TIENDAS VIRTUALES, PAGOS, SEGURIDADES
Concepto 2014073518-001 del 22 de septiembre de 2014

Sintesis: *La Circular Externa 042 de 2012 establece una serie de medidas encaminadas a fortalecer la seguridad y la calidad en el manejo de la información de los clientes y usuarios de las entidades vigiladas por la Superintendencia Financiera de Colombia, bien sea que acudan directamente a las oficinas, a cualquiera de los medios (tarjetas débito y crédito) o de los canales (cajeros automáticos, receptores de cheques, receptores de dinero en efectivo, datáfonos, sistemas de audio respuesta –IVR-, centros de atención telefónica -Call Center, Contac Center- sistemas de acceso remoto para clientes, Internet y dispositivos móviles) a través de los cuales éstas prestan sus servicios*

«(…) correo electrónico radicado en esta Superintendencia bajo el número arriba indicado, mediante el cual consulta *"(…) si es seguro registrar mi tarjeta de crédito en pay pal para realizar pagos; y si es seguro comprar desde Colombia en tiendas virtuales(…)"*.

Sobre el particular, proceden las siguientes consideraciones:

En primer lugar, debemos precisarle que (…) no es una empresa sujeta a la inspección, vigilancia y control de la Superintendencia Financiera de Colombia, según los registros que lleva este Organismo, razón por la cual no es posible pronunciarnos sobre su actividad y condiciones bajo las cuales opera, ni tampoco está dentro de las facultades atribuidas a esta Autoridad Administrativa, calificar las condiciones de seguridad bajo las cuales desarrolla su objeto social.

En este orden de ideas, a título meramente informativo, es preciso advertirle que si se trata de una tarjeta emitida por un establecimiento de crédito en Colombia, este Organismo ha impartido instrucciones a las entidades vigiladas sobre unos requerimientos mínimos de seguridad y calidad que deben cumplir para la realización de operaciones a través de los diferentes canales habilitados para la prestación de los servicios.

En efecto, en relación con las entidades que vigila esta Superintendencia, resulta pertinente anotar que cada institución goza de autonomía y libertad para adoptar los mecanismos de seguridad que, a su juicio y por virtud del profesionalismo y conocimiento de los riesgos que comporta la actividad que le es característica, estime suficientes para minimizar la ocurrencia de situaciones que afecten el normal desarrollo de sus operaciones o los intereses de sus clientes y usuarios.

Sin perjuicio de lo anterior esta Superintendencia, en desarrollo de sus facultades legales, ha expedido varios instructivos que propenden por la seguridad y calidad en el manejo de la información de los clientes a través de los diferentes medios y canales dispuestos por las entidades vigiladas para su atención.

La Circular Externa 042 de 2012 es la instrucción más reciente, en la cual se establecen una serie de medidas encaminadas a fortalecer la seguridad y la calidad en el manejo de la información de los clientes y usuarios de las entidades vigiladas por la Superintendencia Financiera de Colombia, bien sea que acudan directamente a las oficinas, a cualquiera de los medios (tarjetas débito y crédito) o de los canales (cajeros automáticos, receptores de cheques, receptores de dinero en efectivo, datáfonos, sistemas de audio respuesta –IVR-, centros de atención telefónica -Call Center, Contac Center- sistemas de acceso remoto para clientes, Internet y dispositivos móviles) a través de los cuales éstas prestan sus servicios.

Para su referencia, el texto completo de la Circular Externa 042 de 2012, se encuentra disponible en la siguiente dirección electrónica:
http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ce042_12.rtf

En el mismo sentido, como quiera que la responsabilidad al realizar el tipo de operaciones como la señalada en su consulta, es del tarjetahabiente, nos permitimos hacerle algunas recomendaciones de seguridad que usted podrá tener en cuenta en el momento de realizar transacciones a través de comercios electrónicos:

- No acceda desde sitios de Internet públicos o equipos de cómputo de los cuales no se encuentre seguro para realizar sus transacciones o actualizaciones de datos en el portal de su entidad bancaria o establecimientos de comercio donde usted deba suministrar información confidencial acerca de sus instrumentos financieros.

- Al ingresar al portal transaccional de su entidad financiera verifique que aparece el prefijo “https” y que en la parte inferior o superior del sitio se observe un “candado” cerrado. Esto puede aplicar para las pasarelas de pago que apoyaran su compra.

- Evite el suministro de información personal, claves y credenciales de acceso de los canales transaccionales a sitios de los cuales no se encuentre seguro.

- Indague acerca de las medidas de seguridad con las que cuenta la “pasarela de pago” que utilizara para realizar su transacción, al igual que, sobre el comercio electrónico con el cual se encuentra interactuando.

- Mantenga permanentemente actualizado el antivirus de su equipo de cómputo, esto evitara el ingreso de virus o “troyanos” que puedan acceder a su información personal.

- Con el fin de evitar “*phising*”: no responda correos electrónicos que hayan sido dirigidos para la solicitud de datos de sus cuentas bancarias, credenciales de acceso a sus portales o que soliciten la modificación de sus datos personales, estos normalmente son enviados por personas no ajenas al Banco que buscan aprovecharse de los consumidores financieros. En este caso comuníquese con su banco y verifique la validez del correo electrónico. Igualmente al recibir notificaciones de un correo electrónico desconocido no acceda a los links referenciados, ingrese directamente a la url (dirección Web) de su entidad financiera desde su navegador.

- Consulte las recomendaciones de su entidad financiera relacionadas con el manejo de los canales electrónicos, así podrá actualizarse acerca de las medidas de seguridad que puedan ofrecerle.

(…).»