Servicio Nacional
del Consumidor

Fraude en Medios de Pago en Chile
Tipologías del Fraude

Subdirección de Consumo Financiero
Coordinación de Economía del Comportamiento
Departamento de Investigaciones Colectivas Financieras
Departamento Protección al Consumidor Financiero y Supervisión de Mercado

Julio de 2025

Resumen ejecutivo

En los últimos años, Chile ha experimentado un aumento sin precedentes en las reclamaciones por fraudes en medios de pago digital. Por ejemplo, en el sector bancario, las reclamaciones se duplicaron en 2023, pasando de 311.000 a 684.000 anuales. Este incremento también se reflejó en los montos reclamados, que ascendieron de $108 mil millones a $243 mil millones. Destaca el caso de Banco Estado, que fue el más afectado por este fenómeno, donde las reclamaciones se triplicaron y los montos se multiplicaron por siete entre 2022 y 2023.

Frente a esta situación, diversos actores de la industria financiera expresaron que el crecimiento sustancial en los patrones de reclamación por fraude podría vincularse a fenómenos de riesgo moral o, incluso, a conductas de autofraude, lo que generó un debate relevante en torno a la adecuación de los incentivos regulatorios y la efectividad de los mecanismos de control. Como respuesta regulatoria, se modificó la Ley N.º 20.009 sobre la limitación de la responsabilidad de los usuarios de tarjetas de pago y transacciones electrónicas en casos de extravío, hurto, robo o fraude, con la entrada en vigencia de la Ley N.º 21.673 el 30 de mayo de 2024.

En este contexto, el presente estudio tuvo como objetivo profundizar en la comprensión integral del fenómeno del fraude en medios de pago digital en Chile, buscando responder las siguientes preguntas de investigación:

1. ¿El fenómeno observado en el país es un caso aislado o se replica en otras partes del mundo?
2. ¿Qué tipologías de fraude afectaron a los consumidores en el país durante este período analizado?
3. ¿Cuáles son las potenciales vulnerabilidades de seguridad que podrían facilitar la ocurrencia de fraudes?
4. En cuanto a las campañas de concientización, ¿logran informar adecuadamente sobre los riesgos que enfrentan los consumidores?

1. ¿El fenómeno observado en el país es un caso aislado o se replica en otras partes del mundo?

Las cifras internacionales del cibercrimen revelan un crecimiento exponencial en las denuncias por fraude cibernético a nivel mundial durante los últimos años. Este fenómeno es particularmente notorio en el periodo posterior al brote de la pandemia del

Coronavirus, episodio que impulsó significativamente la adopción de medios de pago digitales a nivel global, contribuyendo así al aumento de estos delitos. Esta tendencia se observa en la mayoría de los países. Además, según el informe Global de Riesgos del World Economic Forum de 2024, la inseguridad cibernética se posiciona en el cuarto lugar del ranking de Riesgos Globales de corto plazo más graves.

Una excepción a esta tendencia global es la exhibida por la Unión Europea, donde mejoras regulatorias han logrado mitigar el impacto de los fraudes, especialmente aquellos vinculados con tarjetas de crédito y débito. En 2021, el fraude con tarjetas en la UE alcanzó su nivel más bajo desde que el Eurosistema comenzó a recopilar dicha información en 2008. Esto se atribuye principalmente a la implementación de la Directiva sobre Servicios de Pago (PSD2), que incluye la autenticación reforzada de clientes (SCA) y estándares de comunicación abiertos, comunes y seguros, lo que revirtió la tendencia creciente del fraude de forma remota (*card-not-present fraud*). De hecho, datos recientes muestran que las tasas de fraude son aproximadamente diez veces mayores cuando la contraparte se encuentra fuera del Espacio Económico Europeo, donde la SCA no siempre se aplica.

2. ¿Qué tipologías de fraude afectaron a los consumidores en el país durante este período analizado?

Con el objeto de identificar las tipologías o modus operandi del fraude en medios de pago que afectan a los consumidores en Chile, se analizaron cuantitativa y cualitativamente cerca de 10.000 reclamos por fraude ingresados por los consumidores al SERNAC durante el año 2023, basándose en las descripciones provistas por los propios consumidores.

El análisis textual de cada reclamo permitió identificar tres patrones comunes en las descripciones de los consumidores:

i) **Casos de *Phishing*** (9,1% de los reclamos, N=900) Este tipo de fraude se caracteriza por el uso de técnicas de manipulación sofisticadas (ingeniería social) para obtener información del consumidor y su medio de pago. Dentro de esta categoría, se identificaron tres patrones específicos:
   a. Fraudes a través de llamadas fraudulentas (*vishing*, 6,4% del total, n=638)
   b. Fraudes mediante mensajes de texto o correos electrónicos (*phishing/malware*, 2% del total, n=198), y
   c. Fraudes a través del registro de compras o ventas fraudulentas (0,6% del total, n=64).

ii) **Casos de suplantación de identidad** (24,2% de los reclamos, N=2.396); A diferencia del phishing, este tipo de fraude se caracteriza por realizarse sin el conocimiento directo de la víctima. Los reclamos por suplantación de identidad describen fraudes originados por diversos mecanismos:
   a. Robo o pérdida de celular y/o documentos personales y bancarios (8.2% de los casos, n=807).
   b. Uso indebido de billeteras digitales (6% de los casos, n=590).
   c. Clonación de productos financieros (4.6% de los casos, n=456).
   d. Suplantación y apertura de productos financieros (*New Account Fraud*, 4.5% de los casos, n=449).

e. Portabilidad numérica fraudulenta (SIM *swapping*, 0.9% de los casos, n=94).

iii) **Desconocimiento General de Movimientos y/o Cobros** (66,7% de los reclamos, n=6.603): Esta categoría agrupa denuncias de cobros o transferencias bancarias no reconocidas por el titular, donde el texto del reclamo carece de información detallada para identificar un modus operandi específico de fraude.

El análisis de los datos de fraude revela patrones distintivos por género y rango etario:

- En todas las subcategorías de fraude, se observa una mayor incidencia en mujeres, destacando los casos de phishing, donde aproximadamente dos tercios de las víctimas son mujeres.
- Respecto a la edad, los fraudes de portabilidad numérica afectan principalmente a personas mayores, mientras que los jóvenes son más vulnerables al mal uso de billeteras digitales y a las compras o ventas fraudulentas.

En cuanto a las respuestas de los proveedores financieros a los reclamos:

- Las modalidades con mayor porcentaje de cierres favorables (reclamos aceptados total o parcialmente) son la "portabilidad numérica fraudulenta" (74%) y la "suplantación de identidad con apertura de productos" (63%).
- En contraste, los reclamos asociados al phishing presentan un menor porcentaje de cierres favorables, especialmente en "compra o ventas fraudulentas" (31%) y "llamadas fraudulentas" (36%).

Además, se observa que el phishing es más frecuente en productos bancarios, mientras que la suplantación de identidad (a través de "portabilidad numérica fraudulenta" y "apertura de productos por usurpación de identidad") predomina en productos de proveedores del retail financiero.

3. ¿Cuáles son las potenciales vulnerabilidades de seguridad que podrían facilitar la ocurrencia de fraudes?

a) Tecnología Dual-Tone Multi-Frequency (DTMF):

Las llamadas fraudulentas emplean la tecnología *Dual-Tone Multi-Frequency* (DTMF), la cual permite a los estafadores identificar los números digitados por la víctima. Dado que cada número se asocia a un sonido distinto, al ingresar la clave a través del teclado, el estafador puede descifrar la contraseña numérica de la víctima. Es imperativo que las campañas de las instituciones financieras informen sobre esta técnica en sus comunicaciones con sus clientes.

b) Filtración de datos personales:

Las acciones de *phishing* pueden resultar especialmente convincentes cuando incluyen datos personales y financieros del consumidor que, en principio, solo deberían ser conocidos por el emisor del medio de pago, tales como el nombre de su ejecutivo de cuentas o detalles de transacciones pasadas. Los accesos no autorizados a bases de datos personales de los consumidores financieros en poder de sus instituciones representan un alto riesgo de servir como fuente de información para futuras acciones de *phishing*. De hecho, aun cuando estas filtraciones de datos no impliquen el acceso a

las claves de seguridad de los consumidores, el conocimiento que proporcionan sobre el usuario aumenta la efectividad de las técnicas de engaño o ingeniería social.

c) Páginas WEB y Aplicaciones fraudulentas:

En Chile, los datos del CSIRT (equipo de respuesta ante incidentes de Seguridad Informática, dependiente del Ministerio del Interior y Seguridad Pública) y la CMF evidenciaron una creciente presencia del phishing en el mercado nacional.

El CSIRT, en 2023, emitió aproximadamente 700 alertas de phishing que se distribuían a través de sitios web, correos electrónicos y SMS fraudulentos. De estas alertas, el 40% correspondió a suplantación de bancos, el 34% a retail y el 15% a instituciones de gobierno. Notablemente, cerca del 47% de los casos bancarios fueron falsificaciones de Banco Estado.

Por su parte, la CMF, a través de su sitio de alertas ciudadanas, identificó en 2023:

- 16 sitios que ofrecían aplicaciones fraudulentas, algunas aún activas al momento del informe.
- 56 entidades que ofrecían créditos fraudulentos, operando vía web, WhatsApp y redes sociales (principalmente Facebook).
- 13 entidades que ofrecían inversiones online mediante páginas web y redes sociales.

Sin embargo, las plataformas en línea y los motores de búsqueda, como Google, permiten reportar sitios web fraudulentos, pero no pueden cerrarlos directamente. Esto se debe a que la clausura de una web implica un proceso legal y de jurisdicción que no siempre corresponde a estas plataformas. Sin embargo, la denuncia es crucial, ya que puede contribuir a que la página sea retirada de los resultados de búsqueda y a que las autoridades investiguen el caso.

d) Riesgo asociado a la pérdida, Robo o clonación de celulares:

El celular se ha convertido en un medio clave para la verificación de identidad en trámites digitales. El uso de códigos enviados por SMS para la autenticación de dos factores (2FA) o verificación de identidad es una práctica muy común y extendida en la mayoría de los servicios en línea. Además, el correo electrónico, accesible desde el celular por sincronización automática de aplicaciones, es otro medio de verificación. Sin embargo, el acceso no autorizado a un celular puede comprometer el correo si la sesión está abierta, no hay bloqueo de pantalla o la 2FA es vulnerable.
Las amplias funcionalidades de los teléfonos celulares si bien son ventajosas, implican riesgos significativos al ser una "entrada a tus datos personales". Los principales riesgos incluyen:

- Realización de compras no autorizadas.
- Clonación del número IMEI.
- Acceso a contraseñas e información de inicio de sesión.
- Hackeo de cuentas de correo electrónico y bloqueo de acceso.
- Violación de cuentas bancarias o aplicaciones de inversión.
- Hackeo de IDs de Google o Apple y eliminación de 2FA.
- Ejecución de estafas de *phishing* a contactos.
- Uso de fotos confidenciales para chantaje o extorsión.

e) Deficientes protocolos de autentificación de la identidad:

Portabilidad numérica fraudulenta o clonación de tarjeta SIM (SIM Swapping)
Este es un tipo de fraude en el que los delincuentes transfieren el número de teléfono de una víctima a una nueva cuenta o proveedor de servicios sin el consentimiento del titular o logran que se genere un duplicado de la tarjeta SIM al reportar un extravío o daño del celular. El objetivo es tomar control del número telefónico, el cual se utiliza como un medio de verificación de identidad, como se mencionó previamente. Los denunciantes de este tipo de estafas sostienen que existen escasas medidas de seguridad implementadas por las empresas de telecomunicaciones en la comprobación de identidad del solicitante. Esto se debe, argumentan, a que la portabilidad se realizó vía telefónica sin una verificación adecuada de la identidad del solicitante o porque no se cotejaron los datos personales aportados por el defraudador.

Suplantación de identidad y apertura de productos financieros (New Account Fraud)
Es un tipo de robo de identidad donde el estafador usa identidades robadas o fabricadas para abrir cuentas en nombre de otra persona. Esto puede incluir cuentas bancarias, tarjetas de crédito, préstamos, u otros productos financieros. La meta de este fraude es usualmente obtener un crédito o hacer compras bajo una identidad robada, dejando a la víctima con facturas y daño financiero potencialmente de largo plazo.

Acceso y mal uso de billeteras digitales
Durante el periodo de análisis de este estudio respecto del funcionamiento de las billeteras digitales, se evidenció que algunos proveedores utilizaban el número de teléfono o correos electrónicos registrados por el titular como principal medio de verificación, dado que a través de estos se podían recuperar diversas claves empleadas en las billeteras. Estos protocolos de seguridad podrían ser vulnerados mediante el robo del celular o la portabilidad numérica fraudulenta.

f) Riesgos asociados a la autentificación biométrica:

Como se mencionó previamente, algunos fraudes se originan por la debilidad en los controles de autenticación de identidad de los consumidores por parte de los proveedores financieros. Ante esto, la regulación ha avanzado en dos frentes clave: la promoción de una autenticación de identidad más robusta y la regulación de la protección y el tratamiento de los datos personales.

La autenticación reforzada del cliente (*Strong Customer Authentication*) es un procedimiento que requiere el uso de al menos dos factores de autenticación independientes de categorías diferentes, lo que significa que la vulneración de uno no compromete la fiabilidad de los demás. Estos factores se clasifican en:

- Conocimiento: Algo que solo el usuario conoce (ej., contraseñas o PIN).
- Posesión: Algo que solo el usuario posee (ej., token o mensaje a dispositivo registrado).
- Inherencia: Algo que el usuario es (ej., biometría facial, huella dactilar, o datos biométricos conductuales).

En el caso de los factores de inherencia, como la biometría facial, surgen dos importantes riesgos:

Protección de Datos Biométricos: La vulneración de datos biométricos genera un riesgo permanente, ya que, a diferencia de una contraseña, el rostro no puede "cambiarse". Una vez expuestos, estos registros pueden facilitar suplantaciones de identidad y otros usos ilícitos.

Spoofing/Deepfakes: La amenaza del spoofing persiste como un desafío significativo, dado que elementos como fotografías, videos, máscaras 3D o deepfakes pueden eludir los sistemas de detección si la capacidad de verificación de vivacidad (liveness detection) es insuficiente. La irrupción de la inteligencia artificial exacerba esta problemática. Un "deepfake" se define como contenido multimedia (videos, audios o imágenes) generado mediante inteligencia artificial (IA) con el propósito de manipular o falsificar la apariencia o voz de un individuo, simulando acciones o declaraciones que nunca ocurrieron.

4. En cuanto a las campañas de concientización, ¿logran informar adecuadamente sobre los riesgos que enfrentan los consumidores?

Las recientes modificaciones a la Ley N° 20.009 de Fraude establecieron la obligación de las entidades financieras de proporcionar a sus usuarios, de manera periódica, clara, accesible y actualizada, toda la información necesaria sobre medidas de seguridad e instrucciones para el uso seguro de los medios de pago, promoviendo así prácticas responsables. En este contexto, es conveniente que las campañas de educación y prevención del fraude se relacionen directamente con las experiencias de fraude sufridas por los consumidores en el país, como las descritas en este estudio.

Además, la normativa estipuló que los usuarios deberán informarse y adoptar todas las medidas necesarias para prevenir el uso indebido, el fraude u otros riesgos asociados a la utilización de los medios de pago y sus mecanismos de autenticación. Actualmente, las campañas de seguridad promovidas por instituciones financieras y reguladores constituyen el principal medio de información para las personas. En este sentido, se analizaron las campañas de prevención del fraude publicadas en los sitios web de 91 proveedores financieros durante abril y mayo de 2024 –mencionados en los reclamos de fraude de los consumidores durante el 2023–, evaluando su referencia explícita a las distintas modalidades de fraude identificadas en este estudio.

El análisis arrojó los siguientes resultados:

- **Baja Prevalencia y Enfoque Limitado de Campañas:** Solo el 18% (16 de 91) de las instituciones financieras analizadas mantenía campañas de seguridad disponibles en sus sitios web. Estas campañas se centraron principalmente en el *phishing*, con escasa o nula mención a otros tipos de fraude asociados a la suplantación.
- **Contenido Incompleto y Heterogéneo en Campañas de *Phishing*:** Aunque más del 80% de las campañas proporcionaba información sobre el tipo de fraude, cómo reconocerlo y medidas preventivas (de forma completa o parcial), solo el 25% explicaba el *modus operandi* en detalle. La mayoría de estas campañas omitía las consecuencias para las víctimas, los pasos a seguir en caso de ser estafado y la inclusión de ejemplos concretos de correos o SMS fraudulentos.

- **Interpretación Restrictiva de Mensajes Preventivos:** Los reclamos de consumidores de 2023 demuestran que mensajes como "nunca des tus claves ni contraseñas" son interpretados de manera limitada por los usuarios. Muchos entregan información (ej., códigos de verificación, datos de tarjeta) sin reconocer que están revelando datos sensibles, ya sea porque no los perciben como "la clave personal" o porque creen estar seguros al digitar la clave en el teclado del teléfono.
- **Falsa Sensación de Seguridad por Manejo de Datos Personales por parte del Estafador:** Las campañas de concientización no suelen transparentar que los estafadores pueden manejar información personal detallada de la víctima (nombre, RUT, número de cuenta, saldos, movimientos, productos bancarios, nombre de ejecutivos). Esta situación facilita el engaño y genera en la víctima una falsa sensación de estar interactuando con su banco, lo que sugiere una brecha entre la percepción de seguridad y una posible vulneración de datos bancarios.

El diagnóstico presentado en este informe busca contribuir a que los distintos componentes del ecosistema financiero –i.e. emisores, usuarios y supervisores- mitiguen el riesgo de fraude al consumidor.