ESCRITO DE RECLAMACIÓN FORMAL

Operación de Pago No Autorizada — Phishing / Fraude Bancario

Al amparo del RDL 19/2018 de Servicios de Pago y la STS 571/2025 del Tribunal Supremo

---

■ I. DATOS DEL RECLAMANTE

Nombre y apellidos	[NOMBRE COMPLETO]
DNI / NIE	[NÚMERO DE DOCUMENTO]
Domicilio	[CALLE, NÚMERO, PISO — CIUDAD — CP]
Teléfono de contacto	[TELÉFONO]
Correo electrónico	[EMAIL]
Cuenta / tarjeta afectada	[IBAN O ÚLTIMOS 4 DÍGITOS]

■ II. ENTIDAD DESTINATARIA

AL SERVICIO DE ATENCIÓN AL CLIENTE DE:

Entidad bancaria	[NOMBRE DEL BANCO]
Dirección SAC	[DIRECCIÓN DEL SERVICIO DE ATENCIÓN AL CLIENTE]
Fecha de presentación	[DD/MM/AAAA]
Referencia interna	[NÚMERO DE INCIDENCIA, si lo tienen]

■ III. LEGITIMACIÓN Y RELACIÓN CONTRACTUAL

La parte reclamante es cliente de **[NOMBRE DEL BANCO]**, titular de la cuenta/tarjeta indicada, vinculada mediante contrato de servicios de pago sujeto al **Real Decreto-ley 19/2018, de 23 de noviembre**, que transpone la Directiva (UE) 2015/2366 (PSD2).

En virtud de dicha relación contractual, la entidad actúa como proveedora de servicios de pago y asume las obligaciones legales de seguridad, autenticación y reintegro que se detallan en el fundamento jurídico de este escrito.

■ IV. RELACIÓN DE HECHOS

PRIMERO. Con fecha aproximada de **[FECHA DEL FRAUDE]**, la parte reclamante fue víctima de una operación de fraude de la modalidad **[PHISHING / SMISHING / VISHING / OTRA]**, mediante la cual terceros no autorizados accedieron a sus credenciales bancarias y ejecutaron operaciones de pago sin su consentimiento libre e informado.

SEGUNDO. Las operaciones fraudulentas se detallan en la tabla siguiente, por las que se reclama el reintegro total de **[IMPORTE TOTAL] €**:

FECHA	IMPORTE	CONCEPTO / DESCRIPCIÓN	DESTINO (si consta)
[DD/MM/AAAA]	[XXX,XX €]	[Transferencia no autorizada / Cargo fraudulento]	[Cuenta destino]
[DD/MM/AAAA]	[XXX,XX €]	[Transferencia no autorizada / Cargo fraudulento]	[Cuenta destino]
[DD/MM/AAAA]	[XXX,XX €]	[Transferencia no autorizada / Cargo fraudulento]	[Cuenta destino]
[DD/MM/AAAA]	[XXX,XX €]	[Transferencia no autorizada / Cargo fraudulento]	[Cuenta destino]
[DD/MM/AAAA]	[XXX,XX €]	[Transferencia no autorizada / Cargo fraudulento]	[Cuenta destino]
IMPORTE TOTAL RECLAMADO		**[TOTAL €]**	

TERCERO. Tan pronto como la parte reclamante tuvo conocimiento de las operaciones, procedió a notificarlo a la entidad bancaria, exigiendo el bloqueo de los medios de pago afectados. Asimismo, se procedió a interponer denuncia ante **[POLICÍA NACIONAL / GUARDIA CIVIL / ERTZAINTZA / MOSSOS]**, con número de diligencias previas **[NÚMERO DE DENUNCIA, si consta]**.

CUARTO. Las operaciones referidas no fueron en ningún momento autorizadas por la parte reclamante de forma libre, voluntaria e informada, conforme exige el artículo 36 del RDL 19/2018. El consentimiento aparente obtenido mediante técnicas de ingeniería social no constituye autorización válida a efectos de la normativa de servicios de pago, conforme a la jurisprudencia consolidada del Tribunal Supremo.

■ V. FUNDAMENTO JURÍDICO

1. Operación no autorizada — Artículo 36 RDL 19/2018

Define operación de pago autorizada exclusivamente aquella en la que el ordenante ha dado su consentimiento. El fraude mediante phishing implica que el consentimiento fue obtenido mediante engaño, por lo que no concurre el requisito legal de autorización válida.

2. Inversión de la carga de la prueba — Artículo 44 RDL 19/2018

Corresponde al proveedor de servicios de pago —la entidad bancaria— demostrar que la operación fue autenticada correctamente y que no hubo fallo de seguridad. La mera alegación de que se utilizaron las credenciales correctas es insuficiente para acreditar la autorización del cliente.

3. Obligación de reintegro inmediato — Artículo 45.1 RDL 19/2018

«En caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación». La obligación de reintegro es inmediata y no queda condicionada al resultado de ninguna investigación interna.

4. Responsabilidad del proveedor — Artículo 46 RDL 19/2018

La entidad únicamente queda exonerada si acredita la negligencia grave del usuario. Ser víctima de una técnica de fraude sofisticada no constituye negligencia grave, conforme a la doctrina jurisprudencial mayoritaria de las Audiencias Provinciales y el Tribunal Supremo.

5. Sentencia del Tribunal Supremo 571/2025, de 9 de abril

La Sala Primera del Tribunal Supremo, en sentencia núm. 571/2025 (rec. 1151/2023), ha establecido que el simple hecho de que un tercero accediera a las credenciales del usuario no exime automáticamente al banco de responsabilidad. El banco debe implementar sistemas de detección de operaciones anómalas y responder cuando estos fallen. Esta doctrina consolida la responsabilidad cuasi objetiva del proveedor frente a fraudes por phishing.

6. Normativa complementaria

- Reglamento Delegado (UE) 2018/389: obligación de autenticación reforzada (SCA).
- Orden ECE/1263/2019: plazo de 15 días hábiles para resolver reclamaciones de servicios de pago.
- Orden ECC/2502/2012 y Ley 7/2017: procedimiento ante el Banco de España y resolución alternativa de litigios.
- RGPD (UE) 2016/679: posible brecha de datos personales cuya notificación a la AEPD corresponde a la entidad.

■ VI. PETICIÓN FORMAL

En virtud de todo lo expuesto, se solicita a la entidad que, en el plazo máximo de **15 días hábiles** desde la recepción del presente escrito:

1. Proceda al **reintegro íntegro del importe reclamado de [IMPORTE TOTAL] €**, más los intereses legales devengados desde la fecha de cada cargo fraudulento hasta la fecha de restitución efectiva.
2. Inicie una **investigación interna rigurosa** para determinar las circunstancias del fraude, los fallos de seguridad que lo posibilitaron y las medidas correctoras adoptadas.
3. Adopte las **medidas de refuerzo de seguridad** necesarias para evitar incidentes similares, en cumplimiento del Reglamento Delegado (UE) 2018/389.
4. Emita **resolución escrita y motivada** en el plazo legalmente previsto, conforme a la Orden ECE/1263/2019.
5. Si se hubiera producido una **brecha de datos personales**, proceda a su notificación a la Agencia Española de Protección de Datos en los términos del artículo 33 del RGPD.

■ VII. DOCUMENTACIÓN APORTADA

- Copia del DNI / NIE del reclamante.
- Copia de la denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado (si disponible).
- Extractos bancarios o capturas de pantalla que acreditan los cargos fraudulentos.
- Capturas de los mensajes, correos o llamadas fraudulentas recibidas (si disponibles).
- Cualquier otra documentación relevante para acreditar los hechos.

■ VIII. PLAZOS Y ADVERTENCIA DE ESCALADA

Plazo resolución SAC	15 días hábiles desde recepción (Orden ECE/1263/2019)
Si deniega o no contesta	Reclamación ante el Banco de España — Dpto. de Conducta de Mercado y Reclamaciones
Vía judicial	Demanda civil ante Juzgado de Primera Instancia, más intereses, costas y daños
Plazo de prescripción	5 años desde cada operación fraudulenta (art. 1964 Código Civil)

En caso de no obtener respuesta satisfactoria en el plazo indicado, la parte reclamante se reserva el derecho a ejercitar todas las acciones legales a su disposición, incluyendo la reclamación ante el Banco de España, la vía judicial civil y, en su caso, la denuncia ante la Agencia Española de Protección de Datos.

En [CIUDAD], a [DD] de [MES] de [AÑO].

Fdo.: [NOMBRE Y APELLIDOS]
DNI/NIE: [NÚMERO]