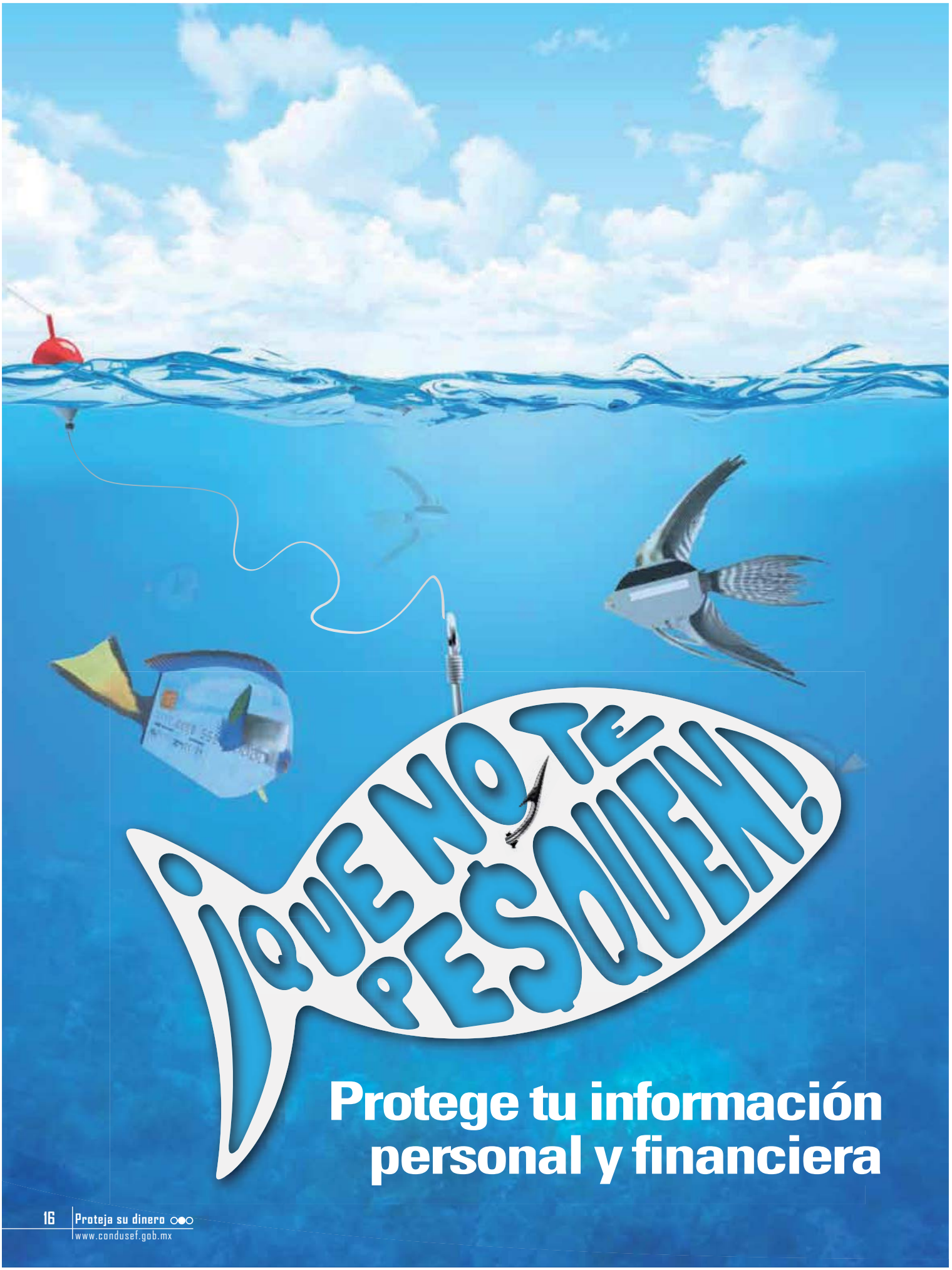


Protege tu información personal y financiera

En 2011 el monto reclamado por los usuarios ante la Condusef, relacionado con posibles fraudes con sus tarjetas de crédito y débito, transferencias electrónicas o cheques, ascendió a 476 millones de pesos y se estima que los bancos anualmente reembolsan 800 millones de pesos por cargos no reconocidos por el cliente. La clonación es un delito que ocasiona pérdidas tanto a usuarios como a instituciones financieras.

También conocida como *skimming*, la clonación consiste en copiar los datos que contiene la banda magnética de una tarjeta al deslizarla en un pequeño dispositivo llamado *skimmer*. La información se almacena para luego transferirla a una tarjeta nueva que los delincuentes usarán para hacer compras a tu nombre en establecimientos o por internet.

Contrario a lo que se podría pensar, este procedimiento es muy sencillo y no requiere de expertos en informática, toma segundos y sólo se necesita el *skimmer*, que cabe en la palma de la mano.

Esta práctica no sólo ocurre en México, sus dimensiones han alcanzado esferas internacionales, pues el crimen organizado viaja de un país a otro para no ser detectado. Si atendemos a los foros de usuarios, vemos que la mayoría de los reportes de clonación provienen de bares y restaurantes, tiendas comerciales o departamentales, hoteles y centros turísticos. Sin embargo, cualquier lugar es propicio para cometer el delito.

Tú como usuario de los servicios financieros y el banco como la institución que los oferta son corresponsables de la seguridad de los mismos. Veamos qué le toca hacer a los bancos.

¿Qué hacen los bancos?

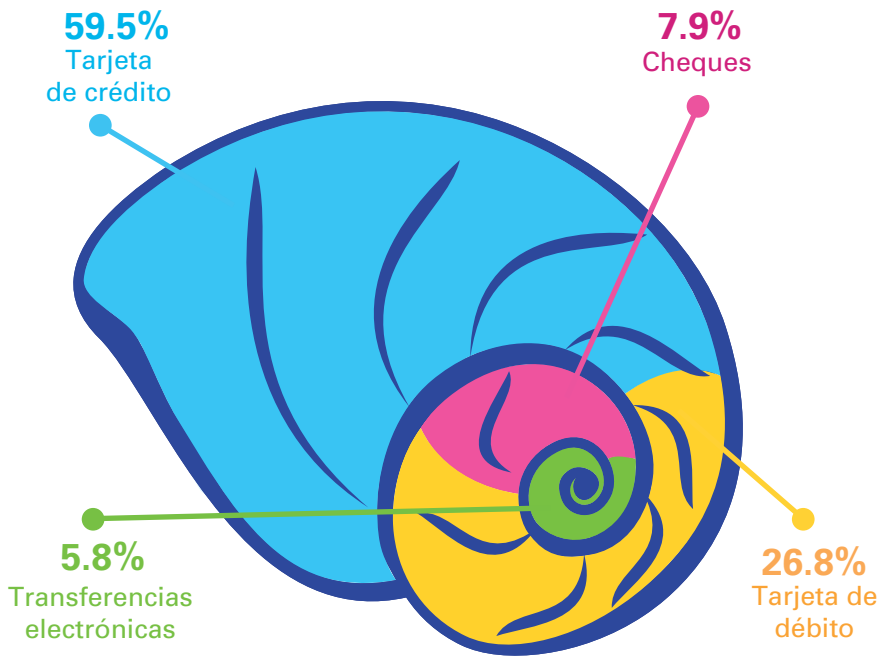
Las instituciones financieras tienen hasta diciembre de 2013 para migrar todos sus plásticos de banda magnética a *chip*. En ese lapso, también los lectores de tarjetas en puntos de venta, los cajeros automáticos y las cajas registradoras deberán haberse adaptado a esa tecnología. Esta obligación impuesta por la Comisión Nacional Bancaria y de Valores busca reducir prácticas fraudulentas, pues la tecnología del *chip* es más segura que la banda magnética. La información que guarda el primero, sólo puede ser descifrada por el banco, se activa únicamente con la clave personal del usuario (NIP), que sólo él conoce. Así, para completar una operación en un comercio será necesario que éste lo teclee, de lo contrario el pago no podrá ser completado. Si tu plástico aún no cuenta con el chip pregúntale a tu banco cuando realizará el cambio.

A partir de diciembre de 2013, los bancos deberán asumir el riesgo y por tanto los costos de las operaciones realizadas mediante el uso de tarjetas sin circuito integrado (*chip*) en cajeros automáticos o terminales punto de venta, que no sean reconocidas por los usuarios. Los montos deberán ser abonados a la cuenta del cliente a más tardar cuarenta y ocho horas posteriores a la reclamación[1].

1 Circular Única de Bancos, artículo 310, cuarto párrafo de la fracción III y Décimo Transitorio (DOF 27 de enero de 2010).

Cargos no reconocidos: posibles fraudes

(Quejas de los usuarios presentadas ante Condusef)



Fuente: Condusef.

Sistemas de pago en línea

Ante el aumento de amenazas en el comercio electrónico, hay empresas cuya labor consiste en ofrecer a sus clientes sistemas de pagos seguros. El más popular de estos servicios es *PayPal*. Cuando creas tu cuenta en su portal debes registrar los datos de tu tarjeta de crédito o débito para que se efectúen los cargos de las compras que realices en comercios que utilizan su plataforma de cobro. La ventaja es que ellos funcionan como intermediario, así no tienes que revelar tu información a cada uno de los comercios electrónicos donde compres. Pero el problema es que si compartes tus datos con estos servicios de pago, equivale a darle tu información a un tercero. Un defraudador podría apoderarse de tu cuenta de *PayPal* y realizar consumos no autorizados por ti.

Para estos casos, la empresa tiene previsto un proceso de reclamación donde notificas la compra que no reconoces a más tardar 60 días después de que se realizó el cargo. *PayPal* puede tardar el tiempo que quiera para hacer la investigación, pero si ésta demora más de 90 días te hará un abono provisional por lo reclamado. Cuando concluya la investigación te notificará el resultado: si la resolución es a tu favor, podrás conservar el depósito provisional. Pero si la resolución no te favorece te deberá informar por qué y en caso de que te hayan abonado algo te lo descontará de tu cuenta. Las autoridades mexicanas no podrán ayudarte a resolver esta situación pues este servicio no está regido por las leyes de nuestro país y opera bajo sus propias políticas y condiciones.

PayPal no está regido por autoridades mexicanas, éstas no podrán ayudarte en una controversia.

Si utilizas sistemas de pago en línea como *PayPal* cambia periódicamente tu contraseña, monitorea tu historial de pago (que aparece en su página) para cerciorarte que no se hayan realizado transacciones no autorizadas por ti, no olvides cerrar tu cuenta cada vez que dejes de utilizar el servicio y evita hacer compras en computadoras públicas.

Usuarios de *PayPal* también han sido víctimas del *phishing*, fraude que consiste en el envío de correos electrónicos que aparentan provenir de fuentes confiables (en este caso de *PayPal*) y buscan obtener información confidencial (datos personales como nombre completo, dirección de correo, contraseña y sobre todo datos de tu tarjeta de crédito) para cometer un fraude. Estos correos están perfectamente creados, utilizan logos y mensajes de notificación que hacen referencia a la institución. Si te llega un correo de esta naturaleza, fíjate en el saludo, normalmente empresas como *PayPal* se dirigen a ti por tu nombre y apellido, y no con un saludo general; desconfía si te solicitan información personal.

Con todo esto, muchas empresas de este tipo se han hecho famosas justamente por la experiencia que los usuarios han tenido con ellas y que comparten con otros a través de foros o *blogs*.

Otra forma de hacer compras en línea es directamente en la página del proveedor, por ejemplo las líneas aéreas te solicitan los datos de tu tarjeta para comprar un boleto de avión (el número de tarjeta, el nombre que aparece en ésta, la fecha de expiración y los

tres últimos dígitos de tu número de seguridad (CVV) impreso en la parte posterior de tu plástico). Al igual que los sistemas de pago, esta modalidad de compra tiene sus riesgos, sin embargo los proveedores de tarjetas de crédito *Visa* y *MasterdCard* han ideado un sistema de autenticación en línea para que tus compras sean más seguras. En la página 38 podrás encontrar más información sobre cómo opera dicho sistema.

Imágenes: Rodolfo Pastrana.

Implementa tus medidas

Toma precauciones para que no te pesquen, así la información de tu plástico no caerá en malas manos.

- Cuando la clonación se realiza en cajeros automáticos, además de robar la información de la banda magnética, los defraudadores buscan obtener tu Número de Identificación Personal (NIP). En esos casos, además de colocar el *skimmer* en la ranura donde ingresas tu tarjeta, ponen una microcámara apuntando al teclado para grabar tu NIP. Con estos dos elementos pueden retirar dinero de los cajeros automáticos hasta vaciar tu cuenta.

  Antes de hacer un retiro revisa que el cajero automático no cuente con dispositivos extraños en el lector de tarjetas, que no haya cámaras ocultas y de preferencia tapa con tu mano el teclado a la hora de capturar tu NIP.

- Procura que al pagar en un comercio, la transacción se realice siempre en tu presencia, y cuando te regresen la tarjeta verifica que sea la tuya. En los restaurantes o bares es común que se lleven tu tarjeta para pasarla por la terminal punto de venta, pide que te la lleven hasta tu mesa, si no es posible acude a pagar la cuenta directamente a la caja. No pierdas de vista tu plástico.

- Nunca apuntes tu NIP en tu tarjeta o lo guardes cerca de tu cartera o plásticos. No crees contraseñas con la fecha de tu cumpleaños o números consecutivos como 1234 o repetidos como 8888.

- No dejes tus productos financieros (cheques, tarjetas) en tu auto, al usar un *valet parking* te los pueden clonar.

Seguros contra fraude

Otra medida de seguridad que han implementado los bancos son los seguros contra fraudes en tarjetas de crédito y débito. En la mayoría de los casos se trata de un beneficio adicional que la institución ofrece gratuitamente y en otros tiene un costo. Normalmente ofrecen coberturas por:

Robo, extravío y clonación: protege el saldo de tu cuenta ante estos casos. Una vez que te des cuenta de lo ocurrido deberás dar aviso a tu banco. El periodo de la protección varía de acuerdo a cada institución, pero puede ir entre las 48 y 72 horas previas o bien posteriores a tu reporte.

Operaciones por internet: si alguien hace uso, sin tu autorización, de tu NIP o clave bancaria, *token* o tarjeta de seguridad que utilizas en tu portal bancario para hacer transferencias de fondos, el seguro te cubre por éstas.

Servicios de asistencia: a través de una sola llamada puedes bloquear todas tus tarjetas, también te dan asesoría legal telefónica.

Asistencia por robo de identidad: colaboran contigo y las autoridades para reportar los documentos oficiales extraviados, te proporcionan asesoría legal y gestión judicial y extrajudicial en caso de que hagan uso indebido de tus documentos oficiales.

Robo con violencia de cartera o bolso de uso personal: te cubre por el daño patrimonial que sufras en estos casos, así como los objetos personales. No ampara dinero en efectivo.

Para que te indemnicen en todos los casos, es necesario que te encuentres al corriente con los pagos de tu tarjeta.

Uso fraudulento de celular: te indemniza por el robo de tu teléfono móvil contratado en plan tarifario. Responde por las llamadas hechas, comúnmente durante las siguientes 24 horas al robo o previas hasta el momento del bloqueo del teléfono. Deberás entregar el estado de cuenta del plan tarifario para reclamar.

Estas coberturas te protegen por un número de eventos al año y por ciertos montos establecidos. Verifícalos en tu póliza, dentro de las condiciones generales del seguro.

Para que te indemnicen podría ser necesario que presentes la copia certificada de tu denuncia ante el Ministerio Público. Para los casos en donde el seguro te cubre tarjetas de otras instituciones financieras será necesario el reporte o solicitud de bloqueo del plástico ante el banco correspondiente.

Utilización forzada por terceros de tarjeta de crédito o débito: si eres obligado a retirar efectivo de un cajero automático, utilizando tu tarjeta de débito o crédito, el banco te reintegrará hasta cierto monto. Cuando la ofrecen, la cobertura puede ir desde que haces la primera disposición y hasta las 96 horas siguientes.

Protección de efectivo por retiro en ventanilla o cajero automático: si te asaltan al retirar dinero en un cajero automático o ventanilla, el banco te reintegra el monto de lo robado. Te puede amparar hasta las 96 horas a partir de que hayas realizado el retiro de efectivo.

Reporta de inmediato el siniestro, pues estos seguros te amparan por cierto periodo antes o después del siniestro. Si reclamas fuera de tiempo, no te cubrirán.

Si decides contratar un seguro de este tipo, no olvides preguntar por todas las coberturas y los montos por los que te hacen válido el seguro, así como las condiciones que aplican para cada caso.

Seguros de blindaje ¿Qué ofrece tu banco?

Revisa la protección con que cuenta tu tarjeta.

Crédito

Institución financiera	Protección que ofrece			Reclamación (Confirmación por escrito)	Cobertura	Costo
	Robo o extravío	Clonación o fraude*	Retención en cajeros			
AFIRME Clásica, Oro, Platinum, Blanc.	✓		✓	Dentro de los 90 días naturales posteriores a la fecha de corte.	Desde el momento en que se realiza la notificación telefónica.	Sin costo.
American Express Platinum Credit Card, Platinum Skyplus, Credit Card, The Gold Elite Credit Card.	✓	✓		• Robo o extravío: 90 días naturales, a partir de la fecha de corte. • Clonación: 90 días naturales posteriores a la fecha en que se haya realizado el cargo.	Durante las 48 horas previas al aviso telefónico.	Sin costo.
Banamex Clásica, B Smart, D Súper Tradicional, Travel Pass, Travel Pass Elite Level, Oro, Platinum.	✓	✓	✓	Máximo 10 días hábiles contados a partir de la fecha de aclaración o aviso telefónico.	Desde las 72 horas anteriores al reporte o notificación.	Sin costo. Existe un servicio opcional *LibraPlus* para robo en cajero automático (dos meses gratis, a partir del tercero tiene un costo de $92.80 mensual).
BBVA Bancomer Azul, Congelada, Educación, Oro, Platinum, Rayados, IPN, Visa Infinite.	✓		✓	Plazo de 90 días naturales a partir de la fecha de corte.	Desde el momento en que se realiza la notificación telefónica.	Sin costo.
Ban Bajío Clásica, Garantizada, Oro Internacional.	✓		✓	Plazo máximo de 10 días hábiles contados a partir de la fecha de aclaración o aviso telefónico.	Desde las 72 horas anteriores al reporte o notificación.	Sin costo.
Banorte Clásica, Oro, Oro Mujer Banorte, Platinum.	✓			Dentro de los 45 días naturales posteriores a la fecha de corte.	Cubre consumos o disposiciones de efectivo: • Básica: durante las 48 horas anteriores a la notificación telefónica. • Ampliada: durante las 72 horas anteriores a la notificación telefónica.	Cobertura básica: sin costo. Cobertura ampliada: (costo mensual): Clásica: $59 + IVA Oro: $90 + IVA Oro Mujer Banorte: $59 + IVA Platinum: $130 + IVA
HSBC Clásica, Oro, Platinum, Advance, Opción.	✓	✓		90 días naturales, contados a partir de la fecha en que se haya realizado el cargo.	En caso de robo o extravío cubre las transacciones realizadas durante las 48 horas previas al aviso. En caso de clonación no aplica ningún plazo.	Sin costo.

Débito

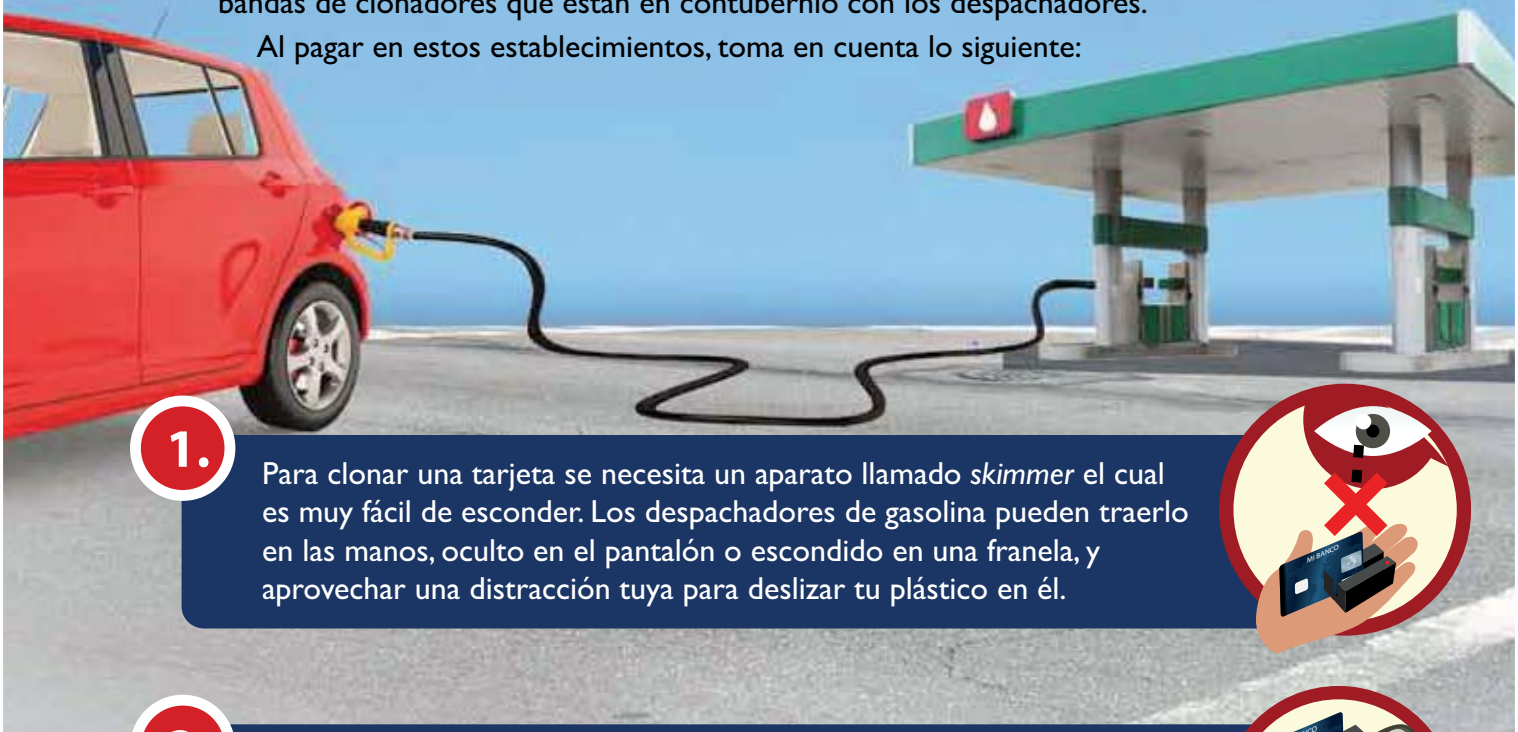
Institución financiera	Protección que ofrece			Reclamación (Confirmación por escrito)	Cobertura	Costo
	Robo o extravío	Clonación o fraude*	Retención en cajeros			
AFIRME Cuenta Juntadito SI.	✓			A más tardar el día hábil siguiente al reporte telefónico.	Desde el momento en que se realiza la notificación telefónica.	Sin costo.
Banamex Perfiles, Cuenta Maestra (Banamex, Opción y Profesionista) Invermático, Mi cuenta, Ahorro, Inteligente.	✓			De inmediato se deberá reportar telefónicamente para obtener un folio de aclaración y entregar la documentación requerida.	El programa *Débito Seguro Banamex* te cubre desde las 72 horas anteriores al reporte del robo o extravío. Dependiendo del tipo de cuenta la suma asegurada puede oscilar entre $5,000 y $100,000.	Sin costo.
BBVA Bancomer Libretón, Winner Card, Libretón con chequera, Blue Access, Versátil, Maestra Personas Físicas.	✓		✓	Plazo de 90 días naturales a partir de la fecha de corte.	Desde el momento en que se realiza la notificación telefónica.	Sin costo.
BANORTE EL BANCO FUERTE DE MEXICO Enlace Global, Enlace Dinámica Nómina, Enlace Tradicional sin chequera, Enlace Inteligente, Suma, Suma Menores, Suma Nómina, Suma Estudiantes, Banorte Fácil, Enlace Express.	✓	✓		Plazo de 90 días naturales a partir de la fecha de corte.	*Blindaje Banorte* brinda protección contra cargos fraudulentos por hasta 72 horas anteriores al reporte. El saldo queda protegido al momento de levantar el reporte hasta por $20,000 en cuentas de cheques y hasta por $10,000 en cuentas sin chequera.	Sin costo.
HSBC Nómina, Flexible, Flexible con chequera, Advance, Premier.	✓	✓	✓	Plazo de 90 días naturales a partir de la fecha de corte.	Desde las 72 horas anteriores a la notificación del evento. En caso de robo de cheques o de transferencias no autorizadas, el cliente tiene 20 días para dar aviso.	Sin costo.

Fuente: Registro de Contratos de Adhesión (Condusef).
Fecha de elaboración: marzo de 2012.
Nota: los seguros que no tienen costo vienen incluidos al abrir la cuenta.
*Falsificación de tarjetas titulares o adicionales, por ejemplo: robo de identidad.

¡Precaución en gasolineras!

Además de fijarte que la bomba marque ceros, al cargar combustible debes vigilar que no te clonen tu tarjeta. Se ha identificado que en algunos de estos sitios, operan bandas de clonadores que están en contubernio con los despachadores.

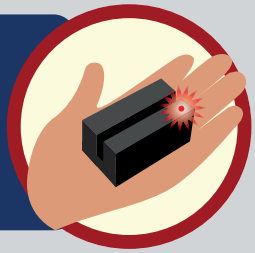
Al pagar en estos establecimientos, toma en cuenta lo siguiente:



1. Para clonar una tarjeta se necesita un aparato llamado *skimmer* el cual es muy fácil de esconder. Los despachadores de gasolina pueden traerlo en las manos, oculto en el pantalón o escondido en una franela, y aprovechar una distracción tuya para deslizar tu plástico en él.

2. Al pagar, no pierdas nunca de vista tu tarjeta, si te indican que tienen que llevársela a algún lugar apartado porque no cuentan con terminal inalámbrica diles que la llevarás personalmente.

3. Verifica que el despachador no cuente con algún dispositivo extraño debajo de la terminal (TPV) al hacer la operación. Algunos *skimmers* tienen un led o pequeño foco que parpadea al ser operado (así puedes detectarlos).



4. Cuando el despachador deslice tu tarjeta, pídele que de inmediato te la regrese, pues aprovechan el momento en el que estás firmando el *voucher* para hacer la clonación, anotar los números de tu tarjeta y el número de identificación (CVV) de la misma.

Dejarle a quien sea tu tarjeta sin tu supervisión es como entregarle tu cartera llena de dinero.

Infografía: Rodolfo Pastrana.