzata (ad es., e-mail o SMS ricevuti, schermate dei siti visitati, ecc.);*
6. *Trasmettere questo Modulo insieme alla documentazione richiesta tramite le seguenti modalità:*
 - *inviare mail al seguente indirizzo: presidio.incidenti.sicurezza@bpp.it oppure presidio.incidenti.sicurezza@pec.bpp.it avendo cura di utilizzare per l’invio lo stesso indirizzo di posta elettronica riportato nella sezione introduttiva del Modulo con i Suoi dati identificativi,*
oppure
 - *consegnare a mano la documentazione complessiva presso la Filiale di radicamento del conto corrente/di pagamento che avrà cura di inoltrarla al suddetto indirizzo mail.*
7. *Se le operazioni disconosciute riguardano diversi conti di pagamento dovrà essere compilato un modulo per ogni conto di addebito,*

Alla ricezione della documentazione, si verificherà il contenuto e gli eventuali allegati consegnati e si procederà alla valutazione della Sua richiesta.



MODULO DISCONOSCIMENTO OPERAZIONI DI PAGAMENTO

Spett.
Banca Popolare Pugliese

_____, li ____/____/____

Io sottoscritto¹ _____ nato a _____

(_____) il ____/____/____ residente in _____ (____)

telefono _____ mail/PEC _____

[*inserire solo nel caso di contestazioni relative a conti intestati a enti/persone giuridiche*] in qualità di
legale rappresentante di _____

con sede in _____ partita IVA/CF _____

COMUNICA

il disconoscimento delle operazioni di pagamento sottoindicate, addebitate sul rapporto di Conto di
Pagamento n. _____ intestato a _____

presso la Filiale di _____

¹ I dati personali conferiti attraverso la compilazione del presente modulo saranno trattati in conformità a quanto previsto nell' "informativa ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679" rilasciata in sede di apertura del rapporto inerente al servizio di pagamento e/o in occasione del conferimento di un ordine di pagamento. L'informativa è altresì pubblicata, con gli eventuali dovuti aggiornamenti, sul sito istituzionale della Banca (www.bpp.it) all'interno della sezione dedicata alla privacy

**OPERAZIONI DI PAGAMENTO OGGETTO DI DISCONOSCIMENTO***(compilazione obbligatoria)*

DATA OPERAZIONE	IMPORTO <i>(espresso in Euro)</i>	DESCRIZIONE <i>Per es.: beneficiario, canale di esecuzione dell'operazione, estremi dello strumento di pagamento utilizzato (es.: numero carta, codice utenza Internet utilizzato)</i>	TIPO OPERAZIONE <i>Inserire alternativamente una delle seguenti voci: "Bonifico", "Operazioni con carta", "Addebito SDD", ecc.</i>

Le operazioni di pagamento disconosciute sono state effettuate:*(possono essere valorizzate anche più opzioni, se necessario)*

- tramite canale on line - rapporto di Internet/Home Banking a me intestato/intestato a _____
- tramite Terze Parti-Prestatori di servizi di disposizione di ordini di pagamento "PISP" su canale on line - rapporto di Internet/Home Banking n. _____ a me intestato/intestato a _____
[se conosciuto, indicare la denominazione/sito della Terza Parte: _____]
- tramite ATM
- tramite mandato di pagamento (SDD)

In relazione a quanto sopra,

DICHIARA*(valorizzare anche più di un'opzione, se necessario)*

- non ho eseguito le disposizioni di pagamento, né ho fornito a terzi (consapevolmente o meno) i codici/credenziali per effettuarla
- ho eseguito le disposizioni di pagamento, seguendo istruzioni ricevute telefonicamente o via chat da soggetti che ritenevo affidabili;

**Ulteriori informazioni a corredo della richiesta di rimborso che possono essere utili nella istruttoria dell'evento.**

DOMANDA PER IL CLIENTE – Sezione Internet Banking		RISPOSTA	
1	<ul style="list-style-type: none">Ha provveduto al blocco dello strumento di pagamento (Internet Banking)? <p><i>In caso di risposta negativa, a ricezione del presente modulo, la Banca provvederà d'ufficio al blocco</i></p>	SI <input type="checkbox"/>	NO <input type="checkbox"/>
		In data / /	
2	Ha sempre custodito le credenziali (Codice utente, Password, PIN, OTP) in modo da garantirne l'assoluta segretezza, senza mai comunicarle a soggetti terzi?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
3	<p>Ha ricevuto richieste urgenti (telefoniche, via SMS o email) di fornire codici, autorizzare pagamenti per "stornare" operazioni sospette o per mettere in sicurezza il conto?</p> <ul style="list-style-type: none">Solo se ha risposto "SI" alla domanda precedente: ha fornito tali codici o autorizzato le operazioni mentre era in linea con il presunto operatore? [] SI [] NO <p>Fornisca i dettagli sul mezzo di contatto: Mezzo di contatto: [] Chiamata Vocale [] SMS [] Email [] Chat (WhatsApp, ecc.)</p> <p>Numero/Mittente/Indirizzo visualizzato: _____</p> <p>Nome del suo Operatore Telefonico: _____</p> <p>Verifica attendibilità (per SMS): Il messaggio ricevuto appariva nella stessa coda (chat) dei messaggi autentici inviati in precedenza dalla Banca? [] SI, era nella chat abituale della Banca [] NO, era un nuovo messaggio/mittente</p>	SI <input type="checkbox"/>	NO <input type="checkbox"/>
4	Ha subito furti/smarrimenti di documenti, portafogli o dispositivi (smartphone/PC)? contenenti le credenziali di sicurezza dello strumento di pagamento?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
5	Ha ricevuto, tramite contatto via sms/telefono/e-mail, richieste di reset password/codici di attivazione App che non ha generato lei personalmente e ha confermato tali operazioni su richiesta di un terzo soggetto?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
6	<p>Ha ricevuto messaggi SMS e/o e-mail in cui Le venivano richieste attività (tramite, ad esempio, download di allegati e/o richieste di cliccare link) quali ad esempio:</p> <ul style="list-style-type: none">aggiornamento/conferma dei dati personali,verifica/aggiornamento o riattivazione del Suo account, <p>Solo se ha risposto "SI" alla domanda precedente: il messaggio o l'email ricevuta presentava errori ortografici o rimandava a un link (sito web) che non sembrava quello ufficiale della Banca?</p> <p>_____</p> <p>_____</p> <p>Allegare videata</p>	SI <input type="checkbox"/>	NO <input type="checkbox"/>
7	Ha ricevuto contatti telefonici da soggetti che si sono presentati come operatori della Banca (es. Ufficio Antifrode, Sicurezza, Assistenza Tecnica) o di altre Autorità?	SI <input type="checkbox"/>	NO <input type="checkbox"/>



	<p>Solo se ha risposto "SI" alla domanda precedente: compilare i seguenti dettagli fondamentali per l'istruttoria:</p> <p>Numero chiamante visualizzato: _____</p> <p>Durante la chiamata, Le è stato chiesto di:</p> <p>[] Fornire/leggere a voce codici OTP ricevuti via SMS o tramite App?</p> <p>[] Comunicare le credenziali di accesso (User ID / Password / PIN)?</p> <p>[] Autorizzare operazioni tramite Notifica Push sul cellulare per "annullare" o "stornare" pagamenti sospetti?</p> <p>[] Effettuare Lei stesso dei bonifici/ricariche su altri conti per "mettere in sicurezza" i fondi? (<i>Indice di operazione sotto dettatura</i>)</p> <p>Il numero chiamante appariva identico a quello ufficiale della Banca o della carta?</p> <p>o [] SI [] NO [] NON RICORDO</p>		
8	Ha ricevuto richieste da parte di fornitori, creditori o aziende di servizi (tramite e-mail, lettera, messaggio SMS o chiamata telefonica) di modificare le coordinate IBAN verso le quali effettuare pagamenti?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
9	Ha inserito su dispositivi o piattaforme informatiche riferibili ad intermediari finanziari (banche, gestori di carte o fornitori di servizi di pagamento) i suoi dati personali, le sue coordinate IBAN o i dati delle sue carte di pagamento?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
10	Ha avuto contatti da persone che Le hanno formulato richieste di prestiti di denaro, pagamenti urgenti, richieste di aiuto economico per vari motivi?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
11	Ha ricevuto richieste da sedicenti operatori /tecnici informatici di customer care di aziende apparentemente di Sua fiducia di installare programmi/software o app sul suo dispositivo (PC e/o cellulare)?	SI <input type="checkbox"/>	NO <input type="checkbox"/>

DOMANDA PER IL CLIENTE – Sezione Carte di Debito/Credito		RISPOSTA	
1	<p>Ha provveduto al blocco dello strumento di pagamento (carta di pagamento)?</p> <p><i>In caso di risposta positiva indicare la data del blocco</i></p> <p><i>In caso di risposta negativa, a ricezione del presente modulo, la Banca provvederà d'ufficio ad apporre il relativo blocco</i></p>	SI <input type="checkbox"/>	NO <input type="checkbox"/>
		In data / /	
2	Ha subito il furto/smarrimento/clonazione della carta di pagamento?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
3	Ha smarrito il codice personale segreto (PIN) della Sua carta di pagamento?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
4	Ha ceduto, anche solo temporaneamente, la carta di pagamento a terzi?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
5	Ha comunicato a qualcuno il codice personale segreto (PIN) della sua carta di pagamento?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
6	Ha conservato il PIN della sua carta di pagamento in un luogo non accessibile a terzi?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
7	Ha subito furti/smarrimenti che hanno coinvolto documenti o supporti contenenti il PIN della carta di pagamento?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
8	Ha utilizzato la carta di pagamento negli ultimi 3 giorni?	SI <input type="checkbox"/>	NO <input type="checkbox"/>
9	<p>Utilizza la carta per acquisti su siti di e-commerce, piattaforme di Gaming/Scommesse online, o la ha associata a portafogli digitali (es. Apple Pay, PayPal) e servizi di abbonamento (es. Netflix, Amazon Prime)?</p> <p>Solo se ha risposto "SI" alla domanda precedente:</p> <ul style="list-style-type: none"> indichi i principali siti o servizi di abbonamento presso i quali la carta è stata utilizzata/registrata: _____ Le operazioni sono state effettuate mentre era connesso: _____ 		



<input type="checkbox"/> alla Sua rete abituale (Casa/Ufficio)		
<input type="checkbox"/> a una rete Wi-Fi pubblica		<input type="checkbox"/>

CHIEDE

il rimborso dell'importo delle operazioni oggetto di disconoscimento elencate con riaccredito sul rapporto sopra indicato.

PRENDE ATTO CHE:

- a) Entro la giornata lavorativa successiva al ricevimento della segnalazione di disconoscimento (la segnalazione si intende ricevuta il giorno successivo se pervenuta dopo la chiusura degli uffici della Banca come comunicati alla Clientela), la Banca procederà ad eseguire il riaccredito dell'importo non autorizzato, applicando la stessa data valuta dell'addebito eseguito sul rapporto, nel caso in cui:
- l'operazione non sia stata autorizzata tramite autenticazione forte (SCA);
 - l'operazione abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti connessi al servizio di disposizione di ordine di pagamento prestato;
 - se il disconoscimento è relativo ad operazioni eseguite dopo la comunicazione del cliente dello smarrimento/furto dello strumento di pagamento.
- Qualora l'operazione disconosciuta sia stata eseguita con carte di Pagamento NEXI, l'eventuale riaccredito entro la giornata lavorativa successiva alla segnalazione e l'eventuale successivo riaddebito del conto del Cliente, saranno effettuati dalla Banca previa autorizzazione di NEXI;
- b) In tutti i casi in cui l'operazione di pagamento è stata autenticata con SCA e in assenza di elementi relativi alla colpa e negligenza del cliente, la Banca entro la giornata successiva, risconterà il cliente, comunicando il ri-accredito della somma disconosciuta. Si evidenzia la possibilità di riaddebito dell'importo rimborsato. Il cliente è quindi invitato a mantenere la disponibilità dei fondi sul conto di pagamento fino al termine del procedimento di verifica, e comunque entro 120 giorni dalla ricezione della richiesta di disconoscimento. Trascorso tale termine senza riaddebito, il rimborso sarà considerato definitivo. La Banca conserva, in ogni caso, il diritto di intraprendere le ordinarie iniziative per il recupero delle somme rimborsate;
- c) La Banca rifiuta il rimborso qualora dall'istruttoria si evinca che l'operazione disconosciuta è stata causata dal mancato rispetto degli obblighi posti a carico dell'utente stesso (per esempio, la custodia dello strumento di pagamento) in ragione di suoi comportamenti caratterizzati da dolo o colpa grave. Stesso dicasi nelle ipotesi in cui, sebbene il cliente non fornisca prove concrete sulle circostanze di fatto della frode che afferma di aver patito, la Banca accerti che l'operazione di pagamento è stata autenticata con SCA senza disservizi nelle misure di sicurezza e nel sistema di alerting verso il Cliente e non siano stati rilevati indicatori di anomalia;
- d) Qualora sussista il motivato sospetto che l'operazione non autorizzata derivi da un comportamento fraudolento posto in essere dall'utente dei servizi di pagamento, la Banca sospende il rimborso delle somme al Cliente; la Banca, laddove disponga di elementi idonei a provare il comportamento fraudolento, doloso o gravemente colposo del cliente, può respingere il rimborso senza la sospensione.

DICHIARA

- di aver presentato formale denuncia in data / / in relazione agli eventi sopra descritti all'Autorità competente. A tal fine allego copia della denuncia presentata all'Autorità competente di _____
- di non aver potuto ancora presentare formale denuncia all'Autorità competente in relazione a quanto sopra descritto.



La denuncia alle Autorità competenti può assumere rilevanza nella conduzione delle valutazioni istruttorie sulle operazioni non autorizzate, in quanto contenente ulteriori dettagli informativi utili per contestualizzare i fatti su cui si basano le richieste di rimborso avanzate sulle operazioni oggetto di disconoscimento.

Qualora non sia stata presentata denuncia alle Autorità competenti, si raccomanda di procedere alla prima occasione utile, attesa l'importante rilevanza probatoria che tale documentazione assolve nell'interesse del Cliente nelle decisioni sul tema delle operazioni di pagamento non autorizzate presso le sedi giudiziali e stragiudiziali.

DICHIARA INFINE

- di aver fornito con il presente Modulo dati ed informazioni della cui esattezza, completezza e veridicità mi assumo la piena responsabilità;
- di essere a conoscenza delle conseguenze derivanti dalla eventuale falsità di tutti o di alcuni di tali dati ed informazioni e delle connesse responsabilità a mio carico;
- di tenere sollevata la Banca da ogni responsabilità che possa derivarle dalle iniziative intraprese in conseguenza di eventuali false affermazioni da me effettuate nella presente dichiarazione.

AUTORIZZA

la Banca Popolare Pugliese a utilizzare i recapiti indicati nel presente modulo per ricevere comunicazioni sullo stato della richiesta;

la Banca Popolare Pugliese, qualora dalle verifiche effettuate risulti che l'operazione sia stata regolarmente autorizzata, ad addebitare sul rapporto indicato le somme precedentemente rimborsate.

Documentazione allegata:

- copia (fronte/retro) del documento di identità e del codice fiscale [obbligatoria]
- eventuale copia della denuncia presentata all'Autorità competente
- revoca del mandato all'addebito inviata al creditore/Banca
- copia delle e-mail ricevute (riferite ai fatti descritti)
- copia degli SMS ricevuti (riferite ai fatti descritti)
- copia delle schermate dei siti web visitati (riferite ai fatti descritti)
- copia delle ricevute o degli scontrini (riferite ai fatti descritti)
- screenshot delle telefonate ricevute o delle chat scambiate (riferite ai fatti descritti)
- documenti relativi all'operazione (riferite ai fatti descritti)
- altro [*indicare ulteriore documentazione allegata*]: _

Luogo _____, lì ____/____/____

Firma _____