

MODULO DI DISCONOSCIMENTO OPERAZIONI DI PAGAMENTO TRAMITE BONIFICO BANCARIO NON AUTORIZZATE E ISTANZA DI RIMBORSO

Per consentire a Banca Popolare di Sondrio (di seguito "Banca") di gestire la pratica, il presente Modulo deve essere compilato in ogni sua parte, sottoscritto e corredato della documentazione richiesta, **Data di presentazione:** ____/____/____

Filiale di riferimento (se presentazione in filiale): _____

SEZIONE 1: DATI DEL RICHIEDENTE (Titolare del rapporto)

Nome: _____ Cognome: _____

Luogo di nascita: _____ Data di nascita: ____/____/____

Codice Fiscale: _____

Indirizzo di residenza: _____

N. Civico: _____ CAP: _____ Comune: _____

Telefono/ Cellulare: _____ E-mail/ PEC: _____

Estremi Documento Identità:

Tipo _____ Numero _____ Data Scadenza _____

SEZIONE 2: RIFERIMENTI DEL CONTO/STRUMENTO DI PAGAMENTO

IBAN Conto Corrente di addebito/riaccredito: _____

Numero Carta (se il disconoscimento riguarda operazioni su carta): _____

Altro strumento (specificare): _____

SEZIONE 3: INFORMAZIONI GENERALI SULL'EVENTO

1. Data in cui si è accorto/a per la prima volta delle operazioni disconosciute: ____/____/____

2. Come si è accorto/a delle operazioni disconosciute?

☐ Controllo estratto conto/lista movimenti online

☐ Notifica SMS/ E-mail/ Push da parte della Banca

☐ Comunicazione da parte di terzi (specificare: _____)

☐ Altro (specificare: _____)

3. Ha presentato/intende presentare denuncia alle Autorità competenti?

☐ SI, in data ____/____/____ presso _____ (allegare copia) Prot. N. _____

☐ NO, ma mi impegno a presentarla entro 7 giorni e a fornirne copia alla Banca.

☐ NO (specificare il motivo, se diverso da quelli sopra): _____)

4. Descrizione delle circostanze dell'evento (come ritiene sia avvenuto l'evento):

SEZIONE 4: DETTAGLIO DELLE OPERAZIONI OGGETTO DI DISCONOSCIMENTO

(Compilare una riga per ogni operazione disconosciuta)

N.	Data Operazione	Data Valuta/ Contabile	Beneficiario/Descrizione Operazione	Importo (€)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Importo Totale Disconosciuto: _____ €

SEZIONE 5: SPECIFICHE DELL'OPERAZIONE

5.B - BONIFICI (Da compilare se almeno una delle operazioni disconosciute è un bonifico)

Domanda	Risposta	Dettagli/Note (se necessario)
1. Ha disposto Lei l'operazione, pur essendo stato/a indotto/a su richiesta di terzi (es. su beneficiario/causale)?	SI ☐ NO ☐	
2. Ha ricevuto e inserito i codici autorizzativi (es. OTP, conferma via app) per questo/i bonifico/i?	SI ☐ NO ☐	
3. Prima di queste operazioni, ha ricevuto e-mail, SMS, telefonate o altri messaggi che Le chiedevano di fornire dati personali/bancari, o di cliccare link, o di installare software?	SI ☐ NO ☐	
4. Se SI al punto precedente ha seguito le istruzioni?	SI ☐ NO ☐	
5. Ha effettuato l'accesso al Suo servizio di Internet/Mobile Banking da un dispositivo che utilizza abitualmente e che ritiene sicuro?	SI ☐ NO ☐	

6. Ha notato anomalie durante l'accesso o l'utilizzo del servizio di Internet/Mobile Banking (es. lentezza, pagine anomale, richieste di codici insolite)?	SI ☐ NO ☐	
--	---	--

SEZIONE 6: CONTESTO OPERAZIONI DISCONOSCIUTE

Domanda	Risposta	Dettagli/Note (se necessario)
1. I Suoi codici personali (PIN, password Internet/Mobile Banking, codici OTP) erano conservati su supporti cartacei o digitali (es. post-it, file non protetti, rubrica telefono) o comunicati a terzi, inclusi familiari, conviventi o conoscenti?	SI ☐ NO ☐	
2. Le password utilizzate per i servizi bancari sono complesse, cioè formate secondo i canoni di sicurezza (es: contenenti lettere maiuscole/minuscole, numeri, simboli)?	SI ☐ NO ☐	
3. Le password utilizzate per i servizi bancari sono utilizzate anche per altri servizi online (es: e-mail, social network, shopping online)?	SI ☐ NO ☐	
4. Accede ai servizi bancari online e autorizza pagamenti prevalentemente da dispositivi (PC, smartphone, tablet) di Suo uso esclusivo e protetti da password, PIN o sistemi biometrici?	SI ☐ NO ☐	
5. Ha mai utilizzato le Sue credenziali di accesso ai servizi bancari (es. User ID, password) o effettuato operazioni da computer o reti Wi-Fi pubbliche (es. internet point, hotel, aeroporti, bar)?	SI ☐ NO ☐	
6. Mantiene regolarmente aggiornati il sistema operativo, il browser e le applicazioni (inclusa l'app della Banca) sui dispositivi che utilizza per le operazioni bancarie?	SI ☐ NO ☐	
7. Utilizza un software antivirus/antimalware affidabile e aggiornato sui dispositivi da cui effettua operazioni bancarie (in particolare PC)?	SI ☐ NO ☐	
8. Sui dispositivi che utilizza per operazioni bancarie, sono attivi sistemi di blocco automatico dello schermo dopo un breve periodo di inattività?	SI ☐ NO ☐	
9. Negli ultimi mesi, prima delle operazioni contestate, ha cliccato su link o aperto allegati contenuti in e-mail, SMS o messaggi di social media/messaggistica istantanea di dubbia provenienza o dal contenuto sospetto/allarmistico?	SI ☐ NO ☐	

10. Negli ultimi mesi, prima delle operazioni contestate, ha installato sui Suoi dispositivi software o applicazioni provenienti da store non ufficiali o da fonti non verificate?	SI ☐ NO ☐	
11. Negli ultimi mesi, prima delle operazioni contestate, ha ricevuto chiamate telefoniche, e-mail, SMS o altri messaggi, anche tramite applicazioni solitamente in uso che, presentandosi come incaricati della Banca o di altre entità (es. Poste, Agenzia Entrate, corrieri), Le richiedevano di fornire dati personali, codici di accesso, dati di carte, o di compiere determinate azioni (es. cliccare link, effettuare pagamenti di prova, installare software di assistenza remota)?	SI ☐ NO ☐	
12. Se SI alla domanda precedente, tali comunicazioni sospette Le prospettavano conseguenze negative immediate (es. blocco del conto, multe, perdita di denaro) qualora non avesse agito tempestivamente secondo le istruzioni ricevute?	SI ☐ NO ☐	
13. Se SI alla domanda 11, ha fornito i dati richiesti, seguito le istruzioni o cliccato sui link proposti senza prima verificare l'autenticità della richiesta attraverso i canali di contatto ufficiali e noti della Banca o dell'entità in questione (es. contattando il Suo gestore o il numero verde ufficiale della Banca o quello dei presunti richiedenti)?	SI ☐ NO ☐	
14. Se le operazioni contestate sono bonifici verso nuovi beneficiari o acquisti online da nuovi venditori, ha adottato cautele per verificarne l'identità e l'affidabilità (es. ricerca recensioni, verifica partita IVA, controllo dati di contatto) prima di procedere?	SI ☐ NO ☐	
15. Ha attivato i servizi di notifica (SMS alert, notifiche push dell'app) offerti dalla Banca per essere informato in tempo reale sulle operazioni disposte con i Suoi strumenti di pagamento?	SI ☐ NO ☐	
16. Controlla regolarmente (almeno settimanalmente o più frequentemente in base alla Sua operatività) e con attenzione gli estratti conto e le liste movimenti del Suo conto corrente e delle Sue carte, anche tramite i canali online della Banca?	SI ☐ NO ☐	
17. Ha segnalato alla Banca le operazioni contestate non appena ne è venuto/a a conoscenza o comunque senza ingiustificato ritardo?	SI ☐ NO ☐	
18. Qualora le operazioni contestate riguardassero una carta di pagamento e siano state effettuate su un terminale POS fisico o uno sportello ATM, ricorda se questi Le sono sembrati manomessi, presentavano	SI ☐ NO ☐	

anomalie o se l'esercente/altra persona ha compiuto manovre insolite con la Sua carta?		
19. Ha mai consentito a terzi (anche se persone di fiducia) di utilizzare i Suoi strumenti di pagamento o dispositivi personali mentre erano attive sessioni di home banking, memorizzate password bancarie o quando l'accesso all'app bancaria era possibile senza una nuova autenticazione? Altresi, ha eventualmente fornito le credenziali a terzi?	SI ☐ NO ☐	

SEZIONE 7: DICHIARAZIONI DEL CLIENTE

Il/La sottoscritto/a, consapevole delle responsabilità civili e penali previste dalla legge in caso di dichiarazioni mendaci (art. 76 D.P.R. 445/2000 e ss.mm.ii):

- DICHIARA che tutte le informazioni fornite nel presente modulo sono complete e veritiere.
- DICHIARA di non aver autorizzato, né direttamente né indirettamente, le operazioni sopra indicate e dettagliate, e di non averne beneficiato in alcun modo.
- SI IMPEGNA a comunicare tempestivamente alla Banca ogni eventuale ulteriore informazione utile ai fini dell'istruttoria o al recupero delle somme.
- SI IMPEGNA a fornire alla Banca, qualora non già allegata, copia della denuncia/querela sporta presso le competenti Autorità Giudiziarie o di Pubblica Sicurezza entro 7 (sette) giorni dalla presentazione del presente modulo, qualora tale documento sia necessario per la gestione della pratica.
- PRENDE ATTO che la Banca si riserva di effettuare ogni verifica ritenuta opportuna e che, in caso di accertamento di dichiarazioni non veritiere o mendaci o di comportamenti del Cliente che configurino dolo o colpa grave ai sensi della normativa vigente, la Banca potrà respingere l'istanza di rimborso o, se già effettuato, potrà procedere al riaddebito delle somme, oltre a tutelare i propri diritti nelle sedi competenti.

SEZIONE 9: ALLEGATI (Barrare le caselle corrispondenti ai documenti allegati)

- ☐ Copia del documento di identità in corso di validità del richiedente.
- ☐ Copia della denuncia/querela sporta alle Autorità competenti (se presentata).
- ☐ Eventuale corrispondenza scambiata con terzi (es. esercente, presunta banca, ecc.).
- ☐ Screenshot di messaggi sospetti, pagine web fraudolente, ecc.
- ☐ Altro (specificare): _____

Firma del Richiedente (per esteso e leggibile)

Luogo e Data: _____, __/__/____