Tarjetas contactless: mitos, verdades y algunos consejos para evitar fraudes

Especialistas de Visa, Eset, Mastercard y Midinero explicaron qué tan seguras son las nuevas tarjetas de pago sin contacto. Además, desde el Banco Central se detalló si el innovador sistema está alineado a la normativa local.

PÍA MESA

Se estima que en Uruguay ya circulan alrededor de **50.000 tarjetas contactless** —pago por proximidad, es decir, sin contacto—, y más de 20.000 comercios que ya aceptan esta tecnología que permite que los usuarios realicen transacciones sin tener que insertar la tarjeta e ingresar el PIN como se exige con los plásticos tradicionales.

Sin embargo, **pese a que las nuevas tarjetas ahorran tiempo a los clientes también pueden ser objeto de fraude**. Sobre esto y respecto a la protección que ofrecen los emisores de este producto al usuario, El País consultó a diversos especialistas que explicaron qué tan seguros son los nuevos plásticos y qué recaudos se pueden tomar.

Las transacciones realizadas con esta tecnología son más rápidas dado que no exigen que el cliente introduzca un PIN o firme un cupón, excepto en aquellas compras que superen los $ 1.000.

Esta “flexibilidad” en el método de pago no va contra la normativa actual, dado que en diciembre del año pasado el **Banco Central (BCU)** aprobó la Circular Nº 2.316 que incorporó la definición de esta nueva tecnología de pago, **para transacciones presenciales por hasta el equivalente a 5.000 Unidades Indexadas (UI), unos $ 21.100.**

Según se explicó a El País desde el Departamento de Comunicación del BCU, “el uso de tecnología de pago sin contacto contempla los requerimientos que establece la reglamentación”.

Para el experto en seguridad de la información y director de Eset Uruguay, José Luis López, el BCU "flexibilizó las condiciones de exigencia de PIN porque es una tendencia que se da a nivel mundial y que responde a una lógica de facilitación del comercio".

A modo de ejemplo, López mencionó que en Europa las ventas mínimas de 20 euros con este tipo de tarjetas también prescinden de la exigencia del PIN. "Esto no es un invento uruguayo", señaló.

No obstante, el director de Eset Uruguay dijo que "como toda nueva tecnología" tiene sus propios riesgos y recomendó "conocer el sistema" para poder actuar de forma más segura.

Los riesgos de una nueva tecnología

El hecho de que para utilizar este tipo de tarjetas no se exija el PIN en las compras por bajos montos, puede llevar a que el usuario sea **víctima de robo** y que si no se da cuenta los delincuentes puedan utilizar la tarjeta para realizar compras por montos menores a $ 1.000.

Por otro lado, el director de Eset manifestó que "en otros países del mundo" se han viralizado videos en los que se muestra cómo los estafadores pueden "leer" una tarjeta de este tipo si solamente se acerca lo suficiente a la persona.

Sobre este punto, **el presidente de Mastercard (uno de los emisores de este tipo de instrumentos) para el Cono Sur, João Pedro Paro Neto**, explicó a El País que cuando se realiza una transacción sin contacto, la tarjeta o el dispositivo le proporciona al lector un número único y dinámico que identifica "de forma única y segura cada transacción".

Según explicó, esto implicaría que para un estafador "sería extremadamente difícil copiar la tecnología de encriptación avanzada que se usa para generar este número dinámico y crear una versión falsificada".

Como otra forma de confirmar la seguridad de las transacciones, el presidente de Mastercard remarcó que para que una compra sea autenticada y autorizada por teléfono o en línea, "por lo general se deben presentar varios datos, incluido el código de tres dígitos en el reverso de una tarjeta y el nombre y la dirección de facturación del titular".

Y explicó que dado que en el dispositivo no se envían el código, la dirección de facturación, la información del código postal o el nombre en la interfaz de la tarjeta sin contacto, “el delincuente no tendrá la información que generalmente se necesita para realizar transacciones de pago, ya sea en persona, por teléfono o en línea”.

Lo cierto es que existen aplicaciones para teléfonos inteligentes que posibilitan que el teléfono lea algunos datos de la tarjeta sin contacto, pero ante esto **el ejecutivo de Mastercard** señaló que “solo pueden leer el número de cuenta y la fecha de vencimiento”.

En línea con esto, el experto en seguridad de Eset consideró que “aunque no es imposible, es realmente muy difícil elaborar una estafa con este tipo de tarjetas” y añadió que la seguridad no solo es vigilada por el usuario, sino también por los emisores.

Sobre esto, el presidente de Mastercard confirmó que “los emisores poseen reglas” y que “si las transacciones salen del padrón de transacciones del tarjetahabiente, los emisores no las aceptan”.

Fuentes de Midinero coincidieron en que “no es viable” que solo con la cercanía se puedan robar los datos de la tarjeta,

Asimismo, según explicaron a El País, “el nivel de fraude con contactless es muy inferior a los de la tarjeta con contacto”.

La política de "Cero responsabilidad" de Visa.

Al igual que con las tarjetas tradicionales, los emisores tienen políticas de protección y seguridad de las transacciones de sus clientes. En el caso de **Visa**, la compañía explica que los pagos contactless están protegidos “por las mismas tecnologías” que los otros productos de la firma.

Según indica la empresa, “cada producto de pago de Visa está protegido con seguridad a nivel de tarjeta, de terminal y de red”, mediante la utilización de inteligencia artificial, algoritmos criptográficos y analítica en tiempo real que buscan evitar el fraude.

SEGURIDAD

También Mastercard lo tiene

Al igual que Visa, Mastercard ejecuta la política “responsabilidad cero”. Dicha medida asegura a los clientes que en caso de robo o de fraude, no deberán hacerse cargo de aquellas transacciones que no reconozcan como propias.

Empero, si el usuario llega a ser víctima de fraude, **los clientes de Visa están protegidos con una política llamada “Cero Responsabilidad”** en la que el tarjetahabiente no será responsable por cargos no autorizados.

Algunos tips para un buen uso.

Con el objetivo de evitar el robo o fraude de las tarjetas contactless, desde **Mastercard** brindaron consejos para un buen uso del producto.

Por un lado, recomendaron monitorear las cuentas y revisarlas por transacciones que no se reconozcan.

Sumado a eso, recordaron que el usuario debe saber que “nadie debe comunicarse” para solicitar información personal ni datos de su cuenta, y que “si esto ocurre, la persona afectada se debe comunicar con su banco”.

¿Qué se debe hacer en caso de robo o fraude?

”Los pagos sin contacto son seguros”, dijo a El País **João Pedro Paro Neto, presidente de Mastercard para el Cono Sur**. Sin embargo, recomendó que en caso de que un cliente sospeche de una actividad fraudulenta se comunique con la institución financiera que emitió la tarjeta.

Además, manifestó que existe la posibilidad de denunciar una actividad sospechosa a través del sitio web de la institución.

En el caso de **Visa**, la compañía coincide en que se debe “notificar de inmediato” cualquier uso no autorizado y explica que “la transacción en cuestión debe ser asentada a la cuenta del cliente antes de que se puedan emitir fondos de reembolso”.

Por otro lado, la compañía informó que el emisor “podría rehusar, demorar, limitar o rescindir un crédito provisional por transacciones no autorizadas basándose en una demora para reportar el uso no autorizado o verificar un reclamo, o basándose en el estado e historial de la cuenta”.

No obstante, para evitar estas situaciones, desde **Mastercard** aconsejaron qué hacer para minimizar el riesgo. Al respecto, dijeron que los usuarios deberían evitar hacer clic en vínculos que no reconozcan, utilizar contraseñas inteligentes y destruir los resúmenes de cuenta antes de desecharlos.

Desde **Midinero** creen que el **contactless** es más seguro ya que permite que el cliente lleve la tarjeta todo el tiempo en su mano, sin tener que entregarla a nadie.

¿Cuáles son los derechos del consumidor a lo largo del ciclo de la transacción con tarjetas?

La responsabilidad en lo que respecta al ciclo de las transacciones de medios de pago electrónicos recae en los emisores y no en los usuarios.

Así lo establece el artículo 81.3 del **Libro VII de la Recopilación del Sistema de Pagos del Banco Central (BCU),** en el que se establece que los emisores de estos productos “serán responsables frente a los usuarios por asegurar que la calidad del servicio a lo largo del ciclo de la transacción de pago cumpla con los mínimos establecidos por la reglamentación”.

Además, la normativa define que la infraestructura seleccionada para utilizar los instrumentos electrónicos, “debe asegurar la calidad del servicio, a través del cumplimiento de indicadores de calidad aplicables al nivel de servicios, seguridad de la información, seguridad informática, capacidad y continuidad operativa, así como disponibilidad del servicio”.

Esto implica que **“los emisores serán responsables”** por la selección de terceras partes proveedoras de servicios y de dicha infraestructura que cumplan “con los niveles de calidad establecidos”

Entre los indicadores de calidad exigidos está la confidencialidad de los datos de los usuarios y la respuesta a los usuarios ante reclamos por inconsistencias o errores en las transacciones.