

SUPERINTENDENCIA DE BANCOS
Guatemala, C.A.

MODALIDADES DE LOS HECHOS DENUNCIADOS
DEPÓSITOS

TARJETA DE DÉBITO

Uso de tarjetas de débito sin autorización del cuentahabiente, el cual se origina porque las tarjetas han sido extraviadas y/o dejadas sin vigilancia al acceso de terceros no autorizados.

CHEQUES COBRADOS CON FIRMA DISTINTA A LA REGISTRADA

Las causas más comunes por la cuales se lleva a cabo esta irregularidad, son las siguientes:

1. Sustracción indebida mediante el procedimiento conocido como “Llanta Pinchada”.

Esta modalidad usualmente se lleva a cabo utilizando el procedimiento siguiente:

- a) El titular de una cuenta se presenta a la entidad bancaria a recoger su chequera.
- b) Al regresar al parqueo donde se encuentra su vehículo, observa que una de las llantas se encuentra pinchada, procediendo a reemplazarla.
- c) Los delincuentes, al menos 2, se acercan para brindar su ayuda.
- d) Uno de ellos distrae al cuentahabiente que está reemplazando la llanta y ha dejado su vehículo sin llave.
- e) El otro delincuente aprovecha para ingresar al vehículo a hurtarle varios cheques, que podrían ser los últimos, y en algunos casos sus documentos de identificación.
- f) Casi de inmediato, los delincuentes se dirigen al banco a cambiar los cheques hurtados.

SUPERINTENDENCIA DE BANCOS

Guatemala, C.A.

2. Chequeras dejadas a disposición de personas distintas a los titulares de las cuentas

Este caso se da típicamente por el descuido del cuentahabiente y la mala intención de una tercera persona de sustraer dinero de la cuenta de aquél. El proceso común es el siguiente:

- a) El titular deja a la vista, en la oficina o en su casa, y a disposición de un tercero su chequera.
- b) Ante la ausencia del titular, el tercero sustrae uno o más cheques. Esta persona por la relación con el titular, tiene acceso a la firma del cuentahabiente.
- c) El tercero simula la firma del titular de la cuenta y se presenta al banco.
- d) El banco hace efectivo el pago del cheque.

TARJETA DE CRÉDITO Y DÉBITO

CARGOS FRAUDULENTOS

1. Clonación de Tarjetas

Consiste en extraer los datos de la banda magnética de la tarjeta de crédito original para trasladarlos a otra tarjeta de crédito falsa y hacer uso de la misma. Para clonar una tarjeta se emplea una máquina con un chip que copia la información de la banda magnética de los plásticos, los cuales son trasladados a un computador e insertados en una nueva tarjeta de crédito.

SUPERINTENDENCIA DE BANCOS

Guatemala, C.A.

2. Cambio de tarjeta

Personas desconocidas se hacen pasar por promotores de crédito de la entidad emisora de la tarjeta, ofreciendo al cliente una tarjeta que les brindará mayores beneficios. Solicita la tarjeta del cliente para tomar datos, ésta es reemplazada por otra sin que el cliente se percate del hecho, posteriormente, y por lo general después del fraude, el cliente observa que la tarjeta que porta no es la suya.

3. Usurpación de identidad

Esta modalidad consiste en la obtención de datos personales o documentos falsos para ser utilizados en forma fraudulenta suplantando al usuario para obtener la tarjeta de crédito.

4. Retiros por cajero automático con tarjetas de crédito robadas

Sucede en los casos que el tarjetahabiente es asaltado y entre los documentos robados se encuentra la tarjeta de crédito y la información relacionada con el Número Personal de Identificación (PIN), con lo que el delincuente tiene acceso al PIN y al plástico de manera simultánea.

OTROS PROCEDIMIENTOS INDEBIDOS, DETECTADOS EN LAS QUEJAS Y/O GESTIONES

COPIA DE DATOS EN CAJEROS AUTOMÁTICOS (SKIMMING)

El Skimming Schemes, es otra variedad de fraude en el que se utiliza un aparato especial colocado en los cajeros automáticos por los delincuentes.

SUPERINTENDENCIA DE BANCOS

Guatemala, C.A.

Dicho dispositivo consiste en un lector de tarjetas.

El usuario utiliza su tarjeta para retirar dinero, consultar saldos, ver sus últimos movimientos, etc.

Al pasar la tarjeta por este lector, (SKIMMER), se copian los datos de la banda magnética. La clave de la tarjeta es obtenida a través de microcámara oculta que enfoca el teclado o touchscreen del cajero automático.

La filmación es enviada en forma inalámbrica a los delincuentes quienes normalmente se encuentran en un radio no mayor de 100 metros con alguna computadora portátil que recibe estos datos.

Una vez obtenidos el número de tarjeta (copiado de la banda magnética) y la contraseña del usuario se pueden duplicar las tarjetas, las cuales generalmente son usadas en forma inmediata.

SEGUROS

NO PAGO DE RECLAMO DE SINIESTROS

Se da en los casos siguientes:

1. Declaración falsa y/o inexacta al momento de la contratación del seguro.
2. Declaración falsa y/o inexacta de datos ocurridos en un siniestro.
3. La póliza se encuentra en el período de indisputabilidad.
4. La póliza se encuentra vencida por falta de pago.
5. La causa del siniestro está excluida de la cobertura.