LA PERICIA EN TARJETAS DE CREDITOS

UNA INCUMBENCIA INTERDISCIPLINARIA

Y EL FRAUDE INFORMÁTICO EN EL FUERO PENAL

AUTORES: DR. MIGUEL ANGEL GARCÍA CAMACHO
DR. DANIEL BENJAMÍN CIMA
DR. RODOLFO FABIÁN SANCHEZ
DR. CARLOS MARÍA FERNÁNDEZ
Y con la Colaboración Especial de:
CRISTIAN BASUALDO

FACULTAD DE CIENCIAS ECONÓMICAS Y ESTADÍSTICAS
UNIVERSIDAD NACIONAL DE ROSARIO

RESUMEN:

El presente trabajo tiene por objeto, en primer lugar, abordar un tema muy específico como es el caso de las Pericias Contables en Tarjetas de Crédito. Luego de una pequeña introducción al tema de Tarjetas, se pretende el tratamiento de temas que sean de utilidad para el Profesional en Ciencias Económicas, por ejemplo: cómo responder a los ítems periciales contables, que generalmente, y por desconocimiento, están formulados incorrectamente.

En segundo lugar el objetivo es destacar que hoy en día, con la mera actuación del Contador Público, no es suficiente, ya que es una materia de incumbencia interdisciplinaria, requiriéndose, en muchos casos, de la actuación de un Perito en Informática.

Y por último pretendemos tratar un tema de actualidad como es el del Fraude Informático, en sus distintas formas, teniendo en cuenta la reciente sanción de la Ley N° 26.388 que viene a cubrir un vacío legal que existía en la materia.

LA PERICIA EN TARJETAS DE CREDITOS
UNA INCUMBENCIA INTERDISCIPLINARIA
Y EL FRAUDE INFORMÁTICO EN EL FUERO PENAL

CONCEPTOS GENERALES

Cuando hablamos de tarjetas de créditos tenemos que entender que se trata de las múltiples relaciones que involucran a un administrador del sistema, a un emisor, a un titular y sus adicionales y a un proveedor de bienes o servicios. Puede que una misma persona cumpla más de un de esta funciones. Está regido por la ley N° 25065, los Decretos 15/99 y 1387/01 y modificada por la Ley 26.010.
También supletoriamente se aplican las normas del Código Civil y Comercial de la Nación y la Ley de Defensa al Consumidor (Ley 24.240)

Quizás para ver la importancia que tiene hoy en nuestra sociedad este sistema, solo debemos recordar que hoy en la argentina existes solo tres medios de pagos difundidos:

- El dinero fiduciario
- El cheque
- Las tarjetas

Solo deberíamos agregar que hoy las empresas están obligadas a pagar el salario de sus empleados a través de Cajas de Ahorro abiertas en bancos y que estos le suministran a estas personas tarjetas de débitos para que puedan extraer dinero a través de los cajeros automáticos o realizar compras por medio de estas en comercios adheridos al sistema, casi siempre a través de un sistema de tarjetas de créditos.

Tal es así, que la ley define que el sistema de Tarjetas de Créditos es un CONJUNTO complejo y sistematizado de contratos individuales cuya finalidad es:

- Posibilitar compras o locaciones de bienes o servicios u otras
- Obtener préstamos y anticipos de dinero del sistema en comercio o instituciones adheridas
- Diferir el pago
- Financiarlo conforme a las modalidades establecidas en el contrato
- Abonar a proveedores de bienes o servicios en los términos pactados

Quienes participan.

a) Emisor: puede ser una entidad financiera, una entidad bancaria o una entidad comercial. Puede ser una tarjeta de compra y crédito o de débito (solo para las entidades financieras)
b) Titular de la tarjeta: quien solicitó la tarjeta y es el responsable de todos los cargos o consumos, que realice el personalmente o a través de adicionales que el autorice. Serían los usuarios de la misma.
c) Proveedor o comercio adherido: quien proporciona los bienes o servicios al usuarios de la tarjeta, aceptando percibir el importe mediante este sistema de pago.

d) Administrador del sistema: Es quien le da la marca, y quien administra y conoce todo el procedimiento administrativo y comercial del sistema.

En la actualidad podemos hablar de dos sistemas de tarjetas: Cerrado y Abierto.

SISTEMA CERRADO DE TARJETAS

Es evidente que este sistema de tarjetas de créditos es el que tiene una menor complejidad operativa, fruto básicamente de las menores alternativas que le brinda al usuario. Para identificarlo más claramente, lo podemos asociar a las tarjetas que emiten las grandes tiendas o supermercados.

Básicamente es también una tarjeta de compra y crédito, y por ende está alcanzada por las mismas leyes al principio expuestas.

En primer término la Administradora, la Emisora y el Comercio es la misma entidad.

Pues al no haber banco que la emita y como está destinado básicamente a que los consumos se realicen en establecimientos de la emisora, la complejidad del sistema se simplifica.

También podemos mencionar en este aspecto que al no participar en el sistema nacional de pagos, la complejidad de cajeros, débitos automáticos, transacciones internacionales, etc. evitan la complejidad y los riesgos asociados al Sistema de Tarjeta Abierto que a continuación se describe.

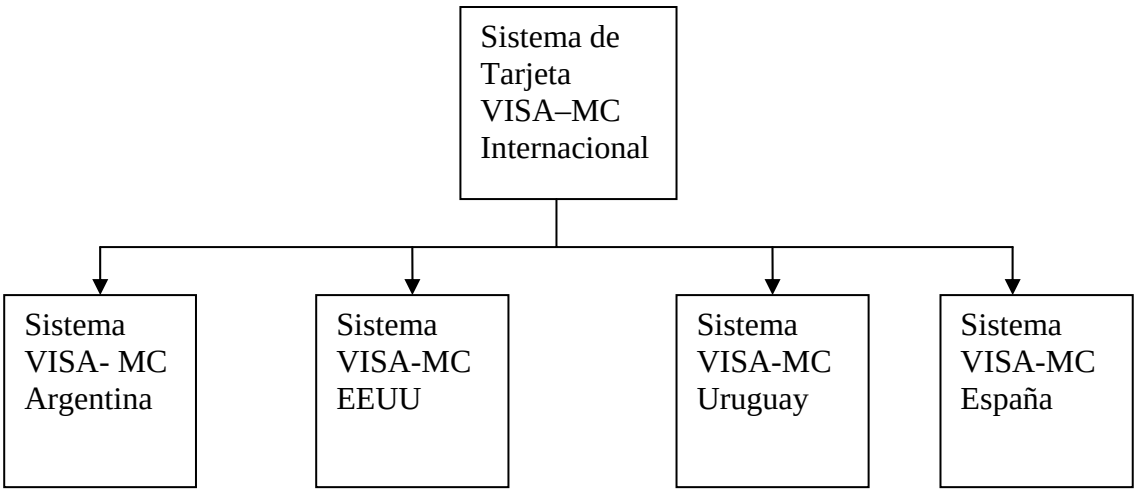
SISTEMA ABIERTO DE TARJETAS

En la actualidad es el más difundido, y cuando pensamos en un sistema de tarjeta de créditos automáticamente lo asociamos a una marca, como por ejemplo pueden ser VISA – MASTER CARD – AMERIAN EXPRESS , etc. etc.

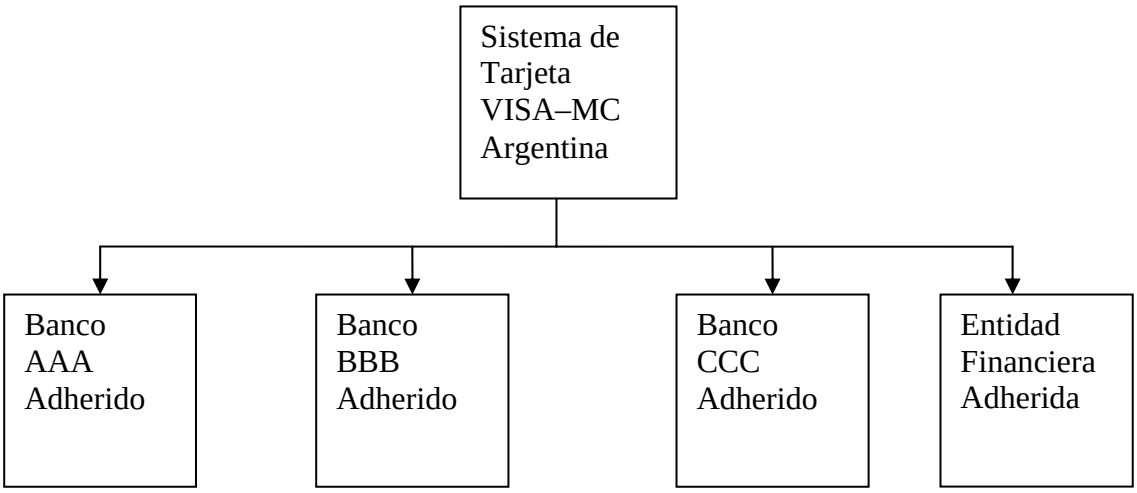
Este sistema es administrado por estas empresas, que a diferencia de un sistema cerrado, no se vinculan directamente con el titular de la tarjeta ni con el comercio adherido, sino que lo hacen a través de entidades financieras, y que como son internacionales, sus sistemas operan de esta forma en casi todo el mundo, a través de sus sistemas financieros, que emiten tarjetas y adhieren a comercios y proveedores de servicios.

Este sistema opera con un sistema supra nacional que interconecta todos los sistemas de cada país en el que opera. De esta forma permite que cualquier tarjeta de créditos emitidas en una país, pueda operar en otro, encargándose de compensar las respectivas divisas a través de los

respectivos bancos centrales Sistema Sistema



Hasta aquí vemos el diseño del sistema de interconectado internacional, pero para operar necesita que cada sistema "nacional" opere efectivamente emitiendo los plásticos y realizando operaciones.



A su vez cada entidad opera como EMISORA de tarjetas de créditos y como vinculante de comercios y proveedores de servicios que se adhieran el sistema

Cuando la entidad emisora de la tarjeta de créditos (Ej. Banco AAA) le entrega el plástico a un titular y a sus adicionales o beneficiario de extensiones, automáticamente le abre un crédito y un sinnúmero de posibilidades para operar, no solo con los comercios o proveedores que el mismo banco tiene como clientes, sino de TODO el sistema nacional e internacional si "el plástico" entregado tiene estas características.

También puede retirar efectivo (obteniendo un crédito o haciéndolo debitar de sus cuentas de depósitos que tiene abiertas en el mencionado banco) de cualquier cajero de la red que se le indique e incluso de redes internacionales, o incluso de comercios con los cuales tenga establecidos estos servicios.

Aquí debemos pensar que las tarjetas emitidas por un banco son muchísimas, al igual que los comercios que adheridos al sistema operan con esta entidad financiera.

El banco emisor se hace responsable frente al sistema de los consumos o retiros de efectivo que la tarjeta emitida por el, realice en cualquier cajero o establecimiento de cualquier lugar del mundo donde halla cajeros habilitados o comercios adheridos.

Es evidente que el hacerse responsable es atender en tiempo y forma los consumos que sus tarjetas emitidas consuman o retiren en efectivo.

Pero la entidad emisora, que le otorgó un crédito al titular de la tarjeta, no sabe lo que su cliente está retirando o consumiendo en cualquier cajero o comercio adherido, pues el no tiene esta información.

¿Quién la tiene? Evidentemente es la ADMINISTRADORA del sistema quien tiene todos estos datos a través de los respectivos bancos, a través de los cuales, los proveedores de servicios, comercios adheridos o redes de cajeros automáticos le informan que determinada tarjeta ha consumido o retirado determinado importe.

¿Quién autoriza estos retiros o consumos?

También es evidente que la administradora, que tiene en su conocimiento los límites asignados por el emisor, es la encargada de distribuir estos límites a toda la red, tanto se de cajeros automáticos, como comercios o proveedores de servicios adheridos al sistema.

En consecuencia, la única que posee todos los datos, de limites asignados, impugnaciones, transacciones realizadas, etc. es la ADMINISTRADORA DEL SISTEMA. Rápidamente podemos concluir que es la única en condiciones de emitir los respectivos resúmenes de estados de las cuentas.

En síntesis, vemos que la ADMINISTRADORA es la que maneja el sistema.

Los bancos o entidades financieras cumplen el rol de emisores de tarjetas, asumiendo el riesgo crediticio de sus clientes, y adhiriendo a los comercios o proveedores de bienes y servicios para que a través de ellos perciban el dinero que el sistema les envía para atender estas ventas realizadas.

El SISTEMA administra el CLEARING entre las entidades participantes, que a través del consumo o retiros de efectivo que sus tarjetas emitidas realicen deben enviar los fondos para pagarles a los proveedores o comercios adheridos, y viceversa, del dinero que recibe del sistema para acreditarle en las cuentas de sus comercios adheridos clientes por el consumo que tarjetas de créditos del sistema realizaron en sus establecimientos.

Si estos consumos corresponden a entidades del exterior, son los bancos centrales de los respectivos países que realizan el pedido de compensación de las divisas que permitan pagarle al comercio proveedor con los fondos que emite el usuario que realizó el consumo.

Si son del país, estas compensaciones se realizan entre entidades a través del SISTEMA NACIONAL DE PAGOS que compensa en las cuentas que las entidades financieras tienen abiertas en el BCRA

Con esta breve síntesis del sistema, quizás ahora comience la operatoria y las dificultades y vulnerabilidades que la misma tiene.

En primer lugar sabemos que han desaparecido en la práctica los denominados "cupones", con lo cual basta observar en supermercados, estaciones de servicios, tiendas, restaurants, la utilización del POSNET

Aquí el medio escrito se reemplaza por un disparo electrónico, y comienzan muchísimos nuevos aspectos a considerar en caso de operaciones que pueden llegar a ser conflictivas por dolo o errores.

Todos sabemos que el robo de identidad es cada vez mas preocupante en una sociedad cada vez mas digitalizada, y aquí nos encontramos con que una tarjeta hoy opera en compras en internet, en cajeros automáticos, en compras en comercios, etc.

También sabemos que el titular de la cuenta, se daría por notificado de este hecho cuando recibe el respectivo resumen que la entidad financiera le envía una vez que lo emitió la administradora.

El plazo de impugnación del mismo por parte del titular es de 30 días de recibido, detallando claramente el error atribuido y aportando todo dato que sirva para esclarecerlo.

Pero si la impugnación no tiene aceptación se abre una etapa donde el cuestionamiento sin duda pasará a la acción judicial y esta deberá dilucidar a quién le asiste el derecho.

Nos enfrentamos a diversas situaciones difíciles de dilucidar y que requieren una intervención Interdisciplinaria

Sabemos que los datos de identidad, además de poder ser robados en una transacción realizada vía internet, también lo puede ser cuando se realizan operaciones a través de un cajero automático.

También vemos a diario que las compras con POSNET tienen una frecuencia y habitualidad que relajan los controles por parte de quienes lo operan en cuanto a la necesidad de identificar a quien realiza la transacción.

Los delitos informáticos han hecho aparecer también verdaderas redes de especialistas en esta materia, lo cual lleva a que las posibilidades de ilícitos sean cada vez más difíciles de detectar.

Todo lo expuesto hace que, hoy día y en estos casos, sea imprescindible un trabajo interdisciplinario; ya no basta con la participación del Contador como Perito, sino que éste requiere del auxilio de la prueba informática la que tendrá que ser relevada por un experto en la materia.

Lo expresado precedentemente es uno de los objetivos del presente trabajo, que con el objetivo de demostrar en hechos fácticos lo descripto, aunó los conocimientos de un Contador especialista en el tema de Entidades Financieras –Profesor de la U.N.R.-Carrera de Contador: Práctica Profesional: Bancos- (Dr. García Camacho), de Contadores con experiencia como Peritos de Oficio (Dr. Cima y Sánchez), de un Perito Contador Oficial (Dr. Fernández), y de la colaboración de Cristian Basualdo por su amplia experiencia como Perito en Informática, sobre todo en el tema de delitos informáticos, y docente del Instituto Superior de Educación Policial (I.S.E.P.).

INCUMBENCIAS DEL PERITO EN INFORMÁTICA EN RELACIÓN CON LA TARJETA

Hoy en día la filosofía de las tarjetas de crédito es la que venimos describiendo. Como se dijo anteriormente podemos desplazarnos a distintos sitios sin necesidad de llevar dinero, aunque el desplazamiento sea hasta la tienda más cercana. Ese documento, la tarjeta, garantiza al comerciante el cobro de la operación a través del emisor de la misma.

Hoy en día la identificación telemática es compleja, y este es el principal problema que tienen los usuarios de las tarjetas: no existe conciencia de la importancia de la validación personal a la hora de utilizar la tarjeta de crédito.

En una tarjeta de crédito existen varios sistemas de seguridad, que en muchos casos pasan desapercibidos por los usuarios. Los más utilizados son tres conjuntos de números que deben mantenerse en secreto (sobre todo el PIN, o número de identificación del usuario).

La seguridad 100%, como siempre, es imposible de alcanzar. Por muchos sistemas de seguridad que se empleen, siempre existirá la posibilidad de que nos “copien” la tarjeta mediante un lector de bandas magnéticas, o muchas otras amenazas cada vez más complejas. Dentro de estas amenazas, sin duda las que están produciendo cada vez más perjuicios para los usuarios son las relacionadas con el uso masivo de tarjetas de crédito para compras por Internet.

Cada vez que tecleamos nuestros códigos de identificación para comprar algo en Internet, esos códigos viajan por la Red y pueden ser interceptados por usuarios maliciosos. Para ello, existen varias maneras de capturar electrónicamente los datos:

Man-in-the-middle (hombre en el medio). Mediante esta técnica, el ladrón de los datos intercepta la comunicación entre el usuario y el sitio web real, actuando a modo de proxy. De esta manera, es capaz de escuchar toda la comunicación entre ambos. Para que tenga éxito, debe ser capaz de redirigir al cliente hacia su proxy en vez de hacia el servidor real. Existen diversas técnicas para conseguirlo, como por ejemplo los proxies transparentes, el DNS Cache Poisoning o envenenamiento de Caché DNS (Domain Name Server, Servidor de Nombres de Dominio) y la ofuscación del URL.

- Aprovechamiento de vulnerabilidades de tipo Cross-Site Scripting en un sitio web, que permiten simular una página web segura de una entidad bancaria, sin que el usuario pueda detectar anomalías en la dirección ni en el certificado de seguridad que aparece en el navegador.

- Aprovechamiento de vulnerabilidades del navegador en el cliente, que permiten mediante el uso de exploits falsear la dirección que aparece en el navegador. De esta manera, se podría redirigir el navegador a un sitio fraudulento, mientras que en la barra de direcciones del navegador se mostraría la URL del sitio de confianza. Mediante esta técnica, también es posible falsear las ventanas pop-up abiertas desde una página web auténtica.

- Algunos ataques de este tipo también hacen uso de exploits en sitios web fraudulentos que, aprovechando alguna vulnerabilidad, permiten descargar troyanos de tipo keylogger que robarán información confidencial del usuario.

- Otra técnica más sofisticada es la denominada Pharming. Se trata de una táctica fraudulenta que consiste en cambiar los contenidos del DNS ya sea a través de la configuración del protocolo TCP/IP o del archivo lmhost (que actúa como una caché local de nombres de servidores), para redirigir los navegadores a páginas falsas en lugar de las auténticas cuando el usuario accede a las mismas a través de su navegador. Además, en caso de que el usuario afectado por el pharming navegue a través de un proxy para garantizar su anonimato, la resolución de nombres del DNS del proxy puede verse afectada de forma que todos los usuarios que lo utilicen sean conducidos al servidor falso en lugar del legítimo.

Pero cualquiera de estos sistemas de robo de datos necesitan de una capacidad técnica de programación y de conocimientos que no siempre están al alcance de todo el mundo. Así que lo más sencillo para conseguir los datos de una tarjeta de crédito es engañar directamente al usuario, mediante la técnica llamada “phishing” Esta técnica consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

A pesar de este desolador panorama, las tecnologías actuales han evolucionado lo suficiente como para evitar la salida de un ordenador de determinados datos. Al igual que se puede prevenir la entrada de virus en un sistema analizando la información entrante, se puede vigilar la información saliente para evitar que los usuarios, en un descuido, puedan equivocarse.

El robo de información personal en un ordenador, tan peligroso cuando son datos sobre bancos, puede ser evitado. Si los usuarios instalan suites de seguridad completas, efectivas e inteligentes, ningún número secreto caerá en manos de usuarios remotos. Ahora solamente queda guardar la tarjeta en un lugar seguro: como alguien dijo, “No busques en la tecnología soluciones a la seguridad física”.

Y, Si a pesar de las seguridades, el sistema fuese engañado, en todos estos casos descriptos, será la prueba informática la que tendrá que ser relevada por un experto en la materia.

EL PROFESIONAL EN CIENCIAS ECONÓMICAS Y LOS PUNTOS PERICIALES REQUERIDOS

Independientemente de los puntos que les sean requeridos en los expedientes, quizás el primer planteo sea si estos lo están en forma correcta o no, y a quién debe requerir la información: Si a la entidad Emisora de la Tarjeta o al Administrador del Sistema, que es el otro objetivo del presente trabajo.

Muchas veces observamos que por desconocimiento o por querer forzar una respuesta técnica para fundar un reclamo, los puntos periciales son absolutamente confusos y muchas veces pueden inducir a un error al pretender responderlos.

En primer lugar si debemos responder sobre los registros contables, debemos atender a que tipo de tarjeta de crédito estamos compulsando.

En un sistema abierto, es una entidad financiera quienes al emitir una tarjeta "bancan" y asumen el pago o el compromiso de realizarlo. Este crédito acordado será ejecutado por el titular o autorizados que con el "plástico" concurra a un proveedor de bienes o servicios o retire dinero.

En los registros contables de esta entidad estará asentado como una operación de crédito los pagos que el sistema le informa por clearing que debe hacer.

Pero tiene que quedarle claro al perito que el banco es muy improbable que "pague los cupones de los consumos", pues los comercios pueden estar adheridos a cualquier banco e incluso puede provenir de retiros de cajeros automáticos de cualquier red o país.

Incluso los cupones físicos han casi desaparecidos frente al sistema electrónico de pago que todos los comercios contratan. Mediante este sistema no solo obtienen la autorización para la venta, sino que simultáneamente la informan al sistema y dentro de los plazos estipulados le serán acreditados los fondos en la cuenta del banco mediante el cual están adheridos al sistema

Conclusión:

El banco atiende los clearing, NO PAGO LOS CONSUMOS DIRECTAMENTE a los comercios adheridos.

Por consiguiente su contabilidad solo refleja los movimientos contables de estos clearing.

En la cuenta Deudores por tarjetas de créditos están los importes que "la entidad financiera" a través de los clearing ASUME como emisora de la tarjeta y otorgante del crédito por compras y adelantos de efectivo otorgado al titular de la misma.

Si al Profesional en Ciencias Económicas se le requiriera que opine sobre los orígenes de las operaciones que figuran en el resumen y se le reclaman al titular, debe el profesional conocer que quien las genera y donde las realiza, son de conocimiento exclusivo del administrador. Este autoriza al negocio o al cajero automático a realizar la transacción.

Por consiguiente, si los puntos requeridos versan sobre los "consumos realizados" u "operaciones que figuran en el resumen" quien conoce estos y por ende confecciona el resumen de cuenta, **es la ADMINISTRADORA. Prueba de ello es que en caso de robo o extravío de la tarjeta, a quien debe avisarse inmediatamente es a la ADMINISTRADORA.**

Si además se lo consultara para que verifique los cupones o los consumos, aquí tendría que consultar a la administradora que medio se utilizó. Si el mismo es electrónico, el origen de las operaciones NO TENDRAN CUPONES FÍSICOS, sino transacciones electrónicas realizadas por el comercio adherido o el cajero electrónico utilizado.

Por esto, además de los libros y registros contables del emisor (entidad financiera en el caso de un sistema abierto) o entidad administradora (emisora en el caso de un sistema cerrado), deberá completar con la documentación respaldatoria y con el complemento de otros profesionales en el caso de que se requiera su participación (profesionales en informática y comunicaciones), a lo cual ya nos hemos referido como uno de los objetivos del presente trabajo.

Cuando hablamos de elementos respaldatorios, el principal a tener en cuenta por el profesional en ciencias económicas es el **Resumen de Cuenta (Confeccionado por la administradora y emitido por la entidad financiera)**

De el obtendrá todos los datos básicos necesarios, como consumos, adelantos, pagos realizados, tasas de interés aplicadas etc.

Es fundamental saber si se encuentran impugnados movimientos o el resumen mismo en tiempo y forma.

Para ello deberá requerir a las partes que les suministren estos elementos, pues en caso de no estar, se dará como válidos los mismos.

CONCLUSIONES FINALES SOBRE EL PROFESIONAL EN CIENCIAS ECONÓMICAS Y LOS PUNTOS PERICIALES REQUERIDOS:

Es casi imposible saber como se realizarán los puntos periciales en el caso particular de las tarjetas, pues la controversia puede ser desde consumos impugnados, intereses cuestionados, costos, comisiones, etc.

Es fundamental para el profesional en Ciencias Económicas saber quienes son las partes intervinientes y que papel juega cada una:

ADMINISTRADORA – EMISORA – TITULAR DE LA TARJETA – COMERCIO ADHERIDO.

Conocer si existe cuestionamiento o impugnación de la liquidación o resumen por el titular, dentro de los 30 días de recibida la liquidación (o resúmen)

A partir de allí podrá requerir la documentación respaldatoria y las registraciones contables al partícipe correspondiente.

LEY N° 26.388 (SOBRE DELITOS INFORMÁTICOS)

En Junio de este año en curso se sanciono en nuestro país la Ley de Delitos Informáticos N° 26.388.

La ley sancionada, **penaliza el accionar de hackers, estafadores digitales y pornógrafos en Internet**. La nueva norma también protege el correo electrónico y otras comunicaciones de esta época como el chat, además de los sistemas de almacenamiento de datos públicos, de empresas de servicios y financieros. A continuación se mencionan algunos artículos de dicha ley.

ARTICULO 1º — Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:

El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

ARTICULO 4º — Sustituyese el artículo 153 del Código Penal, por el siguiente:
Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

ARTICULO 5º — Incorporase como artículo 153 bis del Código Penal, el siguiente:

Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

ARTICULO 8º — Sustituyese el artículo 157 bis del Código Penal, por el siguiente:
Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

ARTICULO 9º — Incorporase como inciso 16 del artículo 173 del Código Penal, el siguiente:
Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

ARTICULO 10. — Incorporase como segundo párrafo del artículo 183 del Código Penal, el siguiente:

En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Ayer era casi total la desprotección por el vacío legal que existía; hoy, con la sanción de la ley 26388, se han receptado y tipificado en nuestro Código Penal conductas criminosas como las descriptas, dando respuesta a la problemática específica derivada del uso indebido de las nuevas tecnologías de la información y de las comunicaciones. Tampoco se tienen dudas de que los bienes y derechos seguirán estando a merced de los delincuentes informáticos, pero es una buena noticia saber y tener presente que acciones como abrir y conocer el contenido de un e-mail ajeno, dañar o ingresar de manera indebida en las bases de datos, los daños a los sistemas informáticos serán castigadas por el Código Penal. De aquí en más, cuando muchos delincuentes aprieten el "enter", se queden mirando la pantalla de la computadora y digan: "¡Listo, hoy terminé!" se preguntarán: "Terminé... ¿o recién empecé?".