What should you do if you detect an unrecognized transaction?

Practical guide to reporting fraud

How to Report Fraud at BBVA

This guide details the coordinated two-phase procedure for managing fraud: first, the urgent stock you must take to protect yourself and report; second, BBVA's security measures and resolution times.

Steps you must follow (The Client)

Unrecognized transaction on your **card**

1. **Immediate Report** through Official Channels

   Contact via Contact BBVA **(900 102 801)**, the app ("Adviser" option), or directly at branches.

Digital fraud **(transfer, Bizum, etc.)**

1. **Immediate Report** through Official Channels

   Contact via Contact BBVA **(900 102 801)**, the App ("Adviser" option), or directly at branches.

2. **Report** to the **Authorities**

   Go to the authorities with details of the events, affected products, and screenshots.

3. **Submission** of **Documentation** to BBVA

   Send the complaint and supporting documents to denunciasdefraude.es@bbva.com or deliver them to your branch.

What we (BBVA) do

Automatic **Blocking** and **Protection**

We immediately block compromised cards and digital access after receiving your notification.

Specialized **Ivestigation** and **Analysis**

Our experts analyze devices, biometrics, geolocation, and operating patterns to verify the fraud.

Resolution and **Final** Communication

You will receive a response within 24–72 hours for cards and about 7 business days for transfers/ Bizum.

Introduction

At BBVA, we are aware of the concern and impact that **being the victim of fraud or a scam can cause.**

To help you, we've put together this guide, where you'll find:

- Help to identify what type of fraud you have suffered
  (Exhibit: Details of Fraud/Scam Types)
- The steps to follow.
- The necessary documentation so that we can process your case.
- A clear explanation of the analysis and resolution process carried out by BBVA.

Our goal is to be by your side every step of the way so that your case is handled quickly, safely, and transparently.

What to do if you think you are the victim of fraud?

Step 1: Report the fraud as soon as possible

If you suspect fraud, the first thing to do is **get in touch with us**, where we will tell you how to proceed. All cases are attended to and investigated. Each case is different; the bank analyzes the circumstances individually and responds accordingly.

You can contact us **via:**

- **BBVA Helpline: 900 102 801**
- The App: by clicking the "Adviser" icon
- The Website: by calling the phone number that appears in the "Your adviser" option
- Your nearest BBA branch

Step 2: Immediate blocking and protection

For us, your peace of mind comes first. Therefore, when we detect any sign of risk, **we activate the most appropriate protection measure according to the situation:**

- **We protect your cards:** We temporarily block or turn them off to prevent anyone else from using them.
- **We secure your access:** We preemptively suspend access to your digital channels to ensure that no further transactions are carried out.
- **We monitor your transactions:** We strengthen the monitoring of all your banking activity to detect any unusual transactions instantly.

Step 3: Report the situation

We recommend that you file a report to document the case and help facilitate the investigation; in some instances, we may also request it as part of our assessment.

You can do so at the nearest State Security Forces and Agencies office (open 24 hours a day, 7 days a week).

What information should you include in the report?

When filing the report, it is important that you specify:

- **What has happened**, describing the facts in detail.
- **How you became aware of the** unrecognized transaction.
- **Which product was affected** (account, card, etc.).
- **Which transactions you do not recognize,** indicating amounts and dates if possible.
- **If you have recently shared passwords or personal information.**
- **If you have received any suspicious SMS, email, link or call** related to the incident.

And what documentation do you need to provide when filing the report?

It is recommended that you include:

- **Personal identification documents** (NIF, passport, NIE, etc.).
- **Printout or screenshot of suspicious communications** received or exchanged (e.g., SMS, emails, WhatsApp, etc.).
- **Screenshot of the phone number of the incoming or outgoing call.**
- **Document proving the transactions you do not recognize:** Statement of account or card transactions or, if requested when filing the complaint, a Certificate of Transactions issued by BBVA.

BBVA

How can you obtain the document proving the transactions?

	At the branch	If you are physically present at a BBVA branch, we can provide it for you.
	BBVA Helpline	Call the BBVA Helpline to request that we send you this document by email.
	From your BBVA app/web	**Statement of account transactions:** Access your account or debit card > Search transactions > Enter the date on which the suspicious transaction(s) occurred > Search > Download transactions **Credit card transaction statement:** Access the card > Show more > View statement or Search transactions > Select the date > Show **Account transaction certificate:** Access your account > Show more > Request certificate > Select the transaction certificate > Select the affected transactions > Confirm

Step 4: Submit the claim to BBVA

You can send us the report through our mailbox denunciasdefraude.es@bbva.com or by delivering it directly to your nearest BBVA branch.

Step 5: Review and investigation

Once we receive all the necessary information to analyze your case, our experts review and analyze all security factors to protect your interests:

- **We analyze your online banking access** and suspicious transactions.
- We check if the **device** and the method of **authorization** (like your fingerprint or password) are the ones you normally use.
- We observe the **pattern of the transaction:** the time, the place, and the destination of the amount.

In some cases, to delve deeper into the investigation, **we may need to request additional documentation from you.** If necessary, we will contact you via email or an App notification.

Our commitment is to provide an answer as soon as possible, so **once we receive all the documentation**, the estimated resolution times are:

- **Card incidents:** within a period of **24 to 72 hours.**
- **Fraud in channels (transfers, Bizum, etc.):** within approximately **7 business days**.

Step 6: Final decision

Our team will analyze in detail what happened to determine whether the case allows for a refund or compensation. Once this review is finished, we will personally inform you of the outcome:

- **If the resolution is in your favor:** We will confirm that we have accepted your request and will proceed to credit the corresponding amount to your account as soon as possible.
- **If the resolution is not in your favor:** We'll explain the reasons.

And remember:

- **Never share your passwords, SMS codes, or login details** with anyone.
- **BBVA will never ask you for passwords over the phone, by SMS, or by email.**
- If you have been the victim of digital fraud, **check the security of your devices.**
- **Keep** your operating system and antivirus updated.
- **Be wary of messages** that create **a sense of urgency.**
- **Be wary of messages** that ask **you to click links** or tell you that **you to call a specific phone number:** BBVA will never send this type of message.

Important: You can always verify if a notice is legitimate by contacting us:

- BBVA Helpline: 900 102 801
- Your adviser (you can find your adviser's phone number on the BBVA website/app under the "Your adviser" option
- Your nearest BBVA branch

APPENDICES: Identify the type of fraud/scam

Card theft It refers to the **unauthorized use of a card** following the electronic theft of its details or its physical theft. It can occur through the use of card details in unauthorized online purchases, the theft of the physical card, or the theft of a device with card payment enabled.	**Digital fraud** Unauthorized **access with your credentials** to the various digital channels (App, Web). It is detected when, upon accessing your accounts, there are any unusual or suspicious transactions (such as Bizum payments, transfers, or loan applications) that you do not recognize.
Scam A type of fraud in which the attacker **persuades the customer to carry out a transaction that results in a financial loss**, benefiting the attacker.	**Other** Any other type of fraud detected (document fraud, contracting of unrecognized products, etc.)