Uso no autorizado

Notificación de operaciones de pago no autorizadas o ejecutadas incorrectamente

Cuando un usuario de servicios de pago —por ejemplo, el titular de una tarjeta o el ordenante de una transferencia— tenga conocimiento de que se ha producido una operación de pago no autorizada o ejecutada incorrectamente, deberá comunicarlo a la entidad, sin tardanza injustificada.

Salvo en los casos en los que el proveedor de servicios de pago no hubiera proporcionado o hecho accesible al usuario la información correspondiente a la operación de pago, la comunicación a la que se refiere el apartado precedente deberá producirse en un plazo máximo de 13 meses desde la fecha del adeudo o del abono.

Responsabilidad del proveedor de servicios de pago por operaciones de pago no autorizadas

En estos supuestos, el proveedor de servicios de pago del ordenante debe devolver a este de inmediato el importe de la operación de pago no autorizada, restableciendo la cuenta de pago al estado que habría tenido de no haberse producido la operación de pago no autorizada, en su caso; ello, claro está, con independencia del derecho que asiste a la entidad de efectuar cuantas actuaciones estime convenientes en defensa de sus legítimos intereses.

Prueba de la autenticación y ejecución de operaciones de pago

Como indicamos anteriormente, corresponde a la entidad demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico o por cualquier otra anomalía. No obstante, el registro por parte del proveedor de servicios de pago de la utilización del instrumento de pago no bastará necesariamente para demostrar que la operación fue autorizada por el ordenante ni que este actuó de manera fraudulenta o incumpliendo deliberadamente o por negligencia grave una o varias de las obligaciones que le incumben como usuario del servicio de pago, a saber: i) utilizar el instrumento de pago de conformidad con las condiciones que regulen su emisión y utilización; ii) tomar todas las medidas razonables a fin de proteger los elementos de seguridad personalizados de los que vaya provisto, y iii) en caso de extravío, sustracción o utilización no autorizada del instrumento de pago, notificarlo sin demoras indebidas a la entidad, en cuanto tenga conocimiento de ello, debiendo la entidad adoptar las medidas necesarias para evitar, desde que se produce dicha

comunicación, la utilización ilegítima del instrumento de pago por terceros no autorizados, debiendo contar esta con medios adecuados y gratuitos a fin de posibilitar, en todo momento, que el titular efectúe la comunicación de la operación de pago cuya autoría no reconoce.

La acreditación de las operaciones variará dependiendo del uso dado a la tarjeta, siendo los más habituales los de reintegros en efectivo y los de pago en establecimientos comerciales. En el primero de los casos, la entidad deberá acreditar mediante sus propios registros internos —o los de la entidad propietaria del cajero en el que se llevó a cabo la operación, previa solicitud a esta de la correspondiente documentación justificativa— que esta fue correctamente registrada y que no se vio afectada por ninguna deficiencia. En el segundo de los casos, esto es, cuando la tarjeta se usa como medio de pago en un comercio, cabe exigir a la entidad emisora de la tarjeta que actúa como intermediaria en el pago lo siguiente:

- Que aporte evidencia documental justificativa de la operación, especialmente de la referida a su autenticación, esto es, de la autorización otorgada a la operación por parte del titular conforme al modo pactado por las partes: autenticación mediante tecleo de PIN o mediante boleta firmada.

- Que contacte con el comercio para comprobar la versión de los hechos defendida por su cliente —que asevera que no autorizó la operación en cuestión—, frente a la afirmación del propio comercio beneficiario del pago, recabando para ello cuantos elementos de prueba obren en poder de este o de cualquier otra manera, siempre que se derive de la actuación de la entidad una gestión diligente de la reclamación instada. Y ello tanto en el supuesto de operaciones efectuadas presencialmente como a distancia, debiendo desplegar la entidad una especial diligencia en la averiguación de los hechos cuando esta resulte gravosa para el cliente, como ocurriría en el caso de operaciones realizadas en el extranjero.

- Que realice una gestión diligente y puntual de la reclamación efectuada por su cliente ante la sociedad propietaria del sistema, para conseguir, en su caso, la devolución de los importes adeudados en cuenta si estos no hubieran sido procedentes de acuerdo con las condiciones en que se realizara la contratación.

En cuanto a la valoración de la autenticidad de las firmas contenidas en los resguardos de compras, no corresponde al DCMR efectuar dicha apreciación, pues únicamente los tribunales de justicia, a través de la práctica de los medios de prueba que estimen necesarios, pueden determinar la falsedad de la firma contenida en los resguardos, así como pronunciarse acerca de la diligencia empleada por todos los sujetos intervinientes en el cumplimiento de sus obligaciones; entre ellos, los establecimientos comerciales.

Responsabilidad del ordenante por operaciones de pago no autorizadas derivadas de la utilización de un instrumento de pago extraviado o sustraído

El artículo 32 de la LSP prevé que el ordenante tan solo soportará hasta un máximo de 150 euros —que desde el 24 de febrero de 2019 se ha reducido a 50 euros, por mor de lo dispuesto en el vigente RD-l[1]— de las pérdidas derivadas de la utilización de un instrumento de pago extraviado o sustraído, salvo que la operación de pago no autorizada fuera fruto de una actuación fraudulenta del ordenante o del incumplimiento deliberado o por negligencia grave de sus obligaciones, en cuyo caso este soportará el total de las pérdidas derivadas de las operaciones de pago no autorizadas.

Por otra parte, el ordenante no soportará consecuencia económica alguna derivada del uso fraudulento de la tarjeta extraviada o sustraída con posterioridad a la notificación a la entidad del extravío, la sustracción o la utilización no autorizada del instrumento de pago.

En cuanto a la enervación por parte de las entidades del límite de responsabilidad descrito, es criterio reiterado de este DCMR considerar que en última instancia habrán de ser los tribunales de justicia, y no las entidades de crédito como parte interesada, los que deberán valorar y determinar, en su caso, la existencia de una conducta fraudulenta o el incumplimiento, deliberado o por negligencia grave, de las obligaciones que corresponden al titular en relación con el instrumento de pago.

Fraude con datos de tarjetas

Dentro del apartado que ahora analizamos, y en lo que respecta a la responsabilidad del servicio de pago por operaciones de pago no autorizadas, cabe incluir, a juicio del DCMR, aquellas en las que el titular no ha perdido la posesión del plástico.

En estos casos, para demostrar que las operaciones de pago fueron autenticadas, registradas con exactitud y contabilizadas, las entidades financieras aportan con frecuencia copia de sus registros internos, en los que se reflejan diferentes datos sobre la ejecución de las distintas operaciones de pago. El DCMR ha venido considerando que, además de la aportación de dichos registros, en caso necesario, deben aportar una explicación de su contenido.

Por lo que respecta a la presentación de la documentación justificativa de las operaciones controvertidas, una dificultad añadida aparece cuando la utilización de la tarjeta se produce a distancia, por Internet, utilizando únicamente los datos de aquella en conjunción, en su caso, con otros dispositivos o códigos de seguridad.

[1] Otra novedad interesante en relación con esta cuestión, introducida por el nuevo Real Decreto-ley 19/2018, es la de que el ordenante quedará exento de toda responsabilidad en caso de sustracción, extravío o apropiación indebida del instrumento de pago cuando las operaciones se hayan efectuado de forma no presencial utilizando únicamente los datos impresos en el propio instrumento, siempre que no se haya producido fraude o negligencia grave por su parte en el cumplimiento de sus obligaciones de custodia del instrumento de pago y las credenciales de seguridad, y haya notificado dicha circunstancia sin demora.

Las entidades emisoras de las tarjetas suelen aportar para acreditar tanto la autenticación por parte del titular (no olvidemos que en operaciones a distancia no se puede realizar una identificación presencial del portador de la tarjeta) como la autorización de la operación copia de los registros internos, que, a su vez, les facilitan las redes o las entidades globales. En cualquier caso, desde el punto de vista del cumplimiento de la normativa sobre servicios de pago y de las buenas prácticas con las que se debe proceder con la clientela, resulta imprescindible que la forma de prestar el consentimiento para la realización de las operaciones de pago esté acordada con el cliente y se encuentre debidamente recogida en el contrato, todo ello en los términos que señala la normativa de servicios de pago.

Además, con respecto a esta cuestión, resulta oportuno recordar las ya citadas directrices de la ABE sobre la seguridad de los pagos por Internet, que fueron adoptadas como propias por la Comisión Ejecutiva del Banco de España en su sesión del 24 de marzo de 2015[2] y que han sido incorporadas al derecho positivo a través de las normas sobre seguridad del vigente Real Decreto-ley 19/2018. Estas previsiones establecen un conjunto de requisitos mínimos de seguridad en la lucha contra el fraude, y su finalidad es aumentar la confianza del consumidor en los servicios de pago por Internet. Así, recomiendan con carácter general —salvo en ciertas excepciones [3]— que los proveedores de servicios de pago, para autorizar las operaciones de pago por Internet o para modificar datos sensibles, usen procedimientos de autenticación fuerte del cliente, que se definen como aquellos basados en el uso de dos o más de los siguientes elementos, clasificados como conocimiento, posesión e inherencia:

i) Algo que solo conoce el usuario: por ejemplo, una contraseña, un código o un número de identificación personal fijos.

ii) Algo que solo posee el usuario: por ejemplo, token, tarjeta inteligente, teléfono móvil.

iii) Algo que caracteriza al propio usuario: por ejemplo, una característica biométrica, como su huella dactilar.

Tales elementos, según la ABE, deben ser independientes entre sí (es decir, la violación de uno no debe comprometer la seguridad de los otros) y al menos uno de ellos no debe ser reutilizable ni reproducible, ni debe resultar posible su sustracción, de manera subrepticia a través de Internet.

Del contenido de dichas directrices, también interesa destacar su punto 5, que establece que los proveedores de servicios de pago deben contar con procesos que garanticen que

[2] Pueden consultarse en https://www.bde.es/bde/es/secciones/normativas/Guias/Guias.html.

[3] Pagos de escasa cuantía o a beneficiarios de confianza que el cliente previamente seleccione, pagos a favor de beneficiarios de confianza que estén incluidos en listas blancas que ese cliente haya establecido, operaciones entre dos cuentas del propio cliente dentro de la misma entidad o transferencias dentro de la misma entidad de pago cuando esté justificado por un análisis del riesgo de las operaciones.

todas las operaciones, así como el flujo del proceso del mandato electrónico, quedan adecuadamente registradas.

Por lo tanto, resulta esencial que las operaciones de pago autorizadas por internet queden adecuadamente explicadas, con especial referencia a la forma en que se autenticó el titular y el modo en que se prestó el consentimiento a la operación realizada, también para poder comprobar si la operativa se ajusta a lo establecido en las directrices. Si la entidad emisora de la tarjeta no dispusiera de documentación suficiente, deberá recabarse de los sistemas de tarjetas, redes o plataformas y/o de los establecimientos comerciales intervinientes.

Comercio electrónico seguro

Con frecuencia, las entidades emisoras de tarjetas, ante una reclamación de un titular de tarjeta por la que manifiesta no haber autorizado un pago con los datos de aquella por Internet, se limitan a indicar que se ha realizado mediante «Comercio Electrónico Seguro». Con este sistema se trata de garantizar la seguridad de las compras con tarjeta a través de Internet, de forma que, al efectuar la compra, la plataforma redirige al cliente a un sitio seguro, en el que, además de los datos de la tarjeta —número, caducidad, los tres dígitos del reverso—, debe introducir un código de identificación personal (CIP, habitualmente una OTP) que solo el titular de la tarjeta debe conocer. Los datos de la tarjeta irán encriptados, de forma que el establecimiento comercial no llega a conocer esos datos.