

Opinión

Hernán Libedinsky
Moscovich



Fiscal Regional de Aysén

Prevención de los fraudes con medios de pago electrónicos

Nuestro país ha experimentado cambios profundos en la forma en que compramos, contratamos servicios y realizamos pagos, sobre todo en los últimos años. El comercio electrónico, las aplicaciones móviles y las plataformas digitales llegaron para quedarse.

Para algunos, esto facilita la vida cotidiana, ampliando la oferta disponible y permitiendo acceder a bienes y servicios que antes parecían lejanos, más aún desde un territorio austral como el nuestro. Sin embargo, este avance también ha traído consigo nuevos riesgos que hoy se reflejan con claridad en las cifras delictuales.

Durante el 2025, los delitos asociados al uso fraudulento de tarjetas y otros medios de pago registraron en nuestra región un incremento relevante en el número de causas ingresadas, en relación al año 2024, cifra que compartiremos próximamente en la cuenta pública de la Fiscalía fijada para el 20 de enero.

Se trata de una señal de alerta que no puede dejarnos indiferentes. Detrás de estos números hay personas afectadas y una sensación de inseguridad que impacta en la confianza de la comunidad.

A diferencia de otros ilícitos tradicionales, el fraude con medios de pago no siempre se percibe de inmediato. El delito ocurre en silencio y se manifiesta recién cuando una persona revisa su estado de cuenta y detecta cargos que no reconoce.

En la Fiscalía hemos observado un patrón que se repite con frecuencia: personas que advierten compras en dólares, asociadas a plataformas de juegos en línea, aplicaciones de entretenimiento, streaming, suscripciones digitales o tiendas virtuales internacionales, entre otros.

Puede ocurrir que la víctima nunca tuvo la intención de contratar ese servicio o lo realizó un tercero sin consentimiento. Incluso han ocurrido casos donde autorizó una descarga gratuita sin advertir que luego se transformaría en un cobro periódico, ya sea por engaño, uso no autorizado de datos o por condiciones contractuales poco transparentes que no necesariamente constituyen un delito penal.

El comercio electrónico ha simplificado enormemente el acceso a servicios, pero esa misma facilidad puede convertirse en una puerta de entrada para el fraude si no existen medidas básicas de autocuidado.

Basta con ingresar los datos de una tarjeta una sola vez para que queden almacenados en una plataforma, o con que un tercero tenga acceso momentáneo al teléfono, para que se genere una cadena de cargos, cuya trazabilidad penal y atribución de responsabilidad es compleja. Asociar el pago de las tarjetas con los teléfonos puede ocasionar problemas.

En aquellos casos en que la gente decide denunciar se puede iniciar investigaciones, identificar patrones delictuales y perseguir penalmente a los responsables. No obstante, también es importante señalar que muchos de estos delitos presentan una alta complejidad investigativa, especialmente cuando involucran plataformas extranjeras, servidores fuera del país o intermediarios digitales que operan bajo otras legislaciones, por la necesidad de cooperación internacional.

Por ello, junto con la persecución penal, la prevención se vuelve una herramienta clave. La experiencia investigativa nos permite identificar algunos escenarios de mayor exposición. Por ejemplo, las aplicaciones de juegos y entretenimiento, especialmente aquellas descargadas por niños, niñas y adolescentes, que solicitan datos de tarjetas para acceder a niveles, beneficios o contenidos adicionales.

Además, suscripciones "gratuitas" que, tras un período de prueba, comienzan a cobrar automáticamente en dólares; correos electrónicos, mensajes o enlaces falsos que simulan ser legítimos, como información oficial del banco, de una empresa de reparto o de una plataforma conocida, buscando obtener datos personales o bancarios.

Otros casos se relacionan con almacenamiento automático de tarjetas en sitios web o aplicaciones sin revisar sus condiciones.

En muchas situaciones, las personas no detectan de inmediato el fraude porque los montos iniciales son bajos o porque el cobro aparece en moneda extranjera, lo que dificulta reconocerlo a simple vista.

Frente a este escenario, recomendamos revisar periódicamente los estados de cuenta, incluyendo los cobros en dólares, idealmente de forma semanal y no solo a fin de mes. También sería adecuado activar notificaciones bancarias por cada compra o movimiento realizado con tarjetas.

Asimismo, no ingresar datos de tarjetas en aplicaciones o sitios de dudosa procedencia o con ofertas extraordinarias, especialmente en juegos o plataformas poco conocidas y desactivar el almacenamiento automático de tarjetas cuando no sea estrictamente necesario.

Otro punto relevante dentro de todo este ámbito es supervisar el uso de dispositivos por parte de niños y adolescentes, configurando límites de compra y controles parentales. Ante un cargo no reconocido, es ideal bloquear de inmediato la tarjeta con el banco, realizar el reclamo correspondiente y luego efectuar la denuncia.

Estas acciones no eliminan completamente el riesgo, pero sí reducen significativamente la posibilidad de ser víctima de fraude. La seguridad hoy también involucra el ámbito digital y la prevención requiere del compromiso de las instituciones públicas, sistema financiero, comercio, familias y los propios usuarios.