



## DISPUTED TRANSACTIONS FORM

*This form can be used to enable Customers (Consumers and Non-Consumers) to notify the Bank of disputed payment transactions on their Current Accounts.*

\*\*\*\*\*

*Please follow these instructions and also carefully read the form on the following pages:*

- 1. complete the Form in its entirety with your personal details and the details of the account where the disputed transactions appeared;*
- 2. "Sign" in the space provided at the bottom of the form;*
- 3. attach any other documents you consider relevant (e.g. emails, screenshots of sites visited and/or text messages received, etc.) and a copy of any reports you have submitted to the competent authorities;*
- 4. send this signed and fully completed form and its attachments to the certified email address: [banca.finnat@pec.finnat.it](mailto:banca.finnat@pec.finnat.it).*

*Once we receive the signed and fully completed documents, we will check the contents and attachments and assess the claim. If the claim is successful, we will refund (under reserve) the transaction amount by the end of the Business Day following the day on which we received this Form.*

First Name and Surname \_\_\_\_\_ Customer CDG \_\_\_\_\_

Chargeback claim for erroneous/unauthorised charge due to a transaction:

- arranged by virtual channel via IB/HB contract branch no. \_\_\_\_\_ cat \_\_\_\_\_ account \_\_\_\_\_
- with BANCOMAT/PagoBANCOMAT card no. \_\_\_\_\_ on account branch \_\_\_\_\_ cat \_\_\_\_\_ account \_\_\_\_\_
- via Sepa Direct Debit (SDD) to account branch \_\_\_\_\_ cat \_\_\_\_\_ account \_\_\_\_\_
- arranged through another channel on account branch \_\_\_\_\_ cat \_\_\_\_\_ account \_\_\_\_\_

*(Mandatory section - to be completed if you dispute payments debited from your current account via unauthorised payment instructions and/or charges)*

QUESTION FOR THE CUSTOMER		RESPONSE	
Internet Banking section			
1	Have you recently received messages via text/email asking you to do anything like the following (i.e. by downloading attachments and/or clicking links): <ul style="list-style-type: none"> <li>- update/confirm your personal data,</li> <li>- check/update or reactivate your account or a shipment to you,</li> <li>- urgently block/reverse suspicious/fraudulent transactions</li> </ul>	YES	NO
2	Has anyone called you purporting to be a financial intermediary (or an anti-fraud or anti-money laundering call centre), asking for sensitive data such as online account login credentials, credit or debit card numbers, security codes and passwords?	YES	NO
3	Have you recently received requests from suppliers, creditors or service companies (by email, letter, text message or phone call) asking you to change the IBAN details to which you make payments?	YES	NO
4	Have you recently entered your personal data, IBAN details or payment card data on devices or IT platforms purporting to be financial intermediaries (banks, card or payment service providers)?	YES	NO
5	Has anyone recently contacted you asking for money loans, urgent payments or financial help for any reason?	YES	NO
6	Have you recently received requests from self-styled customer care workers/IT technicians from companies apparently trusted by you to install programs/software or apps on your device (PC, tablet and/or mobile phone)?	YES	NO
7	Have you recently experienced phone service drops resulting in your not being able to log in to Internet Banking on your phone?	YES	NO
8	Have you activated our EMAIL/PUSH notification service that keeps you informed with security alerts?	YES	NO
9	Do you keep your login credentials (ID Code and Password) separate and inaccessible to third parties, and have not provided them to anyone?	YES	NO
10	Did you always check that "https" and the "closed padlock" symbol appeared in the URL bar?	YES	NO
11	Do you always log out (EXIT button) when you have finished using online banking services?	YES	NO

12	Do you change your password frequently and avoid using the same password for different services?	YES	NO
13	Do you install and regularly update antivirus software to recognise and remove malware?	YES	NO
14	Do you manage your emails carefully to avoid opening spam and clicking on suspicious links?	YES	NO
15	Do you pay close attention to the people accessing your devices (PCs, tablets and/or mobile phones)?	YES	NO
16	Have you always used internet banking via private networks (i.e. internet connection networks NOT open to third parties/public)?	YES	NO
17	Have you activated biometrics on the app to log in and authorise transactions?	YES	NO

Customer Signature\_\_\_\_\_

*(Mandatory section - to be completed if you dispute payments debited from your current account following unauthorised use of your debit card)*

	QUESTION FOR THE CUSTOMER	RESPONSE	
	<b>Payment card section</b>		
1	Have you lost your payment card's Personal Identification Number (PIN)?	YES	NO
2	Have you given your payment card to a third party, even temporarily?	YES	NO
3	Have you told anyone the Personal Identification Number (PIN) of your payment card?	YES	NO
4	If you disclosed your payment card PIN to third parties, did you do so with known and trusted persons?	YES	NO
5	Do you keep your payment card PIN somewhere third parties cannot access it?	YES	NO
6	Have you used your payment card in the last three days?	YES	NO
7	Did you enter your payment card details after receiving potentially fraudulent emails or text messages?	YES	NO
8	Have you activated the NEXI security and control services that notify you of transactions?	YES	NO

Customer Signature\_\_\_\_\_

I, the undersigned

Surname.....First name.....

Tax Code .....

Corporate Name (for companies) .....

Company VAT number or tax code.....

Landline ..... Mobile phone.....

email.....; certified email (if any)

.....

In connection with the following transactions:

TRANSACTION DATE AND TIME	AMOUNT (EURO)	DESCRIPTION (e.g., payee, transaction channel)	TRANSACTION TYPE
<b>TOTAL AMOUNT</b>			

*If you need to report additional transactions to those listed above, you can use the **"ADDITIONAL DISPUTED TRANSACTIONS FORM"** attached to this Form.*

**I HEREBY DECLARE**

*(Mandatory section - please select all applicable options)*

- ☐ that the stated transactions were **not** authorised by me;
- ☐ that the payee of the above transaction has been subsequently altered, without my consent;
- ☐ that the amount of the above transaction has been subsequently altered, without my consent;
- ☐ [to be selected only in the case of SDD debits occurring after a revocation alert] that the creditor/bank has been notified of the revocation of payment instruction no....., effective as of ...../...../..... To this end, I attach a copy of the revocation alert to the creditor;
- ☐ [to be selected only in the case of unauthorised SDD debits] I have never consented to the direct debit instruction to the payee;
- ☐ that the stated transactions were authorised by me but were arranged as a result of manipulation/deception by third parties.

**SUMMARY OF EVENTS****(MUST BE COMPILED)**

*[Please report all relevant facts below. For example: date, time, place, how the transaction took place, any notification received; other circumstances under which the transaction took place; any action taken].*

As a result of the above

**I HEREBY DECLARE**

that I dispute the above transaction(s) as being attributable, in my opinion, to an incorrectly authorised use of the

payment instrument;

### **I ALSO DECLARE**

(Section mandatory in the case of "Unauthorised payment transactions" - select one of the two options):

- ☐ that I have not blocked my card/internet banking profile;
- ☐ that I have blocked my card/internet banking profile by calling the freephone number and/or visiting my branch on (date) \_\_\_\_\_ at (time) \_\_\_\_\_

### **I HEREBY REQUEST**

a refund of the amount of the disputed transactions listed above with chargeback to the above account, noting that:

- A. by the next Business Day following receipt of this Form, signed and fully completed, the Bank will provisionally refund the amount of the stated transactions, restoring the account to the state in which it would have been if the payment transaction had not taken place and ensuring that the amount is available in the account no later than the date of the debit;
- B. reports of unauthorised payment transactions received after 3 p.m. on a Business Day will be deemed to have been received on the next Business Day. For half-working days, this time is moved back from 3 p.m. to 11:30 a.m.;
- C. the Bank may suspend the chargeback in the event of a justified suspicion of fraud;
- D. if, following the chargeback, it is proven that the transactions were correctly authorised, the Bank is entitled to obtain repayment of the refunded amount by debiting the sums on the account and notifying the customer in writing within 60 days.

### **I HEREBY DECLARE**

(Section mandatory in the case of "Unauthorised payment transactions" - select one of the two options)

- ☐ that I have submitted a formal report in relation to the events described above to the competent authority. To this end I attach a copy of the report submitted to the competent authority.
- ☐ that I have not yet been able to submit a formal report to the competent authority in connection with the above. I reserve the right to do so and, if necessary, to provide a copy to the Bank in the knowledge that failure to submit a report could prejudice the initiation of any criminal proceedings against wrongdoers.

*The report to the competent authorities becomes relevant in the course of the investigation into the unauthorised transactions, insofar as it contains further details useful for providing context around the chargeback claims following disputed transactions. Therefore, without prejudice to the acceptance of the claim, it should be noted that failure to send a copy of the report may affect the outcome of the claim made by the Customer, and may consequently entitle the Bank, also in light of an assessment of the specific case, to take action to recover the amount originally refunded within the terms indicated above, where the assessments conducted on the information provided by the Customer through this Form show that the payment transactions are authenticated, correctly recorded and accounted for, and that they have not suffered the consequences of the malfunctioning of the procedures necessary for its execution and/or other reported issues.*

**As such, please submit a report to the competent authorities at the earliest opportunity, also in view of the important evidentiary relevance that this report plays in the customer's interest in decisions on the subject of unauthorised payment transactions in court or out-of-court proceedings.**

**FINALLY, I DECLARE**

- that the data and information provided on this Form is accurate, complete and truthful, for which I accept full responsibility;
- that I am aware of the consequences of providing false data and information and of the related responsibilities incumbent upon me;
- to hold the Bank harmless from any liability it may incur as a result of any false statements made by me in this declaration.

**Attached documentation:**

- ☐ Copy of identity document and tax code (front and back) - always mandatory if this application is submitted by email;
- ☐ [to be selected for "Unauthorised payment transactions" solely if the report is submitted to the competent authority at the same time] copy of the report submitted to the competent authority;
- ☐ other [state any other documents attached] \_\_\_\_\_

Location and Date \_\_\_\_\_ , \_\_\_\_ / \_\_\_\_ / \_\_\_\_

In witness thereof

Signature \_\_\_\_\_

Annex to the Disputed Transactions Form

**ADDITIONAL DISPUTED TRANSACTIONS FORM**

This form is an integral part of the "Disputed Transactions Form" (TO BE COMPLETED IF THE PREVIOUS FORM IS NOT SUFFICIENT).

**Additional disputed transactions:**

TRANSACTION DATE AND TIME	AMOUNT (EURO)	DESCRIPTION (e.g., payee, transaction channel)	TRANSACTION TYPE
<b>TOTAL AMOUNT</b>			

Location and Date \_\_\_\_\_ , \_\_\_\_ / \_\_\_\_ / \_\_\_\_

In witness thereof

Signature \_\_\_\_\_