SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Usuarios de tarjetas de crédito y débito recibirán mayor Protección ante cualquier operación fraudulenta.

- ***SBS pre publicó reglamento de tarjetas de crédito y débito a fin de reforzar medidas de seguridad de dichos instrumentos de pago.***
- ***Norma establece diversos plazos para que las empresas se adecúen a las nuevas disposiciones.***

Lima, 26 de marzo de 2013.- La Superintendencia de Banca, Seguros y AFP (SBS) pre publico el proyecto de Reglamento de Tarjetas de Crédito y Débito el mismo que tiene por finalidad reforzar las medidas actualmente vigentes sobre expedición, administración y seguridad en el uso de dichos instrumentos de pago.

La norma que estará a disposición del público para sus sugerencias en la página web de la SBS hasta el próximo 22 de abril, precisa las medidas de seguridad que deberán ser aplicables a las tarjetas de crédito y de débito. Así, se señala, entre otros puntos, que las tarjetas deberán contar con un circuito integrado o chip que permita almacenar y procesar información del usuario y sus transacciones, cumpliendo estándares internacionales de interoperabilidad para el uso y verificación de las tarjetas así como para la autenticación de pagos.

Al respecto, el reglamento señala que las empresas deberán aplicar las siguientes medidas:

- Reglas de seguridad definidas en el chip de las tarjetas que deben ser utilizadas para verificar la autenticidad de la tarjeta, validad la identidad del usuario mediante el uso de una clave o firma u otros mecanismos de autenticación.
- Aplicar procedimientos criptográficos sobre los datos críticos y claves almacenadas en el chip de las tarjetas, así como sobre aquellos existentes en los mensajes intercambiados entre las tarjetas, los terminales de punto de venta, los cajeros automáticos y las empresas emisoras.
- En caso las empresas emisoras permitan la autorización de transacciones fuera de línea, deben de aplicar un método de autenticación de datos que brinde adecuadas condiciones de seguridad sin afectar la calidad y el rendimiento del servicio provisto al usuario.
- Establecer límites por transacción según el perfil de riesgo del usuario y aquellos que permitan restringir el número de transacciones consecutivas procesadas fuera de línea.

En cuanto a las medidas de seguridad relativas al usuario, la propuesta establece que las empresas deberán adoptar como mínimo las siguientes precauciones:

- Entregar la primera clave o número secreto de la tarjeta obligando a su cambio antes de realizar la primera transacción.
- Otorgar a los usuarios la opción de contar con un servicio de notificaciones que les informe de todas las transacciones realizadas con sus tarjetas, inmediatamente después de ser registradas por la empresa mediante mensajes de texto a un teléfono móvil y/o correo electrónico, entre otros mecanismos que puedan ser pactados con los usuarios.
- Poner a disposición de los usuarios la posibilidad de comunicar a la empresa que realizarán operaciones con su tarjeta de crédito desde el extranjero, antes de la realización de estas operaciones con su tarjeta de crédito.

La norma también prevé medidas de seguridad respecto al monitoreo y realización de operaciones, para lo cual se establece que las empresas deberán adoptar como mínimo las siguientes medidas:

- Contar con sistemas de monitoreo de transacciones que tengan como objetivo detectar aquellas transacciones que no corresponden al comportamiento habitual de consumo del usuario.
- Implementar procedimientos complementarios para gestionar las alertas generadas por el sistema de monitoreo de transacciones.
- Identificar patrones de fraude mediante el análisis sistemático de la información histórica de las transacciones, los que deberán incorporarse al sistema de monitoreo de transacciones.
- Establecer límites y controles en los diversos canales de atención que permitan mitigar las pérdidas por fraude.
- En el caso de operaciones de retiro, depósito o disposición en efectivo, según corresponda, u otras con finalidad informativa como información sobre las transacciones realizadas u otra similar, deberá requerirse la clave secreta del usuario, en cada oportunidad, sin importar el canal utilizado para tal efecto.

Adicionalmente se prevén medidas exigibles a las empresas sobre gestión de seguridad de la información y de continuidad del negocio, así como aquellas que deben tener en cuenta los negocios afiliados.

Transacciones fraudulentas

Con relación a las transacciones que pudieran corresponder a patrones de fraude, el proyecto establece que las empresas deberán contar con procedimientos para la atención de estas acciones, los que deberán incluir cuando menos mecanismos para la comunicación inmediata al usuario sobre posibles fraude así como las acciones para proceder con el bloqueo temporal o definitivo de la tarjeta, en caso sea necesario.

Precisa también que ante el rechazo de una transacción o el reclamo por parte del usuario de que esta fue ejecutada incorrectamente, las empresas será responsable de demostrar que las transacciones fueron autenticadas y registradas. Al respecto señala que los registros asociados a la transacción no son suficientes para probar que el usuario autorizó la transacción o que actuó de manera fraudulenta o negligente.

Indica también que el usuario no es responsable de ninguna pérdida en los siguientes casos:

- Transacciones realizadas luego de que la empresa fuera notificada del extravío, sustracción o uso no autorizado de la tarjeta o de la información que la contiene.

- Cuando las fallas en el sistema de la empresa impiden la recepción y/o registro de la notificación realizada por parte del usuario, respecto a la pérdida o sustracción de la tarjeta.
- Cuando las tarjetas hayan sido objeto de clonación.
- Por el funcionamiento defectuoso de los canales o sistemas puestos a disposición de los usuarios por las empresas para efectuar operaciones.
- Por la manipulación de los cajeros automáticos o los ambientes en que estos operan, así como los terminales de puntos de venta.
- Cuando se haya producido suplantación del usuario.
- En el caso de transacciones realizadas luego de la cancelación de la tarjeta o cuando esta haya expirado.

Otras medidas

La norma establece también que las empresas deberán otorgar a los usuarios la opción de contar con un servicio de notificaciones que les informe de todas las transacciones realizadas con sus tarjetas, inmediatamente después de ser registradas por la empresa, mediante mensajes de texto a un teléfono móvil y/o correo electrónico, entre otros mecanismos que pueden ser pactados con los usuarios. Las empresas deberán contar con sistemas de monitoreo de transacciones, que tengan como objetivo detectar aquellas transacciones que no corresponden al comportamiento habitual de consumo del usuario.

De igual forma, se modifica el contenido mínimo de los estados de cuenta a fin de otorgar información adicional a los usuarios. Así el estado de cuenta debe incluir el monto mínimo de pago, conforme a la circular de pago mínimo, debiéndose desglosar el monto que será utilizado para el pago principal, los intereses, comisiones y cualquier otro concepto aplicable conforme a la circular mencionada. También se debe incluir la tasa de interés compensatorio efectivo anual aplicable a cada consumo o transacción bajo modalidad revolvente o cuotas fijas, así como la tasa de interés moratorio efectivo anual o penalidad por incumplimiento aplicable a la fecha del estado de cuenta.

Cabe precisar que el reglamento en su tercera disposición final, establece los plazos máximos de adecuación que deberán cumplir las empresas para adaptarse a las diferentes disposiciones legales contenidas en la presente propuesta.

Gerencia de Comunicaciones e Imagen Institucional