Pagos con tarjeta no autorizados

Notificación de operaciones de pago no autorizadas o ejecutadas incorrectamente

En este epígrafe nos remitimos a lo ya expuesto sobre el particular en el apartado 9.1.6 de este capítulo, «Régimen de las operaciones de pago no autorizadas».

Responsabilidad del proveedor de servicios de pago por operaciones no autorizadas

En este epígrafe nos remitimos a lo ya expuesto sobre el particular en el apartado 9.1.6 de este capítulo, «Régimen de las operaciones de pago no autorizadas».

Prueba de la autenticación y ejecución de las 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 el ordenante 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.

Para demostrar que la operación reclamada fue autenticada, registrada con exactitud y contabilizada, las entidades financieras aportan con frecuencia copia de sus registros internos, en los que se reflejan diferentes datos sobre la ejecución de la misma. El DCE ha venido considerando que, además de la aportación de dichos registros, en caso de ser necesario, deben aportar una explicación de su contenido.

La acreditación de las operaciones variará dependiendo del uso dado a la tarjeta.

Si se tratara de reintegros en efectivo, 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 dicha entidad de la correspondiente documentación justificativa— que esta fue correctamente registrada y que no se vio afectada por ninguna deficiencia.

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, OTP, biometría o boleta firmada.
- Que recabe cuantos elementos de prueba estén a su disposición, de modo que se derive de la actuación de la entidad una gestión diligente de la reclamación instada. Y ello en el supuesto de operaciones efectuadas tanto 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 DCE 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 esos documentos, así como pronunciarse acerca de la diligencia empleada por todos los sujetos intervinientes en el cumplimiento de sus obligaciones. 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 por Internet. Las entidades emisoras de las tarjetas suelen aportar, para acreditar tanto la autenticación por parte del titular como la autorización de la operación, copia de los registros internos, que, a su vez, les facilitan las redes de pago o las entidades globales. En cualquier caso, dichos registros deben quedar adecuadamente explicados, y, desde el punto de vista del cumplimiento de la normativa de transparencia 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.

En la R-202018219, el reclamante mostró su disconformidad con dos compras realizadas con su tarjeta cuya autoría no reconocía, afirmando que él nunca había autorizado pagos por Internet con dicho instrumento, sino solo a través de datáfono.

Por su parte, la entidad reclamada sostenía que no procedía el abono de las operaciones reclamadas, ya que estas habían sido validadas mediante el código de seguridad enviado al teléfono del cliente, aportando al efecto determinada documentación. Toda vez que esta no fue considerada suficiente para acreditar la autoría y registro de la operación, el DCE concluyó que la entidad podría haber quebrantado el artículo 44 RDLSP. Se advertía a la entidad, además, de que sería deseable que, en los casos en que el usuario cambia repentinamente su pauta de uso del instrumento de pago, explicase si dispone de controles (aplicación de técnicas de aprendizaje automático, tecnologías de procesamiento distribuido, reconocimiento de patrones, etc.) que eviten o reduzcan la posible utilización fraudulenta de los instrumentos de pago que utilizan sus clientes.

En ocasiones, las operaciones discutidas han sido efectuadas, ya sea presencialmente en un establecimiento comercial o por Internet, mediante una aplicación de pago móvil a la que fue enrolada la tarjeta de la parte reclamante. En caso de resultar controvertida esa activación, será necesario, además, que la entidad reclamada aporte los registros acreditativos del correspondiente enrolamiento o alta de la tarjeta de su cliente en la aplicación de pago móvil con la que se autorizaron las operaciones en cuestión, y que se evidencie que dicho proceso tuvo lugar por medio de un sistema de autenticación reforzada.

El reclamante de la R-202016412 solicitaba la devolución de unos cargos considerados fraudulentos, pues manifestaba haber sido víctima de un posible phishing y que la tarjeta continuaba en su poder.

La entidad reclamada alegó que las operaciones reclamadas se realizaron de forma presencial con un dispositivo móvil mediante el enrolamiento de la tarjeta del cliente en una aplicación de pago móvil, sin que hubiese existido fallo técnico alguno en su autorización.

Si bien la entidad aportó el registro de las operaciones cuestionadas —aspecto del cual nada se reprochó a su proceder—, no acreditó de manera suficiente en el expediente la vinculación o alta de la tarjeta del reclamante en la aplicación de pago móvil con la que fueron autorizadas las operaciones discutidas. Por este último motivo, el DCE emitió un pronunciamiento contrario a la actuación de la entidad reclamada.

Autenticación reforzada de clientes

De conformidad con lo establecido en el artículo 68 del RDLSP —que, recordemos, transpone a la normativa nacional las disposiciones de la Directiva 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior—, los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes, en la forma, con el contenido y con las excepciones previstas en el

Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017[1], por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros, cuando el ordenante acceda a su cuenta de pago en línea, inicie una operación de pago electrónico y realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.

El Reglamento Delegado persigue como objetivo que los servicios de pago ofrecidos electrónicamente se presten con la adecuada protección, gracias a la adopción de tecnologías que permitan garantizar una autenticación segura del usuario, minimizándose así el riesgo de fraude.

En su artículo 3.5, el RDLSP define la autenticación reforzada como la

autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), que son independientes —es decir, que la vulneración de uno no compromete la fiabilidad de los demás—, y concebida de manera que se proteja la confidencialidad de los datos de identificación.

Esas exenciones a que se refiere la normativa citada que hacen que no sea preciso aplicar la autenticación reforzada de clientes se basan en: i) el nivel de riesgo que entrañe el servicio prestado, ii) el importe de la operación, la frecuencia con la que se repite o ambas cosas, y iii) el canal de pago empleado para la ejecución de la operación. De manera que la norma determina los siguientes supuestos: pagos de escasa cuantía, pagos sin contacto en el terminal de venta, así como en terminales no atendidas para tarifas de transporte o pago de aparcamiento, operaciones frecuentes, pagos a favor de beneficiarios de confianza que estén incluidos en listas blancas que el cliente haya establecido, transferencias entre dos cuentas del propio cliente dentro de la misma entidad, y operaciones de pago electrónico cuando estén justificadas por un análisis del riesgo. Además, se prevé la posibilidad de no aplicar la autenticación reforzada cuando el cliente consulte en línea el saldo de su cuenta de pago o las operaciones ejecutadas en los últimos 90 días.

En la R-202013063, el reclamante solicitaba el abono de una operación de pago con tarjeta que, según indicaba, no había sido efectuada por él.

En sus alegaciones la entidad señaló que el pago se efectuó, una vez informados los campos obligatorios en el sitio web del comercio —número de la tarjeta, fecha de caducidad y CVV—, mediante el envío al reclamante del SMS donde se informaba, entre otros datos, del importe y el código de un solo uso necesario para la autorización de la operación.

[1] De aplicación desde el 1 de enero de 2021, tras la finalización del período concedido a las entidades para adaptarse a las exigencias establecidas por la norma.

Por cuanto la entidad reclamada acreditó la correcta autenticación de las operaciones, así como el empleo de autenticación reforzada en el pago cuestionado, no se encontraron motivos para emitir una opinión desfavorable a su actuación.

Por el contrario, en la R-202017211, en la que el reclamante afirmaba no haber realizado la operación de pago controvertida por Internet y pedía su devolución, el DCE concluyó que el proceder de la entidad reclamada fue contrario a las buenas prácticas y usos financieros debido a que, pese a manifestar que la operación reclamada había sido autorizada con un método de autenticación reforzada (código de un único uso remitido por SMS), no aportó documento acreditativo de dicho extremo.

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

El artículo 46 del RDLSP prevé que el ordenante soportará hasta un máximo de 50 euros 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. Y 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.

En cuanto a la enervación por parte de las entidades del límite de responsabilidad descrito, es criterio reiterado de este DCE 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.