UNIVERSIDAD NACIONAL DE INGENIERIA

Facultad de Ingeniería Industrial y de Sistemas

" FRAUDE EN TRANSACCIONES POR INTERNET CON TARJETA DE CREDITO".

INFORME DE SUFICIENCIA

Para Optar el Titulo Profesional de:

INGENIERO DE SISTEMAS

MATOS PEREZ, ALFREDO MANUEL

LIMA - PERU

2005

AGRADECIMIENTO

Olga y Alfredo, por estar siempre conmigo

INDICE

1.ANTECEDENTES

2. MARCO TEORICO

3. PROCESO DE TOMA DE DECISIONES

DESCRIPTORES TEMATICOS

- Tarjeta de Crédito
- Fraude
- Banca
- Internet
- VISA
- E-Comerme
- CrediBank

RESUMEN EJECUTIVO

A inicios del 2001 se confirmó, la tendencia del año anterior, del incremento de pago por seguros mediante transacciones fraudulentas con Tarjeta de Crédito en un Banco Líder del país. Este incremento llegó a superar el tope mensual de seguros por fraude previsto normalmente, en vista de que los reclamos por consumos no reconocidos de sus clientes eran totalmente válidos. En la mayoría de los casos, se trataba de transacciones de compra realizadas fuera de la red local y el cliente no había participado en la operación. Se trataba de autorizaciones que en su mensajería indicaban provenir del punto de servicio llamado correo y teléfono, el cual es usado por algunos adquirentes para enviar transacciones realizadas en Internet y en muchos casos tenían como origen haber sido realizadas desde Estados Unidos y Venezuela.

Esto motivó la inmediata acción del Banco de Crédito que conformó un equipo de trabajo entre usuarios y personal de sistemas y quienes plantearon como solución una serie de acciones especificas siendo la principal la adecuación del software de tarjetas de crédito – por el éxito de su impacto - para lograr prevenir estas transacciones fraudulentas. Esta adecuación se definió para 3 horizontes:

- En el corto plazo, se pondría en funcionamiento por mes aproximadamente la aplicación de algoritmos que identifiquen las transacciones fraudulentas durante el proceso de autorizaciones. Esta estrategia es el sustento de este informe.

- En el mediano plazo, en los próximos seis meses con la integración de una herramienta de monitoreo que permita construir alarmas en función de información diaria e histórica.
- En el largo plazo, en el próximo año, con la adquisición de algún paquete de software especializado en identificar comportamientos de segmentos de cliente a través de redes neuronales.

La estrategia de corto plazo fue instalada en el mes de Febrero del 2001 y luego de realizar algunos ajustes a nivel de parámetros del software permitió rápidamente identificar las transacciones fraudulentas mediante la denegación directa de la autorización o indirecta a través del sistema de referidos. Esto originó que las organizaciones de fraude dejaran de operar con las tarjetas del Banco Líder y de ese modo se empezó a recuperar no solo los fondos perdidos sino la tranquilidad de los clientes.

Finalmente, tras el análisis y solución del problema se concluyó que el fraude, al igual que la delincuencia organizada, nunca se rinde y siempre buscan nuevas formas de ataque. Por ello el Banco decidió revisar permanentemente las estrategias de corto, mediano y largo plazo así como el compromiso de evaluar el éxito de su aplicación mes a mes.

INTRODUCCIÓN

El objetivo del trabajo es demostrar que el uso de las Tecnologías de Información y una eficiente respuesta de un organización puede ser muy valiosa ante los retos actuales ocurridos a partir de los Negocios Electrónicos por Internet.

Los logros del presente trabajo nos han podido evidenciar:

- Que la explosión en el uso de Internet ha requerido que las organizaciones cambien sus reglas, tecnologías y procedimientos.
- Que en todo proceso de maduración, la transformación de los modelos empresariales es por partes y de forma diferente para cada empresa.
- Que es muy importante que las organizaciones preparen y conformen equipos de trabajo de modo que tengan el conocimiento adecuado del E-Commerce[1], la tecnología asociada y las formas en que estas tecnologías se pueden adaptar y alinear a la organización.

Finalmente debo manifestar que la principal limitación del trabajo fueron las restricciones de confidencialidad del Banco Líder, ya que como en cualquier institución financiera, alguna de la información numérica y algorítmica ha sido restringida

[1] E-Commerce o Comercio Electrónico. Conjuntamente con el E-Processes conforman el E-Business de las organizaciones.

CAPITULO I

ANTECEDENTES

Diagnóstico estratégico

Hoy en día, muchas de las transacciones comerciales se realizan a través de diferentes medios de pago electrónicos, siendo el de mayor uso las Tarjeta de Crédito.

Los actores que intervienen en el negocio de Tarjeta de Crédito para completar una compra son los siguientes:

- El Comprador, cliente o tarjetahabiente
- El Vendedor, usualmente un Establecimiento Comercial o un Cajero Automático
- El Emisor (Issuer) de la tarjeta que presenta el cliente y en el que reside la cuenta a cargar. Usualmente es un banco.
- El Adquirente (Acquirer), que es la entidad que en nombre del vendedor recibe la transacción y donde reside la cuenta a la que se hará la liquidación de pago. En nuestro caso, para las transacciones locales en el Perú para la marca VISA, el adquirente es VISANET[2] y para la marca American Express podemos considerar para fines de este caso a ExpressNet[3].

[2] VISANET es el nombre comercial de la empresa Compañía Peruana de Medios de Pago.

[3] ExpressNet es una empresa formada por el Banco Líder y el otro Banco emisor de la Tarjeta AMEX. Si bien la adquirencia de las transacciones locales corresponde al Banco en el cual está afiliado el Establecimiento Comercial, los temas de la liquidación, selección de establecimientos, capacitación y seguimiento de los mismos corresponden a ExpressNet.

- La Red de Medios de Pagos (Schema) que en nuestro caso son VISA International -con sede principal en Miami- y American Express Global Network Services (AEGNS) –con sede principal en Phoenix- y que sirven como regulador e intermediario entre los actores mencionados

Por lo tanto, en el tema de Fraude corresponde tomar acción en la prevención, detección y corrección tanto al Emisor como del Adquirente. El presente informe muestra el caso de un Banco en su rol de Emisor.

Fortalezas y Debilidades

Las fortalezas del Banco Líder, en cuanto a su rol de Emisor de Tarjetas de Crédito son:

- Posición de Mercado, es el primer banco emisor de Tarjetas en el medio, llegando a tener aproximadamente 150,000 tarjetas VISA y 30,000 tarjetas American Express.
- Imagen de solidez, le permite mantener su gran participación en los mercados de depósitos y colocaciones, manteniendo el 30% de su participación en ambos casos
- Uso de tecnología, el Banco ha demostrado iniciativa en invertir en tecnologías nuevas y mejorar las existentes. El portal ViaBCP ha sido un portal de vanguardia en el país, sin embargo el tema de la seguridad es un tema que trasciende al banco por lo que el E-commerce no ha podido ser potenciado en el mismo.
- Equipo de trabajo, el contar con una organización grande (mas de 5,000 empleados en planilla) le permite armar equipos de profesionales altamente competitivos y que están constantemente capacitados.

Las debilidades del Banco Líder, en cuanto a su rol de Emisor son:

- Toma de decisiones, su organización jerárquica a veces no le permite tomar decisiones fluidas debido a sus diversos niveles de aprobación

- Alto volumen de tarjetas, siendo éste un indicador apetitoso para cualquier organización de fraude
- Procedimientos rígidos. Por lo general, el Banco no ha innovado proactivamente sus procedimientos de trabajo, sino por el contrario lo ha hecho de modo reactivo debido fundamentalmente a su tamaño

Oportunidades y Riesgos

Las oportunidades del Banco Líder, en cuanto a su rol de Emisor son:

- Anticiparse a olas mayores de Fraude y obtener know-how en el tema para combatirlo, es decir prepararse en estrategias contra el fraude
- La recesión. El impacto financiero del fraude es fácilmente demostrable en los resultados de la empresa, lo que en un entorno de recesión, exige a la Gerencia General tomar decisiones rápidas y efectivas.

Los riesgos que tiene el Banco Líder, en cuanto a su rol de Emisor son:

- Debe mantener una continuidad operativa para su alto volumen transaccional, es decir cualquier modificación a los sistemas debe ser realizado con un nivel de calidad optimo en su resultado y tiempo de respuesta
- No existe legislación ni jurisprudencia completa sobre el tema del fraude. Si bien VISANET tiene un Departamento de Fraude que eventualmente coordina y apoya a los emisores, no existe un esfuerzo a nivel nacional y menos gubernamental al respecto.
- Afrontar el problema de la seguridad y confidencial pues en Internet el uso de la Tarjeta de Crédito no es un medio de pago totalmente seguro. Esto inclusive ha dado origen a esfuerzos como el Proyecto SET de VISA pero sin éxito en el país por consideraciones de costos.

Diagnóstico funcional

Productos

Los Productos involucrados son tarjetas de crédito bancarias de las marcas VISA y American Express.

Las Tarjetas de Crédito son productos que acceden a una línea de crédito del tarjetahabiente. Localmente operan a través de la red de poco más de 10,000 establecimientos VISANET y de los cuales aproximadamente el 90%[4] cuentan con maquinas POS[5].

En el caso de VISA corresponden a los siguientes tipos de tarjetas :

- CrediBank Clásica: tarjeta de crédito estándar
- CrediBank Oro: tarjeta de crédito VIP[6]
- CrediBank Empresarial: tarjeta de crédito dirigida a empresas
- CrediBank Clásica Mobil: tarjeta de crédito estándar asociada[7] a Mobil Co.
- CrediBank Oro Mobil: tarjeta de crédito VIP asociada a Mobil Co.

En el caso de American Express corresponden a los siguientes tipos de tarjetas:

- Tarjeta American Express : tarjeta de cargo estándar
- Tarjeta American Express Gold: tarjeta de cargo VIP

[4] El 10% restante no tiene una máquina de POS pues la relación costo-beneficio no la justifica, dado su bajo volumen de ventas.

[5] P.O.S. o Point of Sales, que significa Punto de Ventas

[6] VIP o Very Important Person

[7] Asociación con fines de fidelizar a los clientes

ñ Tarjeta de Crédito American Express : tarjeta de crédito estándar

En estos 3 casos corresponden a productos bi-moneda, es decir que presentan facturaciones paralelas en Soles y US Dólares según sean los consumos realizados.

Clientes

A excepción de la tarjeta CrediBank Empresarial, los clientes impactados son Personas Naturales de los segmentos alto y medio del mercado. En el caso de CrediBank Empresarial, los clientes son empresas medianas, grandes y corporaciones aunque los tarjetahabientes son los propietarios y ejecutivos de sus empresas .

En el caso de Personas Naturales los clientes por lo general tienen otros productos bancarios, típicamente cuentan al menos con una cuenta de depósito, en las que se le realiza el cargo mensual facturado por los consumos en Tarjeta de Crédito.

En el caso de Personas Jurídicas, los clientes cuentan con una línea de financiamiento parte de toda una Propuesta Crediticia en diferentes líneas de crédito aprobada por el Banco. Cada empresa en coordinación con su Funcionario de Negocios y en base jerarquías, funciones y otras consideraciones distribuyen el importe de la línea de crédito en tarjeta de crédito entre sus ejecutivos y accionistas.

Debe mencionarse que los clientes pueden realizar sus consumos en cualquier establecimiento afiliado a VISA o American Express, según sea el caso, tanto en el Perú como en el extranjero, en cualquier punto de servicio autorizado e identificado con los logos respectivos.

Desde el punto de vista de la seguridad, el cliente cuenta con lo siguiente:

- Número de Identificación Personal o PIN[8], el cual se exige típicamente en las transacciones de Cajeros Automáticos.

- Número de Verificación de Tarjeta o CVV1[9] para VISA o CSC[10] para AMEX, el cual está grabado en la banda magnética de la tarjeta. Por simplicidad llamaremos CVV en adelante a estos dos términos.
- En el caso de VISA, se tiene un segundo Número de Verificación de Tarjeta o CVV2, el cual es visible en la parte posterior de la tarjeta y cuyo objetivo es que sea usado en transacciones donde no hay lectura de banda.

Proveedores

Entre los principales proveedores del producto Tarjeta de Crédito tenemos a:

- GEMPLUS, HOGIER GARTNER, TRANSTEX: Fabricantes de los plásticos
- DataCard y NBS: Es la plataforma de producción que permite grabar los plásticos (embossing)
- Hermes: Es la empresa de seguridad encargada de la distribución de las tarjetas
- Enotria: Es la empresa proveedora de la papelería e impresiones.
- PaySys: Es el proveedor del software Vision Plus del Sistema de Tarjeta de Crédito

[8] P.I.N. o Personal Identification Number

[9] C.V.V. o Card Verification Value

[10] C.S.C. o Card Security Code

Procesos

Tanto las marcas VISA como American Express trabajan de modo estándar a nivel mundial con los siguientes procesos centrales:

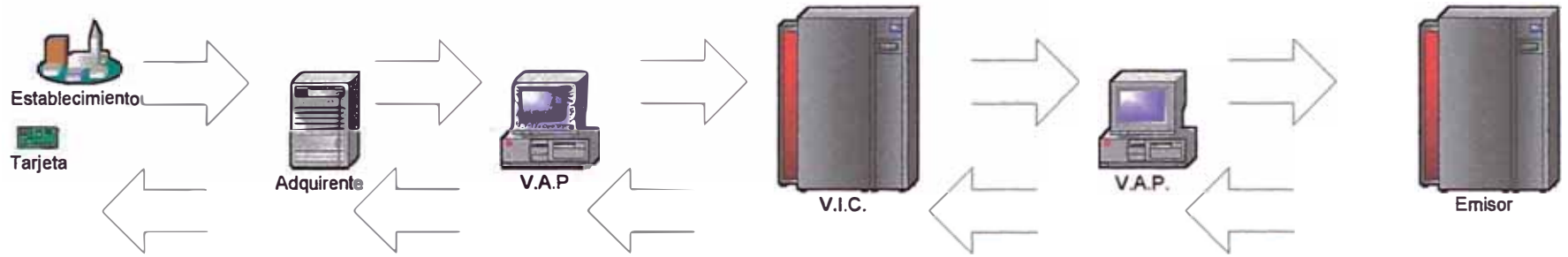
1. Autorización, es cuando el emisor aprueba o declina una transacción de venta antes que la compra sea terminada o el dinero en efectivo entregado.
2. Clearing es cuando la transacción es entregada del adquirente al emisor para su cargo en la cuenta del tarjetahabiente.
3. Settlement es el proceso de calcular y determinar la posición financiera neta de cada miembro participante para todas las transacciones entregadas.

Describiremos el proceso de Autorizaciones que además de ser el que inicia el negocio, es el motivo de este informe. Para ello seguiremos paso a paso el caso normal para una Autorización y descrito de una manera simple para el caso de VISA:

1. La transacción se inicia cuando una tarjeta es:
   - Insertada en un ATM o,
   - Su banda magnética es capturada por un POS, o
   - Sus datos son ingresados en un terminal para POS

   Según sea el caso, el dispositivo de ingreso exigirá el ingreso del PIN

2. El establecimiento crea entonces un mensaje de solicitud de autorización y lo envía al adquirente. El pedido incluye el tipo de transacción, el nombre del establecimiento, el PIN encriptado (si se hubiera requerido) y el importe de la transacción



RED DE COMUNICACIONES
VISANET

REQUEST

RESPONSE

3. El adquirente graba un log de este pedido, excluyendo la información del PIN, y envía el mensaje a la red VISA.

4. VISA registra la transacción, realiza las conversiones de moneda si se requiriesen, y rutea el mensaje al Emisor. El ruteo se basa en el numero de la tarjeta y en opciones de ruteo que haya definido el Emisor.

5. El emisor verifica el PIN, cheque el importe de la transacción contra el saldo disponible de la cuenta (Open to Buy) y realizar chequeos de limites de actividad diaria y otros controles que tuviera definido. El emisor registra la transacción y si la aprueba, retiene los fondos o reduce la disponibilidad de la cuenta del tarjetahabiente por el importe de la compra. El emisor crea un mensaje de respuesta a la autorización basado en los resultados de todos estas ediciones y controles y lo envia de regreso a la red VISA.

6. VISA registra el mensaje y lo envía al Adquirente
7. El adquirente registra la respuesta y la direcciona al establecimiento para completar la transacción. El adquirente se asegura que la respuesta se entregó con éxito. Si al tarjetahabiente no se le requirió el ingreso de PIN, entonces se le requerirá su firma.

Típicamente a la respuesta de autorización en el mundo de Tarjeta de Crédito pueden existir 3 opciones :

- Aprobar la solicitud de autorización
- Denegar la solicitud de autorización
- Referir la solicitud de autorización, que consiste en un mecanismo que por alguna razón de negocios exige que se llame al establecimiento para verificar la información del cliente.

Es importante indicar que no solo el Emisor puede resolver la solicitud de una Autorización. También pueden responder:

- El Adquirente, en el caso que el Emisor y el Adquirente hayan elegido la opción Límite de Piso.
- La Red Visa, en el caso que:
  - El Emisor no este disponible
  - El Emisor lo haya solicitado
  - Transacciones Internacional de Viajeros

Igualmente las funciones de verificación de PIN y CVV pueden ser realizadas por VISA si el Emisor así lo decidiera.

Complementariamente al Proceso de Autorizaciones, existen los procesos propios de banco que en este caso se agrupan en:

- Aprobación del Crédito, que consiste en la presentación, evaluación y decisión de las solicitudes de crédito que presentan los clientes
- Emisión de Plásticos, que consiste en el proceso de producción de grabación de plásticos con los estándares que los partners VISA y American Express exigen
- Distribución de Plásticos, que consiste en el envío de las tarjetas e información asociada según elección del cliente, a oficinas del Banco o alguna dirección en particular. En ambos casos se realiza esta mensajería a través de un Servicio de Mensajería de Valores de la empresa Hermes.

Organización de la Empresa

El Departamento de Fraude pertenece al Servicio de Atención al Cliente del Area de Operaciones Centrales del Banco y reporta a la Gerencia General Adjunta. Este departamento es el encargo de prevenir, detectar y corregir las

transacciones de Fraude que se realizan en los diversos productos bancarios siendo el principal involucrado el de Tarjeta de Crédito.

El Departamento de Tarjeta de Crédito VISA, pertenece al Area de Marketing que reporta a la División de Banca Personal y ésta a su vez a la Gerencia General. Su función es promover y mantener el uso de los productos VISA.

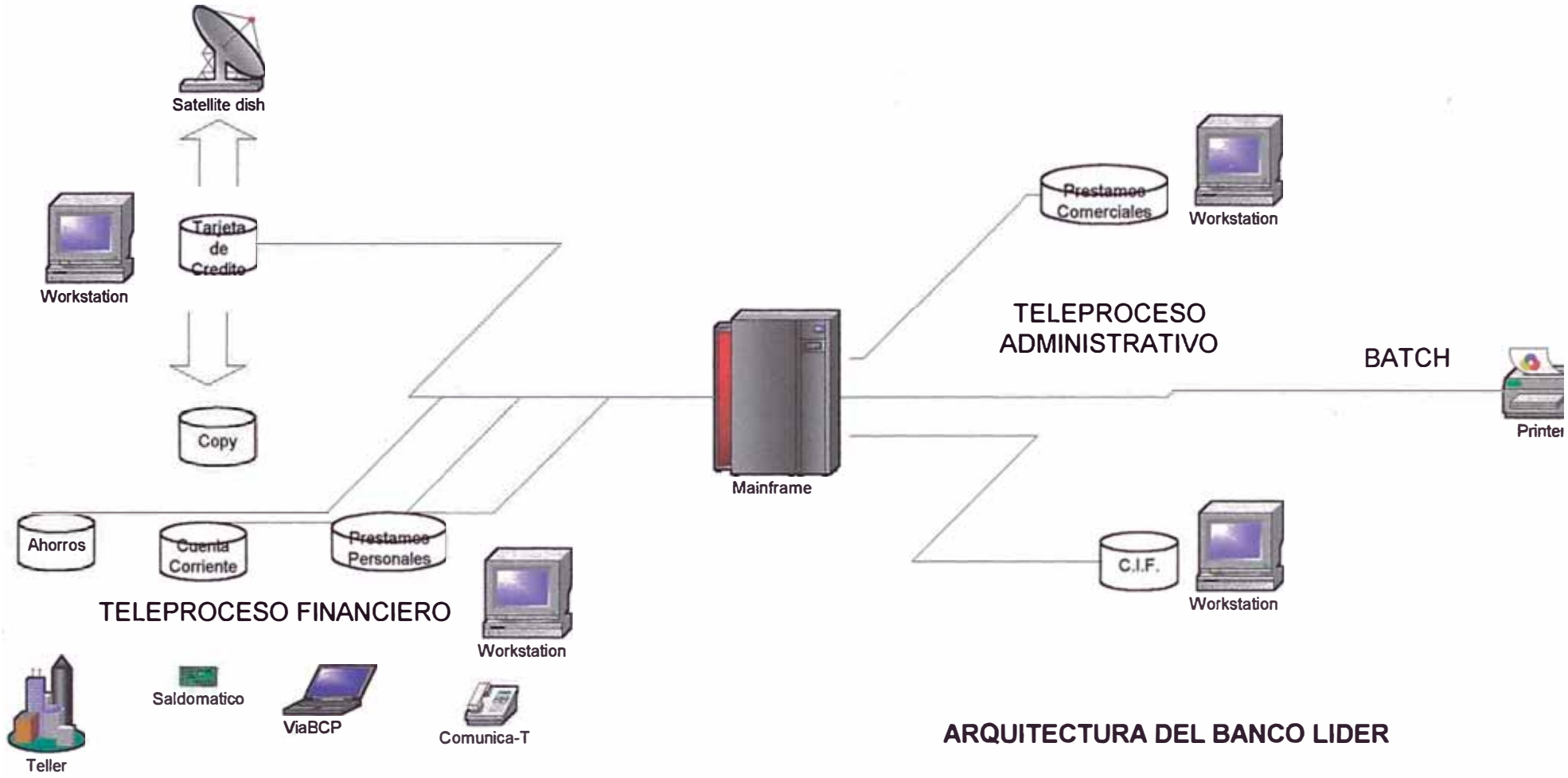
Los Departamentos de Tarjeta de Crédito, técnico y funcional pertenecen a la División de Sistemas y Organización que reportan a la misma Gerencia General Adjunta. Su función es dar solución a las unidades Usuarias en sus diversos requerimientos de negocios.

Estadísticas Actuales en el Mercado Peruano

Las tarjetas de crédito de las tiendas se han convertido en una inmediata alternativa para poder adquirir mil y un productos cuando no se dispone de dinero en efectivo.

En el mercado local, por un lado existen las tarjetas emitidas por financieras vinculadas a grandes tiendas por departamentos. Asimismo, los grandes centros comerciales han presentado sus propias tarjetas, que ofrecen al público la posibilidad de pagar productos y servicios de todas las tiendas que agrupa cada uno de ellos. A esta oferta también se suman las tiendas de electrodomésticos.

Las tarjetas de crédito emitidas por las financieras son las que tienen actualmente su participación de 40,65% en el mercado. Su crecimiento anual ha sido mayor que la de los bancos.


Satellite dish
Workstation
Tarjeta de Credito
Copy
Ahorros
Cuenta Corriente
Prestamos Personales
TELEPROCESO FINANCIERO
Workstation
Saldomatico
ViaBCP
Comunica-T
Teller
Mainframe
Prestamos Comerciales
Workstation
TELEPROCESO ADMINISTRATIVO
BATCH
Printer
C.I.F.
Workstation
ARQUITECTURA DEL BANCO LIDER

Si a las cifras nos remitimos, en diciembre el 2003 existían poco más de un millón de tarjetas de financieras activas y, en la actualidad, hay más de un millón 410 mil, es decir han aumentado en 32%. Esto se debe a que estas empresas se dirigen a un segmento más amplio con menores líneas de crédito como lo demuestra el monto promedio utilizado (S/.614).

La maquinita no para de funcionar: cada vez más, los bancos y las empresas financieras hacen uso de ella para emitir el llamado dinero plástico. Actualmente, el número de tarjetas de crédito bancarias activas en el mercado peruano sobrepasa los dos millones, habiendo experimentado un crecimiento significativo en los últimos años.

Hacia marzo del 2005, del total de tarjetas de crédito bancarias activas en nuestro país, las de marca privada ocupan el 46,9% del total del mercado; Visa, el 33,2%; Mastercard, el 16,32%; American Express, el 2,72%, y Diners con un 0,86% de participación.

Con tantas tarjetas en el mercado, las compras y transacciones realizadas con ellas muestran un ritmo acelerado. El monto utilizado con las tarjetas de bancos se ha incrementado de 474 a 731 millones de dólares, desde diciembre del 2003 a fines de abril de este año.

Parece ser que el motivo es el elevado número de comercios que aceptan este medio de pago. Desde hace varios años, se ha experimentado una creciente afiliación de establecimientos comerciales ubicados principalmente en la denominada Nueva Lima (distritos del Cono Norte y el lado Este de la capital), hasta contar actualmente con 3,500 establecimientos de esa zona que duplican la facturación en tarjetas de crédito.

En el caso de provincias, la situación no es diferente. El interior del país ha experimentado, de mayo a 2004 a mayo del 2005, un crecimiento de 137% en el uso de tarjetas de crédito afiliadas a esta empresa. Además, en todo el país, Procesos MC Perú posee más de 19 mil establecimientos afiliados.

Arequipa es el departamento que muestra un mayor crecimiento en el uso de tarjetas, con un 264% de mayo del 2004 a mayo del 2005, Le sigue Piura con 199,9%, Chiclayo con 161,8% y Trujillo con 122,9%.

CAPITULO II

MARCO TEORICO

Tipos de Tarjetas en el Mercado Local Actual

El objetivo del presente estudio fueron las Tarjetas de Crédito VISA del Banco Líder del País, por lo tanto es conveniente identificar los diferentes tipos de tarjetas del mercado local y como se definen.

Por la institución de emisión o simplemente el Emisor

Según sea la organización que respalda las tarjetas, éstas pueden ser:

- Tarjetas Bancarias, emitidas por un Banco
- Tarjetas No Bancarias, dentro de estas se encuentran las Tarjetas emitidas por Financieras vinculadas a grandes tiendas por departamentos o cualquier tienda comercial

Por su Sistema de Afiliación

Según sigue las reglas de negocio entre comercios y emisores de marcas específicas a nivel internacional o no, las tarjetas pueden ser del tipo:

- VISA (33,2% del mercado local)
- American Express (2,72%)
- MasterCard (16,32%)
- Diners (0,86%)
- Marca Privada (46,9%), simplemente todas las demás.

Por la modalidad de cargo en cuenta

- Crédito, aquellas que trabajan con una Línea de Crédito conocida o no por el cliente.
- Débito, aquellas que se respaldan con una cuenta de débito, como una cuenta corriente o ahorros. También en el caso de las VISA se aplican las consideraciones de crédito en su uso por eso se han considerado esta clasificación.

Por su Tecnología

- Sin Chip, típicamente la mayoría de tarjetas en el mercado local
- Con Chip, algunos grupos de tarjetas emitidas por el Banco Líder en Proyectos de Avanzada Tecnológica

Por sus Privilegios

- Clásica (44.07% del mercado), con líneas mínimas de crédito entre 350 y 1700 nuevos soles o 200 y 750 dólares americanos. Se demanda un ingreso desde 350 a 1500 nuevos soles. Costos de Mantenimientos desde 5 hasta 13,50 nuevos soles y 4 dólares en moneda extranjera
- Oro (5,99%), con líneas mínimas de crédito entre 5,500 y 20,000 nuevos soles o 2,000 y 5,000 dólares americanos. Se demanda un ingreso desde 1,670 a 3,000 dólares. Costos de Mantenimientos desde 9 hasta 14 nuevos soles y de 4 a 4,5 dólares en moneda extranjera
- Platinum (1,01%), con datos reservados por los Bancos, usualmente para clientes VIP.

Marco Conceptual

El crecimiento del Internet y del E-Commerce ha sido explosivo. Al respecto, en el primer mercado mundial, es decir Estados Unidos, el numero de adultos con acceso a Internet creció de 88 millones a mediados del 2000 a 104 millones a fines del mismo año y el total de ventas para ese mismo año represento US$ 25.8 billones. Sin embargo este boom también ha sido un lugar fértil para el fraude, por ejemplo la Federal Trade Comisión de Estados Unidos, organización que ve el tema del fraude electrónico en ese país, informó del aumento significativo del número de reclamos que recibió, de 1,000 presentados en 1997 a 25,000 que ocurrieron en el año 2000 (ver Anexo 1).

Según VISA, en su Región Latino América y el Caribe el fraude aumento en 22% el año 2000, variando de 19 a 27 millones de dólares por este concepto. A su vez se evidenció que el índice de fraude (volumen de fraudes entre volumen de ventas) en transacciones internacionales es mayor a las transacciones realizadas en modo doméstico, sin embargo a fines del 2000 la participación del Fraude a nivel internacional era solo del 29% mientras que el 71% correspondía al fraude doméstico.

Pero que es Fraude? Fraude es uno de los tipos de delito informático más comunes en el mundo y consiste en una transacción en la cual el tarjetahabiente no participó ni autorizó. Es importante tipificar los diferentes motivos de fraude:

- Tarjeta perdida, que incluye el caso en el que el tarjetahabiente no recuerda que la haya perdido pero no sabe donde esta
- Tarjeta robada, caso que suele evidenciarse con una denuncia policial
- Tarjeta no recibida, caso por el cual la tarjeta no llego a manos del tarjetahabiente

- Solicitud fraudulenta, caso por el cual un cliente logra aplicar con información falsificada y obtiene una Tarjeta de Crédito
- Tarjeta Falsificada, es una tarjeta cuyos datos no corresponden a la información que tiene el Emisor, es decir la Tarjeta no existe en la Base de Datos del Emisor, por lo tanto nunca fue emitido el numero de esa tarjeta
- Uso Fraudulento del Numero de Tarjeta, es decir la Tarjeta física no estuvo presente pero sin embargo existen transacciones consumos no reconocidos. caso por el cual se han tomado datos físicos y/o magnéticos de la tarjeta, incluye el skimming y las clonaciones.
- Otros tipos como la suplantación de identidad, en el cual se realizan transacciones con una tarjeta obtenida con la documentación de otra persona

Marco Metodológico

Para la Identificación del Problema

Para poder resolver el problema, lo primero que se tuvo que hacer es lograr su identificación y se realizó lo siguiente:

- Análisis de reportes de fraude enviados por los partners. Especialmente en el caso de VISA que tiene un mayor nivel de avance pues cuenta con el Fraud Reporting System (FRS) que es un servicio disponible para ayudar a los miembros a reportar, seguir y analizar transacciones fraudulentas. Para ello consolida información de fraude, ayuda a detectar patrones de fraude y reduce pérdidas.
- Aplicación de OLAP (On-Line Analysis Process) a partir de la información propia que el Banco tenia en el Data Warehouse. Estos archivos fueron entregados al Usuario del Departamento de Fraude para sus

investigaciones y luego permitió complementar y corroborar la información de VISA.

Para la Solución del Problema

Para aplicar su solución se emplearon los siguientes métodos:

- Parametrización dinámica a través de un proceso que podía cargar los parámetros de prevención de fraude en cualquier momento del día, si es que hubiera la necesidad de cambiarlos.
- Aplicación de User Exits, se identificaron dentro del paquete de software aquellos lugares definidos para que se hagan las adecuaciones necesarias
- Code Review, se realizaron reuniones del equipo técnico de trabajo (6 personas) para ver línea a línea la codificación realizada de modo que sea la mas eficiente y que no origine impacto negativo al procesamiento de las autorizaciones
- Pruebas de Regresión para ver el comportamiento normal de la funcionalidad, sus diferentes respuestas y sus tiempos de respuesta

Para la Implantación de la Solución del Problema

Para la implantación de la solución se realizó:

- Instalación Piloto, se eligió un tipo de tarjeta a la cual aplicar los parámetros de detección de fraude
- Monitoreo de Sistemas, se realizó el soporte online y el seguimiento diario tanto a la instalación piloto como a un par de modificación típicas posteriores a la instalación.

CAPITULO III

PROCESO DE TOMA DE DECISIONES

Planteamiento del Problema

El problema a resolver es como detener el problema de transacciones fraudulentas. Para ello se ha tipificado en base al análisis realizado que estas tienen las siguientes características:

- Del total de reclamos por fraude la composición arrojó como casos mayores:
  69% para el caso de Tarjeta Falsificada
  10% para el caso de Tarjeta Perdida
  9 % para el caso de Tarjeta Robada
  8 % para el caso de Uso Indebido de Tarjeta
  4% para los demás casos de Suplantación de Identidad, Tarjeta No Recibida y Solicitud Fraudulenta
- Las transacciones se adquirieron en Estados Unidos (14%) o Venezuela (3%)
- Las transacciones corresponden a tarjetas de todos los tipos VISA (90%) y AMEX (10%)
- Existen transacciones de diferente importe y a cualquier hora del día.
- Hay casos en que existe mas de una transacción diaria para una misma tarjeta. Aunque los montos no son montos altos tampoco son pequeños.

- Para el caso de las transacciones con Tarjeta Falsificada, éstas se realizan en diferentes tipos de establecimientos, siendo los principales rubros según clasificación de categoría comercial:

  Otros[11] 45%

  Super Mercados 10%

  Tiendas por Departamento 4%

  Equipos Electrónicos, Aerolíneas 3%

  Joyerías y Restaurantes 2% cada uno

También se revisó con el simulador VTS[12] y Test Simulator de AMEX la mensajería de autorizaciones tanto para VISA[13] como para American Express respectivamente. Por el volumen de operaciones la muestra con las transacciones VISA permitió evidenciar de manera más rápida el siguiente problema:

Es prudente indicar que las transacciones que piden código de autorización son de dos tipos:

- Las Transacciones que corresponden a Compras en Establecimientos que se canalizan mundialmente a través de los diferentes puntos de venta (tanto en el mundo real como en el virtual, es decir Internet), y,
- Las Transacciones de Disposiciones en Efectivo que se realizan típicamente tanto en terminales ATM como en Teller.

El análisis realizado corresponde a las transacciones del primer tipo.

---

[11] Comprende todos aquellas categorías de comercio que no han podido clasificarse en las otras categorías. Típicamente corresponde a los establecimientos o sitios en Internet.

[12] VISA Test Simulator

[13] Llamada BASE I

Efectivamente se evidenció el uso del dato origen de ingreso de la transacción:

- Transacciones con Lectura de Banda (swiped transactions)
- Transacciones ingresadas manualmente
- Transacciones SET
- Otras transacciones, en las que estaban incluidas el resto de transacciones Internet y las transacciones de correo o teléfono (MO/TO[14])

Por lo tanto un hallazgo importante fue que no hay manera de identificar plenamente por el dato origen, si una transacción en Internet que no es SET, efectivamente se realizó en Internet o si corresponde a una transacción del tipo MOTO. Esto se corroboró con las comunicaciones de respuesta a este tema, vía correo electrónico tanto de VISA como la de AMEX en las que sin reconocerlo explícitamente se afirmaba que se esta trabajando con los miembros en este tema y ya había avances.

Para lograr identificar si la transacción era de Internet, se hubiera requerido datos del Establecimiento y del Adquirente pero esto por lo complejo de la configuración de las redes internacionales de establecimientos y adquirentes no siempre ocurría y era complicado así como confidencial obtenerlo. De hecho, requería un proceso de Certificación –en este caso de VISA- a cada miembro involucrado, es decir un Proyecto entre 3 y 6 meses.

Igualmente se encontró que en algunas transacciones venia el dato del CVV2, penúltimo intento de VISA de proteger las transacciones de Internet. Pero se encontró que no toda la información definida para esta condición era consistente, lo que inclusive motivaba a rechazar transacciones en las que el cliente había ingresado el CVV2 (definido para el caso de transacciones

[14] MO / TO: Mail Order / Telephone Order

ingresadas manualmente) y esto debido al erróneo armado del mensaje por parte del adquirente.

Pero porque además es importante el dato de origen? Lo es porque según este el Adquirente, el Emisor y VISA han definido niveles en los limites de piso. Además en combinación con otros datos como la Categoría de Comercio también se establecen comportamientos de respuesta. Por ello quizás una compra por teléfono (MOTO) como puede ser el pedido de comida en los Estados Unidos, por su importe y naturaleza no requiera ser verificada por el Emisor, pero existirá realmente dicho Establecimiento y será de la categoría Restaurantes? O puede ser el caso de una suscripción por correo a una Revista, que por la frecuencia de su entrega y las condiciones en que el Emisor realiza el cargo en la tarjeta también es aceptada casi universalmente.

Para que los datos de la transacción estén completos crean o toman datos de Establecimientos Reales o Virtuales (Sites) fraudulentos y completan los datos que el Adquirente hubiera registrado. El factor común en ambos casos es que en el dato de País de Origen, es decir el lugar de Adquirencia, venía el código de Estados Unidos o Venezuela. En el caso de Estados Unidos felizmente la mayoría se refería al uso de un código de establecimiento falsificado, correspondiente a una de las compañías de AT&T, para el que hacían pasar todo un juego completo de transacciones de todas las tarjetas del Banco, ,existan o no, dado que conocían los BIN[15] que tenia asignado el Banco, algunas de las cuales que por su monto debajo del Limite de Piso y Tiempo de Respuesta ya habían sido autorizadas indebidamente.

[15] B.I.N o Bank Identification Number, código numético de hasta 6 dígitos asignado por el partner para generar los números de tarjeta o P.A..N. (Primary Accountn Number).

Se evidenció también el problema de algunos reclamos correspondían a transacciones perfectamente autorizadas, en este caso se trataba de tarjetas copiadas, lo que se conoce como modalidad skimming, por el cual se han capturado datos válidos de tarjetas a partir de los mensajes que viajan por las diferentes redes públicas y privadas y donde esta toda la información de la cuenta necesaria para garantizar la transacción. Mas no así los datos de la transacción como el lugar, establecimiento, origen de la transacción que es por donde se planteó en detalle la solución algorítmica, pues nuevamente apareció Venezuela como lugar de adquirencia, es decir concluíamos que una o más bandas especializada en este tipo de delitos estaba en Venezuela. Averiguamos también que en ese país las regulaciones de comercio electrónico así como las de comercio en general son demasiado débiles, por ejemplo pueden meter a la cárcel a un delincuente que este cometiendo un fraude con su tarjeta en un establecimiento, pero lo liberan a las horas de la detención.

Finalmente debemos indicar que también se evidenciaron, aunque no mayoritariamente algunos comportamientos de fraude, como:

- Múltiples compras en un mismo establecimiento el mismo día
- Compras grandes en diversos establecimientos

Alternativas de Solución

Al Problema Central

Las alternativas de solución que se definieron para el problema central fueron:

Procesos de Autorizaciones

	Ventajas	Desventajas
1. Adecuar el software existente para aplicar algoritmos adicionales en el flujo de autorizaciones	Solución Rápida	Alto riesgo por realizar modificaciones a un paquete en su parte transaccional central
2. Adquirir un paquete de software que permita monitorear el fraude	Permite aprovechar otras experiencias integrando un software especializado	Costo y tiempo de la implantación
3. Adquirir un paquete de software especializado en fraude que permite pronosticar comportamientos de mercado	Solución Integral al tema de Fraude semi-automatizando su Monitoreo	Alto costo, proceso de aprendizaje organizacional y gran tiempo de espera antes de ver los resultados

A otros Problemas

La magnitud del problema y la cantidad de información disponible, así como la organización del equipo de trabajo permitió establecer que existía un número menor de casos que no encajaban en las conclusiones del problema central. Estos se referían entonces a exposiciones de riesgo en otros procesos sobre las cuales se presentaron las siguientes alternativas de solución como acción complementaria al tema de la prevención del fraude:

Proceso de Grabación de Tarjetas

Problema: Sustracción de Plásticos y Fuga de Información Computarizada

	Ventajas	Desventajas
1. Restringir el acceso y aumentar el nivel de seguridad	Monitoreo permanente del proceso mediante cámaras ocultas Creación de PINes por separado del proceso de impresión de los mismos	Aumento de costos de equipos así como su mantenimiento y operación
2. Realizar un outsourcing del servicio	Traslado del problema a otra organización Libera recursos	Perdida del control del proceso Potencial fuga de información

Proceso Distribución de Tarjetas

Problema: Exposición de Información e Identificación del Tarjetahabiente

	Ventajas	Desventajas
1. Enviar por separado el PIN del resto de la información de la Tarjeta	Disminuir el riesgo por exposición de información complementaria sensible.	Costo operativo de doble proceso de envío teniendo en cuenta el alto grado de reintentos de entrega por no ubicar al cliente Costos por la Modificación de Software
2. Mantener proceso	No hay cambios en	Exposición de la

unificado de envío del PIN con el resto de información de la Tarjeta	costos. Marketing esta satisfecho con esta modalidad	información
3. Enviar las Tarjetas Desactivadas	Confirmación del receptor de la Tarjeta	Cambio en la modalidad en que opera el cliente Costos por la Modificación de Software

Metodología de Solución

Procesos de Autorizaciones

El monitoreo de cuentas ha permitido detectar el Fraude con el objetivo de reducir las pérdidas identificando rápidamente las transacciones o consumos sospechosos.

Por lo tanto el objetivo era desarrollar una estrategia de respuesta para solicitud de autorizaciones específicas al Banco y evitar pérdidas antes que se complete la transacción.

Para ello el método de solución fue:

1. Identificar los parámetros de riesgo relevante
2. Clasificar cada parámetro de acuerdo al nivel de riesgo
3. Desarrollar modelo de respuesta usando Análisis de Regresión

Los parámetros de riesgo inicialmente identificados fueron:

- Producto
- Código de País
- Modalidad de ingreso de la información: Swiped, Manual, MOTO, SET
- Código de Categoría de Comercio (Merchant Category Code)
- Importe

Se identificó como parámetro de alto riesgo al código de país, de riesgo medio a la modalidad de ingreso de datos y de bajo riesgo al código de categoría de comercio y al importe.

Se logró establecer solo una asociación de variables entre el código de categoría de comercio y el importe pues existía una co-relación demostrada entre ambas variables. Esto motivó a crear una variable mixta.

El conjunto de estos parámetros y su combinación peso y nivel de riesgo daba origen a una matriz de decisión, por la variable producto. El algoritmo de partida para el producto que se elija solo entraría en funcionamiento para las variables:

- País de Origen
- Modalidad de ingreso de datos

Luego de ello en base a los valores de la transacción por categoría de comercio, la transacción era rechazada. El rechazo de estas transacciones se almacenaba en un archivo especial y podía ser accesada online por la central de autorizaciones ante cualquier reclamo. Inicialmente se llamaba al Adquirente de la transacción para tratar de contactar al cliente.

Toma de Decisiones

Procesos de Autorizaciones

El equipo de trabajo decidió optar por la Alternativa 1, es decir realizar la adecuación del software, sin embargo las otras alternativas no se desestimaron.

Proceso de Grabación de Tarjetas

El equipo de trabajo opto por la Alternativa 1. En este sentido se le asignó al Servicio de Seguridad de Información el monitoreo de la producción de tarjetas y adicionalmente se instalaron controles adicionales como actualización de usuarios autorizados, limitación de ingreso al área de Producción, uso de card keys con lectoras en las puertas.

Adicionalmente se decidió comprar un software para plataforma cliente/servidor que permite la administración de claves maestras, las que residirán en software, y que pueda generar los PINes e imprimirlo a su vez. Como un pre-requisito a esta decisión es eliminar cualquier transmisión entre la plataforma mainframe donde reside el sistema de tarjeta de crédito con el sistema de cliente servidor para su grabación, dado que seria innecesario y ahora no prudente que viaje información confidencial.

Proceso Distribución de Tarjetas

El equipo de trabajo opto por la Alternativa 2. Fue muy significado el pedido de Marketing de no alterar los procesos actuales de los tarjetahabientes dada la gran cantidad existente. Sin embargo se aceptó considerar las otras dos alternativas en el caso de VISA cuando se revisen los siguientes puntos:

- Ampliación de la capacidad del producto a la funcionalidad bi-moneda
- Cambio de números de tarjetas diferenciados por usuario
- Cambio de claves maestras de seguridad usadas para la generación de PINes y demás valores de seguridad, recomendado por VISA

Estrategias Adoptadas

Procesos de Autorizaciones

Como se menciono anteriormente al final del problema se logró tener una estrategia general basada en tres horizontes :

- En el corto plazo, se pondría en funcionamiento en un mes aproximadamente la aplicación de algoritmos que identifiquen las transacciones fraudulentas durante el proceso de autorizaciones.
- En el mediano plazo, en los próximos seis meses con la integración de una herramienta de monitoreo que permita construir alarmas en función de información diaria e histórica
- En el largo plazo, en el próximo año, con la adquisición de algún paquete de software especializado en identificar comportamientos de segmentos de cliente a través de redes neuronales .

Para la instalación de la solución de corto plazo se identificó usar el producto CrediBank Oro Mobil para monitorear sus resultados en modalidad Piloto. Se hizo esta elección en base a que tenia el menor volumen de tarjetas, si bien este volumen era mayor que el de los diferentes tipos de tarjetas American Express y el de la CrediBank Empresarial.

Adicionalmente se consideró como valor de la variable País de Origen el código de Venezuela y como valor de modalidad de ingreso el código de transacciones MO/TO.

CAPITULO IV

EVALUACIÓN DE RESULTADOS

Las adecuaciones al software se realizaron a mediados de Febrero del 2001. A fines de marzo se realizo la primera evaluación integral de los resultados de su aplicación con resultados exitosos pues el nivel de fraude disminuyó significativamente, es decir fue menor a los US$30,000 y estaba cubierto por el seguro. La tendencia de la disminución del nivel de fraude se confirmó y acentuó en los meses siguientes.

La relación costo-beneficio fue rápidamente beneficiosa. Los costos incurridos fueron básicamente los siguientes: 160 horas de análisis funcional, 40 horas de revisión técnica y 80 horas de control de calidad realizado por personal del Banco, y 160 horas de diseño técnico, programación y pruebas unitarias del proveedor, cuyo costo fue de $16,000 mas gastos operacionales ($5,000). Por lo tanto, en menos de un mes ya se había recuperado el costo.

El problema había sido controlado y esto lo sabían las organizaciones de fraude que dejaron de prestarle atención al Banco Líder, al menos por el momento.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

El prese nte trab ajo nos h a pe rmitido concluir con lo siguien te:

- Estamos viviendo un momento de gran importancia en la historia de este planeta, en camino hacia la digitalización total. Nuevas tecnologías abren la puerta a productos y servicios innovadores. A medida que el mundo se adapta al rápido desarrollo de las posibilidades en línea, las instituciones financieras se esfuerzan para construir el futuro de los servicios financieros.
- El mundo de Internet ha abierto nuevos mercados y con ello a las transacciones comerciales asociadas a Tarjetas de Crédito, las que están pasando por un periodo de estabilización en cuanto a su seguridad en países como el nuestro, inclusive la presencia de nuevas tecnologías como el chip resolverían este problema pero su costo en estos momentos es significativamente alto.
- El fraude es dinámico y las organizacion es que lo dirigen también. El frau de siem pre irá en evolución según se a el mercado y la tec nología existen te por ello lo importante es tener una ac titud directa y tomar acciones inmed iatas pa ra co ntrolar y minimizar su impacto.
- La so lución a los problem as orga nizac ionales por lo gen eral van mas allá de cam bios a nivel de software sino que involucran cambios en los proce so s y en formas de ha cer los neg ocios.

Finalmente podemos recomendar lo siguiente:

- Como en todo acto delictivo, los actores del negocio de Tarjeta de Crédito deben unir esfuerzos para prevenir, detectar y eliminar cualquier indicio de Fraude pues éste afecta los resultados financieros la institución así como la imagen que los clientes puedan tener de su Banco.
- El rol de adquirente en el Perú que lo ocupa VISANET fundamentalmente debe complementar las medidas contra el fraude. Temas como capacitación a los establecimientos y los puntos de contacto, así como detección de actitudes sospechosas en transacciones y finalmente el compartir la información a tiempo.
- Toda organización debe estar preparada para recibir, controlar y resolver esta ola delictiva informática y por la tanto debe internamente estar organizada con una Unidad responsable de este tema
- Los emisores y adquirentes deben seguir las mejores practicas de Prevención del Fraude por parte de los partners VISA y AMEX así como estar en constante capacitación del tema.

BIBLIOGRAFIA

Prepared State ment on Internet Fraud, Federal Trade Commerce – Abril del 2001
V.I.P System Overview, VISA – Febrero del 2000
Global Online Bus iness Excha nge Manual, AEGNS - Mayo del 2000

ANEXOS

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION ON
"INTERNET FRAUD"
Before the
COMMITTEE ON FINANCE
UNITED STATES SENATE
Washington, D.C. April 5, 2001

Mr. Chairman, I am Hugh Stevenson, Associate Director of the Division of Planning and Information in the Federal Trade Commission's Bureau of Consumer Protection. I am pleased to be here today to testify about the FTC's efforts to combat fraud on the Internet.

As one of the transforming events of our time, the advent of the Internet already has had a profound impact on the marketplace. The Internet has the potential to deliver goods and services more conveniently, faster, and at lower prices than traditional marketing methods. Moreover, at an ever increasing rate, it is stimulating the development of innovative products and services barely conceivable just a few years ago, and enabling consumers to tap into rich sources of information that they can use to make better-informed purchasing decisions.

These developments promise enormous benefits to consumers and the economy. There is real danger, however, that these benefits may not be fully realized if consumers identify the Internet with fraud operators. Fraud on the Internet is an enormous concern for the Commission, and it has prompted a vigorous response using all the tools at the Commission's disposal, including law enforcement and education. The Commission appreciates the Subcommittee's interest in our Internet fraud program, and the Congress' support for funding both the development of our fraud database, Consumer Sentinel, and the creation of our toll-free consumer helpline. The Commission welcomes this opportunity to describe its Internet program and the challenges the agency is confronting.

I. Introduction and Background

A. *The FTC and its Law Enforcement Authority*

The FTC is the federal government's primary consumer protection agency. While most federal agencies have jurisdiction over a specific market sector, the Commission's jurisdiction extends over nearly the entire economy, including business and consumer transactions on the Internet.

Under the Federal Trade Commission Act, the agency's mandate is to take action against "unfair or deceptive acts or practices" and to promote vigorous

competition in the marketplace. The FTC Act authorizes the Commission to halt deception through civil actions filed by its own attorneys in federal district court, as well as through administrative cease and desist actions.[4] Typically these civil actions seek preliminary and permanent injunctions to halt the targeted illegal activity, as well as redress for injured consumers. Where redress is impracticable, Commission actions generally seek disgorgement to the U.S. Treasury of defendants' ill-gotten gains. As discussed below, these tools have proven to be effective in fighting a broad array of fraudulent schemes on the Internet, in spite of the sheer size and reach of the Internet.

B. *The Growth of Ecommerce and Internet Fraud.*

The growth of the Internet and ecommerce has been explosive. The number of American adults with Internet access grew from about 88 million in mid-2000 to more than 104 million at the end of the year.[5] Just this past holiday season, consumers spent an estimated $10.8 billion shopping on the Internet -- a greater than 50 percent increase over the $7 billion they spent online during the same period in 1999.[6] Total ecommerce sales for 2000 were an estimated $25.8 billion, .8 percent of all sales.[7]

Unfortunately, but not surprisingly, the boom in ecommerce has opened up fertile ground for fraud. The Commission's experience is that fraud operators are always among the first to appreciate the potential of a new technology to exploit and deceive consumers. Long-distance telemarketing attracted con artists when it was introduced in the 1970's. They swarmed to pay-per-call technology when it became available in the late 1980's. Internet technology is the latest draw for opportunistic predators who specialize in fraud. The rapid rise in the number of consumer complaints related to online fraud and deception bears this out: in 1997, the Commission received fewer than 1,000 Internet fraud complaints through Consumer Sentinel; a year later, the number had increased eight-fold. In 2000, over 25,000 complaints -- roughly 26 percent of all fraud complaints logged into Consumer Sentinel by various organizations that year -- related to online fraud and deception. The need -- and challenge -- is to act quickly to stem this trend while the online marketplace is still young.

C. The FTC's Response to Protecting Consumers in the Online Marketplace

Stretching its available resources to combat the growing problem of Internet fraud and deception, the Commission has targeted a wide array of online consumer protection problems. This effort has produced significant results. Since 1994 , the Commission has brought 170 Internet-related cases against over 573 defendants. It obtained injunctions stopping the illegal schemes, and ordering more than $180 million in redress or disgorgement,[8] and obtained orders freezing millions more in cases that are still in litigation. Its federal district court actions alone have stopped consumer injury from Internet schemes with estimated annual sales of over $250 million.[9]

II. Challenges Posed by Internet Fraud

The Commission faces a host of novel challenges in its efforts to combat fraud and deception online. Because it is both global in its reach and instantaneous, the

Internet lends itself well not only to adaptations of traditional scams - such as pyramid schemes and false product claims - but also to new high-tech scams that were not possible before development of the Internet. In addition, the Internet enables con artists to cloak themselves in anonymity, which makes it necessary for law enforcement authorities to act much more quickly to stop newly-emerging deceptive schemes before the perpetrators disappear. And because the Internet transcends national boundaries, law enforcement authorities must be more creative and cooperative to successfully combat online fraud. These novel challenges are discussed in greater detail below.

A. *Combating Internet Fraud Requires New Methods of Collecting and Analyzing Information.*

The Commission is developing new methods of collecting and analyzing information about both the offline and online marketplace, drawing upon the power of new technology itself. A central part of this effort is Consumer Sentinel, a web-based consumer fraud database and law enforcement investigative tool.[10] Consumer Sentinel receives Internet fraud complaints from the FTC's Consumer Response Center ("CRC"), which processes both telephone and mail inquiries and complaints.[11] For those consumers who prefer the online environment, an electronic complaint form at www.ftc.gov, first available in May of 1998, permits consumers to channel information about potential scams directly to the CRC and the fraud database.

Consumer Sentinel also benefits from the contributions of many public and private partners. It receives data from other public and private consumer organizations, including 64 local offices of the Better Business Bureaus across the nation, the National Consumers League's National Fraud Information Center, and Project Phonebusters in Canada. Additionally, a U.S. Postal Inspector has served for the past year as the program manager, and the U.S. Postal Inspection Service just signed an agreement to begin sharing consumer complaint data from its central fraud database with Consumer Sentinel.

The Commission provides secure access to this data over the Internet, free of charge, to over 300 U.S., Canadian, and Australian law enforcement organizations -- including the Department of Justice, U.S. Attorneys' offices, the Federal Bureau of Investigation, the Securities and Exchange Commission, the Secret Service, the U.S. Postal Inspection Service, the Internal Revenue Service, the offices of all 50 state Attorneys General, local sheriffs and prosecutors, the Royal Canadian Mounted Police, and the Australian Competition and Consumer Commission. Consumer Sentinel is a dynamic online law enforcement tool to use against all types of fraud, especially online fraud.[12]

The central role that Consumer Sentinel plays in the Commission's law enforcement is exemplified by "Operation Top Ten Dot Cons," the Commission's latest broad "sweep" of fraudulent and deceptive Internet scams. In a year-long law enforcement effort, the FTC and four other U.S. federal agencies,[13] consumer protection organizations from 9 countries,[14] and 23 states[15] announced 251 law enforcement actions against online scammers. The FTC

brought 54 of the cases.[16] The top 10 scams, identified through analysis of complaint data in the Consumer Sentinel database, were:

- Internet Auction Fraud
- Internet Service Provider Scams
- Internet Web Site Design/Promotions ("Web Cramming")[17]
- Internet Information and Adult Services (unauthorized credit card charges)
- Pyramid Scams
- Business Opportunities and Work-At-Home Scams
- Investment Schemes and Get-Rich-Quick Scams
- Travel/Vacation Fraud
- Telephone/Pay-Per-Call Solicitation Frauds (including modem dialers and videotext)[18]
- Health Care Frauds

The Consumer Sentinel data enabled the FTC and the other enforcement agencies that joined us in this project both in the U.S. and abroad to identify not only the top ten types of scams, but also the specific companies generating the highest levels of complaints about each of those types of scams. These companies became the targets for the law enforcement actions that comprised Operation Top Ten Dot Con. Finally, Consumer Sentinel data enabled the Commission and its partners to obtain and develop evidence against these targets from individual consumers whose complaints had been included in the database.

Consumer Sentinel first went online in late 1997. Since then, the Commission has upgraded the capacity of the Consumer Sentinel database and enhanced the agency's complaint-handling systems by creating and staffing a new toll-free consumer helpline at 1-877-FTC-HELP, and adding several new functions to Consumer Sentinel. The first of these new functions, the "Top Violators" report function, allows a law enforcement officer to pull up the most common suspects and schemes by state, region or subject area. The second new function, "Auto Query," enables an investigator to create an automatic search request. This automatic search can be set to run daily, weekly or monthly, and if new

complaints come in to Consumer Sentinel that match the search criteria, Consumer Sentinel will automatically alert the investigator via email. Third, the "Alert" function enables law enforcers to communicate with each other and minimize duplication of their efforts, and a fourth new function performs a search of Commission court orders online. In 2000, Consumer Sentinel received over approximately 100,000 consumer complaints.[19] Currently the database holds over 300,000 consumer complaints.[20]

The Commission's efforts to improve consumer complaint collection and analysis through the Consumer Response Center and Consumer Sentinel are complemented by a proactive program to uncover fraud and deception in broad sectors of the online marketplace through "Surf Days." Surf Days use new technology to detect and analyze emerging Internet problems. While Consumer Sentinel provides data on broad trends and the volume of complaints prompted by particular Internet schemes, Surf Days allow the Commission to take a "snap shot" of a market segment at any given time. The Commission also uses Surf Days to reach new entrepreneurs and alert those who unwittingly may be violating the law.

On a typical Surf Day, Commission staff and personnel from our law enforcement partners -- often state attorneys general, sister federal agencies or private organizations like the Better Business Bureau -- widely "surf" the Internet for a specific type of claim or solicitation that is likely to violate the law. When a suspect site is identified, the page is downloaded and saved as potential evidence, and the operator of the site is sent an email warning that explains the law and provides a link to educational information available at *www.ftc.gov*. Shortly thereafter, a law enforcement team revisits the previously warned sites to determine whether they have remedied their questionable claims or solicitations. The results vary, depending on the targeted practice of the particular Surf Day. In each of these efforts, between 20 to 70 percent of the Web site operators who received a warning come into compliance with the law, either by taking down their sites or modifying their claims or solicitations. Sites that continue to make unlawful claims are targeted for possible law enforcement action.

To date, the Commission has conducted 26 different Surf Days targeting problems ranging from "cure-all" health claims to fraudulent business opportunities and credit repair scams.[21]

More than 250 law enforcement agencies or consumer organizations around the world have joined the Commission in these activities; collectively, they have identified over 6,000 Internet sites making dubious claims. The law enforcement Surf Day has proven so effective that it is now widely used by other government agencies, consumer groups and other private organizations.

B. *Traditional Scams Use the Internet to Expand in Size and Scope.*

Out of the 170 cases brought by the Commission against Internet fraud and deception, over half have targeted old-fashioned scams that have been retooled for the new medium. For example, the Commission has brought 28 actions

against online credit repair schemes, 25 cases against deceptive business opportunities and work-at-home scheme, and 11 cases against pyramid schemes.

It is no surprise that the Internet versions of traditional frauds can be much larger in size and scope than their offline predecessors. A colorful, well-designed Web site imparts a sleek new veneer to an otherwise stale fraud; and the reach of the Internet allows an old-time con artist to think -- and act -- globally, as well.

Pyramid schemes are the most notable example of a fraud whose size and scope are magnified by the Internet.[22] By definition, these schemes require a steady supply of new recruits. The Internet provides an efficient way to reach countless new prospects around the world, and to funnel funds more efficiently and quickly from the victims to the scammers at the top of the pyramid. As a result, the victims are more numerous, the fraud operator's financial "take" is much greater, and the defense is typically well-funded and fierce when the FTC brings suit to stop a pyramid scheme operating online.

Despite the extensive resources required to pursue an online pyramid case, the Commission has asserted a strong enforcement presence, obtaining orders to pay more than $70 million in redress for victims,[23] and pursuing millions more in ongoing litigation. In one case, *FTC v. Fortuna Alliance,* the Commission spent two years in litigation and negotiations and finally obtained a court order finding the defendants in contempt, and a stipulated final order enjoining the defendants from further pyramid activities and requiring them to pay $5.5 million in refunds to over 15,000 victims in the U.S. and 70 foreign countries.[24] More recently, in *FTC v. Five Star Auto Club, Inc.,*[25] the Commission prevailed at trial against another pyramid scheme that lured online consumers to buy in by claiming that an annual fee and $100 monthly payments would give investors the opportunity to lease their "dream vehicle" for "free" while earning between $180 and $80,000 a month by recruiting others to join the scheme. The court issued a permanent injunction shutting down the scheme, barring for life the scheme's principals from any multi-level marketing business, and ordering them to pay $2.9 million in consumer redress.

C. *Scams Are Increasingly High-Tech.*

Although most Internet fraud stems from traditional scams, the number of schemes uniquely and ingeniously exploiting new technology is multiplying. These are the most insidious schemes because they feed on the public's fascination with -- and suspicion of -- new technology. Their ultimate effect can only be to undermine consumer confidence in the online marketplace. To combat this type of high-tech fraud, the Commission has supported staff training and given its staff the tools to be effective cyber-sleuths.

Recognizing that most of its attorneys and investigators need to be Internet savvy, the Commission has hosted beginner and advanced Internet training seminars and held sessions on new technology, investigative techniques, and Internet case law. The Commission also makes this training available to personnel of other law enforcement agencies. In the past year, the Commission has presented Internet training seminars in seven U.S. cities and in Toronto, Canada, and Paris, France.

In addition to FTC staff, these sessions trained approximately 800 individual participants from other law enforcement agencies. These participants represented twenty different countries including the U.S., twenty-six states, twenty-two federal agencies, and fourteen Canadian law enforcement agencies. Among those who have participated are representatives from the offices of state Attorneys General, the Department of Justice and U.S. Attorneys, the Securities and Exchange Commission, the FBI, and the Postal Inspection Service.

In addition to providing regular Internet training, the Commission also provides its staff with the tools they need to investigate high-tech fraud. The FTC's Internet Lab is an important example. With high speed computers that are separate from the agency's network and loaded with the latest hardware and software, the Lab allows staff to investigate fraud and deception in a secure environment and to preserve evidence for litigation.

The Commission has used its training and tools to stop some of the most egregious and technically sophisticated schemes seen on the Internet. For example, the FTC's lawsuit against Verity International, Ltd.,[(26)] was prompted by the influx of hundreds of complaints in the last week of September 2000 through the CRC and logged in Consumer Sentinel. Investigation showed that high charges on consumers' phone lines were being initiated by "dialer" software downloaded from teaser adult web sites. Many line subscribers had no idea why they received bills for these charges. Others discovered that a minor in their household -- or another person who did not have the line subscriber's authorization -- accessed the Web sites and downloaded the dialer software. The dialer program allowed users to access the "videotext" adult content without any means of verifying that the user was the line subscriber, or was authorized by the line subscriber to incur charges on the line for such service. Once downloaded and executed, however, the program actually hijacked the consumer's computer modem by surreptitiously disconnecting the modem from the consumer's local Internet Service Provider, dialing a high-priced international long distance call to Madagascar, and reconnecting the consumer's modem to the Internet from some overseas location, opening at an adult web site. The line subscriber -- the consumer responsible to pay phone charges on the telephone line -- then began incurring charges on their phone lines for the remote connection to the Internet at the rate of $3.99 per minute. The court has ordered a preliminary injunction in this matter, and litigation continues.[(27)]

Earlier, in *FTC v. Carlos Pereira d/b/a atariz.com*,[(28)] the Commission attacked a world-wide, high-tech scheme that allegedly "pagejacked" consumers and then "mousetrapped" them at adult pornography sites. "Pagejacking" is making exact copies of some one else's Web page, including the imbedded text that informs search engines about the subject matter of the site. The defendants allegedly made unauthorized copies of 25 million pages from other Web sites, including those of Paine Webber and the Harvard Law Review. The defendants made one change on each copied page that was hidden from view: they inserted a command to "redirect" any surfer coming to the site to another Web site that

contained sexually-explicit, adult-oriented material. Internet surfers searching for subjects as innocuous as "Oklahoma tornadoes" or "child car seats" would type those terms into a search engine and the search results would list a variety of related sites, including the bogus, copycat site of the defendants. Surfers assumed from the listings that the defendants' sites contained the information they were seeking and clicked on the listing. The "redirect" command imbedded in the copycat site immediately rerouted the consumer to an adult site hosted by the defendants. Once there, defendants "mousetrapped" consumers by incapacitating their Internet browser's "back" and "close" buttons, so that while they were trying to exit the defendants' site, they were sent to additional adult sites in an unavoidable, seemingly endless loop.

Using the new tools available in the Internet Lab, the Commission was able to capture and evaluate evidence of this "pagejacking" and "mousetrapping." In September 1999, the Commission filed suit in federal court and obtained a preliminary order stopping these activities and suspending the Internet domain names of the defendants. Since then, the Court has entered default judgments against two defendants and a stipulated permanent injunction against a third, baring them from future law violations. A fourth defendant, Carlos Pereira, has evaded law enforcement authorities in Portugal.

D. *Online Scams Spread Quickly and Disappear Quickly.*

One hallmark of Internet fraud is the ability of perpetrators to cover their tracks and mask their locations and identities. Using anonymous emails, short-lived Web sites, and falsified domain name registrations, many fraud operators are able to strike quickly, victimize thousands of consumers in a short period of time, and disappear nearly without a trace.

To stop these swift and elusive con artists, law enforcement must move just as fast. The FTC's Internet Rapid Response Team was created for this very purpose. It draws heavily upon complaints collected by the FTC's Consumer Response Center and the Consumer Sentinel system. The team constantly reviews complaint data to spot emerging problems, conduct quick but thorough investigations, and prepare cases for filing in federal courts. Based on such data review, FTC staff had completed the investigation and was in court successfully arguing for an *ex parte* temporary restraining order and asset freeze in *FTC v. Verity International, Ltd.* within a little more than a week after the first complaints begin coming in to the Consumer Response Center.

In another exemplary effort of the Rapid Response Team, *FTC v. Benoit,*[30] the Team quickly moved against defendants who allegedly used deceptive emails or "spam" to dupe consumers into placing expensive international audiotext calls.[31] The defendants allegedly sent thousands of consumers an email stating that each recipient's "order" had been received and that his or her credit card would be billed $250 to $899. The email instructed consumers to call a telephone number in the 767 area code if they had any questions. Most consumers did not realize that 767 was the area code for Dominica, West Indies. When consumers called the number expecting to reach a customer representative, they were connected to an

audiotext entertainment service with sexual content and charged expensive international rates.

Even though a string of telephone carriers could not identify who operated the audiotext number in question, the Internet Rapid Response Team constructed a compelling case in about three weeks. The Commission quickly obtained a federal court order to stop the scheme and freeze any proceeds of the fraud still in the telephone billing system.

E. *Effective Remedies Are More Difficult to Achieve in the Global Online Market.*

The globalization of the marketplace poses new and difficult challenges for consumer protection law enforcement. Anticipating this development, the Commission held public hearings in the fall of 1995 to explore business and consumer issues arising from technological innovation and increasing globalization. Over 200 company executives, business representatives, legal scholars, consumer advocates, and state and federal officials presented testimony, and the Commission published a two-volume report summarizing the testimony and the role of antitrust and consumer protection law in the changing marketplace. As reported in, "Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace," there was a broad consensus that meaningful consumer protection takes: (1) coordinated law enforcement against fraud and deception; (2) private initiatives and public/private partnerships; and (3) consumer education through the combined efforts of government, business, and consumer groups.[32] These principles have guided FTC policy regarding the Internet ever since.

In addition to gathering information through hearings and workshops, the FTC has gained practical knowledge about the effects of globalization and ecommerce through its litigation. In this respect, the Commission has found that pursuing Internet fraud often involves a difficult and costly search for money that has been moved off-shore. For example, in *FTC v. J.K. Publications*,[33] the Commission obtained an *ex parte* temporary restraining order, a preliminary injunction and an asset freeze against defendants that allegedly made unauthorized charges of $19.95 per month on consumers' credit or debit cards for purported Internet services. Based upon evidence gathered by Commission staff, the defendants may have charged over 900,000 consumers a total of $45 million for unordered or unauthorized Internet services. According to the receiver appointed in this case, the defendants moved millions of dollars to the Cayman Islands, Liechtenstein, and Vanuatu in the South Pacific. The Commission continues to litigate this case, and the receiver continues to attempt to locate defendants' foreign assets and repatriate them to the U.S.

In *FTC v. Fortuna Alliance,* one of the pyramid schemes described above, the Commission found that the defendants had transferred $2.8 million to Antigua, West Indies. With the assistance of the U.S. Department of Justice's Office of Foreign Litigation, the Commission obtained an order from an Antiguan court freezing those funds and a stipulated final judgment in U.S. court that required the

defendants to repatriate that money for consumer redress. In the process, however, it cost $280,000 in fees alone to litigate the case in foreign court.[34]

In addition to fraud proceeds moving off-shore quickly, fraudulent online operators may be beyond the reach of the Commission and U.S. courts, practically if not legally. There is now limited recognition of civil judgments from country to country. Even if the Commission were to bring an action and obtain a judgment against a foreign firm that has defrauded U.S. consumers, the judgment might be challenged in the firm's home country, and the ability to collect any consumer redress might be frustrated. In light of this possibility, U.S. law enforcement must look for more effective remedies available under U.S. law and must work more cooperatively with law enforcement officials in other countries. To that end, the FTC has executed cooperation memoranda with agencies in Canada, the United Kingdom, and Australia.[35]

The Commission's actions in *FTC v. Pereira* represent significant strides in the right direction. In that case, the Commission realized that the defendants' "pagejacking" and "mousetrapping" scheme had operated through Web sites registered with a U.S.-based company. Thus, in its request for a temporary restraining order and preliminary injunction, the Commission asked that the registrations for these Web sites be suspended, thereby effectively removing the defendants and their deceptive Web sites from the Internet, pending a full trial. At the same time, the Commission reached out to its international colleagues in Portugal and Australia. The Australian Competition and Consumer Commission (ACCC) proved especially helpful in providing information about the defendants and their business operations in Australia. The ACCC also began its own investigation, executed a number of search warrants, and began pursuing potential legal action against the defendants in that country.

III. Consumer and Business Education

Law enforcement alone cannot stop the tide of fraudulent activity on the Internet. Meaningful consumer protection depends on education as well. Consumers must be given the tools they need to spot potentially fraudulent promotions, and businesses must be advised about how to comply with the law. The FTC's consumer and business education program uses the Internet to communicate anti-fraud and educational messages to reach vast numbers of people in creative and novel ways quickly, simply and at low cost. As more consumers and businesses come online, use of the Internet to disseminate information will grow.

A. Fraud Prevention Information for Consumers

More than 200 of the consumer and business publications produced by the FTC's Bureau of Consumer Protection are available on the agency's Website in both text and .pdf format. Indeed, the growth in the number of our publications viewed online between 1996 and 1999 (140,000 vs. 2.5 million) tells the story of the Internet's coming of age as a mainstream medium and highlights its importance to any large-scale dissemination effort. Those 2.5 million page views are in addition to the 6 million print publications the FTC distributes each year to organizations that disseminate them on the FTC's behalf.

B. Link Program

In addition to placing publications on its own Web site, the FTC actively encourages partners - government agencies, associations, organizations, and corporations with an interest in a particular subject - to link to its information from their sites and to place banner public service announcements provided by the FTC on their sites. Links from the banners allow visitors to click through to the FTC site quickly to get the information they're looking for exactly when they want it. Examples of the varied organizations that have helped drive traffic to the valuable consumer information on *http://www.ftc.gov/* are Yahoo!, American Express, Circuit City, AARP, North American Securities Administrators Association, the Alliance for Investor Education, the Better Business Bureau, CBS, motleyfool.com, the U.S. Patent and Trademark Office, Shape Up America!, the National Institutes of Health, and the Arthritis Foundation.

C. "Teaser" Pages

Too often, warning information about frauds reaches consumers after they've been scammed. For the FTC, the challenge is reaching consumers before they fall victim to a fraudulent scheme. Knowing that many consumers use the Internet to shop for information, agency staff have developed teaser sites that mimic the characteristics that make a site fraudulent and then warn the reader about the fraud. Metatags embedded in the FTC teaser sites make them instantly accessible to consumers who are using major search engines and indexing services as they look for products, services and business opportunities online. The teaser pages link back to the FTC's page, where consumers can find practical, plain English information. The agency has developed more than a dozen such teaser sites on topics ranging from fraudulent business opportunities and wealth-building scams to weight loss products, vacation deals and investments.[36] Feedback from the public has been overwhelmingly positive: visitors express appreciation -- not only for the information, but for the novel, hassle-free and anonymous way it is offered.

D. Consumer.gov.

Following its vision of the Internet as a powerful tool for consumer education and empowerment, the FTC organized a group of five small federal agencies in 1997 to develop and launch a Web site that would offer one-stop access to the incredible array of federal consumer information. On the theory that consumers may not know one federal agency from another, the information is arranged by topic area. Federal agencies have responded well to *consumer.gov*. The site now includes contributions from 170 federal agencies. Consumers also find it useful, with over 182,500 visits to the site recorded in the first half of FY 2001.

Visitors to *consumer.gov* find special initiatives, too: The President's Council on Y2K Conversion asked the FTC to establish a Y2K consumer information site; the Quality Interagency Coordination Task Force requested a special site on health care quality; and the U.S. Postal Inspection Service asked that *consumer.gov* house the site to support the **kNOw Fraud** initiative, an ongoing public-private campaign initiated with the sending of postcards about telemarketing fraud to 115

million American households in the fall of 1999.[37] The FTC continues to maintain the site.

E. Business Education for Online Marketers

As part of its mission, the FTC provides guidance to online marketers on how to assure that basic consumer protection principles apply online. Many of these entrepreneurs are small, start-up companies that are new to the Internet and to marketing in general and are unfamiliar with consumer protection laws. The Commission's publication, *Advertising and Marketing on the Internet: Rules of the Road*, is designed to give practical, plain-English guidance to them.[38] FTC also has used a variety of other approaches to get its messages out to the business community, from posting compliance guides, staff advisory letters and banner public service announcements on the Web to speaking at industry and academic meetings and conferences, using the trade press to promote the availability of information on the agency site, and holding workshops on online issues and posting the transcripts. Most recently, on January 30 of this year, the Commission, in cooperation with the Electronic Retailing Association presented "Etail Details" a case-driven Internet marketing seminar for Internet retailers, marketers, and suppliers on applying offline rules and regulations online. The seminar was designed to ensure etailers understand and comply with FTC rules regarding etailing.

IV. Conclusion

The Commission has been involved in policing the electronic marketplace for six years - before the World Wide Web was widely used by consumers and businesses. So far, we have kept pace with the unprecedented growth of the electronic marketplace by targeting our efforts, making innovative use of the technology, and leveraging our resources. We have done all this with limited resources, and without retreating from our important consumer protection work in traditional markets.

The Commission greatly appreciates the opportunity to describe its efforts to combat fraud on the Internet.

---

1. The views expressed in this statement represent the views of the Commission. My responses to any questions you may have are my own and are not necessarily those of the Commission or any Commissioner.

2. The FTC has limited or no jurisdiction over specified types of entities and activities. These include banks, savings associations, and federal credit unions; regulated common carriers; air carriers; non-retail sales of livestock and meat products under the Packers and Stockyards Act; certain activities of nonprofit corporations; and the business of insurance. *See, e.g.*, 15 U.S.C. §§ 44, 45, 46 (FTC Act); 15 U.S.C. § 21 (Clayton Act); 7 U.S.C. § 227 (Packers and Stockyards Act); 15 U.S.C. § 1011 *et seq.* (McCarran-Ferguson Act).

3. 15 U.S.C. § 45(a). The Commission also has responsibilities under more than 45 additional statutes, *e.g.*, the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, which establishes important privacy protections for consumers' sensitive financial information; the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.*, which mandates disclosures of credit terms; and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et. seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 35 rules governing specific industries and practices, *e.g.*, the

Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; and the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices.

4. 15 U.S.C. §§ 45(a) and 53(b).

5. Pew Internet and American Life Project, *More Online, Doing More* (reported at http://www.pewinternet.org/reports/toc.asp?Report=30) (stating that comparing figures gathered in tracking survey in May and June with figures gathered between Thanksgiving and Christmas, the number of American adults with Internet access grew from about 88 million to more than 104 million in the second half of 2000).

6. Jupiter Communications, Inc., *Online Holiday Sales Increased by 54 percent this Holiday Season, Despite Dot Com Closures and Soft Offline Purchase* (Jan. 17, 2001) (estimating Nov. and Dec. 2000 online sales of $10.8 billion, compared to $7 billion for those months in 1998) (reported at www.jup.com/company/pressrelease.jsp?doc=pr010117). The Census Bureau of the Department of Commerce estimated that in the fourth quarter of 2000, not adjusted for seasonal, holiday, and trading-day differences, online retail sales were $8.686 billion, an increase of 67.1 percent from the 4th quarter of 1999 (reported at www.census.gov/mrts/www/current.html).

7. *Id.*

8. To date the Commission has collected more than $55 million in redress for victims of Internet fraud and deception.

9. These figures are based on estimated annual fraudulent sales by defendants in the twelve months prior to filing the complaint. Fraudulent sales figures are based on, among other things, financial statements, company records, receiver reports, and deposition testimony of company officials.

10. *See* www.consumer.gov/sentinel.

11. The CRC now receives over 12,000 inquiries and complaints per week. They cover a broad spectrum -- everything from complaints about get-rich-quick telemarketing scams and online auction fraud, to questions about consumer rights under various credit statutes and requests for educational materials. Counselors record complaint data, provide information to assist consumers in resolving their complaints, and answer their inquiries.

12. In 1998, the Interagency Resources Management Conference Award recognized Consumer Sentinel as an exceptional initiative to improve government service.

13. U.S. agencies participating included the Commodity Futures Trading Commission, the Department of Justice, the Securities and Exchange Commission and the United States Postal Inspection Service.

14. Participants in "Operation Top Ten Dot Cons" included consumer protection agencies from Australia, Canada, Finland, Germany, Ireland, New Zealand, Norway, the United Kingdom and the United States.

15. Cases were brought by the Attorneys General of Arizona, Colorado, Florida, Illinois, Iowa, Indiana, Louisiana, Maryland, Massachusetts, Michigan, Missouri, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, Tennessee, Texas, and Washington State. Consumer protection offices in West Virginia, and Wisconsin also took action, as did the Louisiana Department of Justice, the Oklahoma Department of Securities, and the Washington State Securities Division.

16. The SEC's contribution to this project consisted of 77 cases.

17. "Web cramming" is a type of unauthorized billing scam. Web crammers call their victims-often small businesses-and offer a "free" Web page; then they start billing the victims, typically on their monthly telephone statements, without authorization. In many cases the small business victims are not even aware that they have a web site or are paying for one.

18. Telephone/Pay-Per-Call Solicitation Frauds are schemes that exploit the telephone billing and collection system to charge consumers for telephone-based entertainment programs ("audiotext"

in industry parlance) or other so-called "enhanced services" that are not telecommunications transmission but are often billed on consumers' telephone bills. Modem dialers and videotext schemes, like the operation attacked in *FTC v. Verity International,* No.00 Civ. 7422(LAK) (S.D.N.Y. 2000), described *infra,* are ones that, unbeknownst to a consumer, cause his or her computer modem to disconnect from his or her usual Internet service provider, dial an expensive international telephone number, and reconnect to the Internet at a remote location overseas, charging the consumer as much as $5.00 or more per minute for as long as the consumer continues online.

19. Consumer Sentinel has also been upgraded and expanded to provide participants access to the Identity Theft Data Clearinghouse, the central repository for federal identity theft complaints

20. The FTC recently has signed an agreement with the Department of Defense to collect consumer complaint from men and women serving in the military through a project called "Soldier Sentinel."

21. The FTC has coordinated or co-sponsored the following Surf Days, listed by date of their announcements: Pyramid Surf Day (Dec. 1996), Credit Repair Surf (April 1997), Business Opportunity Surf Day (April 1997), Coupon Fraud Surf Day (Aug. 1997), North American Health Claims Surf (Oct. 1997), HUD Tracer Surf Day (Nov. 1997), International Surf Day (Oct. 1997), Kids Privacy Surf Day (Dec. 1997), Junk E-mail Harvest (Dec. 1997), Privacy Surf (March 1998), Textile and Wool Labeling Surf (Aug. 1998), Y2K Surf (Sept. 1998), International Health Claims Surf (Nov. 1998), Investment Surf Day (Dec. 1998), Jewelry Guides Surf (Jan. 1999), Pyramid Surf Day II (March 1999), Green Guide Surf (April 1999), Coupon Fraud II Surf Day (June 1999), Jewelry Guides Surf II (January 2000), Scholarship Services Surf (January 2000), GetRichQuick.con Surf (March 2000), False or Unsubstantiated Lice Treatment Claims Surf (April 2000), Credit Repair Surf II (Aug. 2000), Childrens' Online Privacy Protection Act Compliance Surf (Aug. 2000), False Claims of Authenticity for American Indian Arts and Crafts Surf Day (Oct. 2000), and TooLate.Com [Surf of Online Retailers' Compliance with the Mail or Telephone Order Merchandise Rule] (Nov. 2000).

22. Pyramid operators typically promise enormous eamings or investment returns, not based on commissions for retail sales to consumers, but based on commissions for recruiting new pyramid members. Recruitment commissions, of course, are premised on an endless supply of new members. Inevitably, when no more new recruits can be found, these schemes collapse and a vast majority of participants lose the money they invested.

23. To date, the Commission has collected about $42.6 million in these cases.

24. *FTC v. Fortuna Alliance, L.L.C.,*, No. C96-799M (W.D. Wash. 1996). *See also, FTC v. JewelWay International, Inc.*, No. CV97-383 TUC JMR (D. Ariz. 1997) ($5 million in redress for approximately 150,000 investors); *FTC v. Nia Cano,* No. 97-7947-CAS-(AJWx) (C.D. Cal. 1997) (approximately $2 million in redress); *FTC v. FutureNet,* No. 98-1113GHK (AIJx) (C.D. Cal. 1998) ($1 million in consumer redress). *FTC v. Five Star Auto Club, Inc.,* 97 F. Supp. 2d 502 (S.D.N.Y. 2000). ($2.9 million in consumer redress); *FTC v. Equinox International Corp.,* No CV-S-990969-JBR-RLH (D.Nev. 1999) (pyramid promoted through many devices, including some use of the Internet; $50 million in consumer redress).

25. *FTC v. Five Star Auto Club, Inc.*, 97 F. Supp. 2d 502 (S.D.N.Y. 2000).

26. *FTC v. Verity International, Ltd.*, No. 00 Civ. 7422 (LAK)(S.D.N.Y. 2000).

27. Other modem hijacking cases include *FTC v. Audiotex Connection, Inc.*, No. CV-97-0726 (DRH) (E.D.N.Y. 1997) (final stipulated injunction halting the unlawful practice and order that 27,000 victims receive full redress totaling $2.14 million); *FTC v. RJB Telcom, Inc.*, No.CV 00-2017 PHX SRB (D. Az. 2000); *FTC v. Ty Anderson,* No. C 00-1843P (W.D. Wa. 2000).

28. *FTC v. Carlos Pereira d/b/a atariz.com*[(29)]

29. Civil Action No. 99-1367-A)

30. *FTC v. Benoit (previously FTC v. One or More Unknown Parties)*, No. 3:99 CV 181 (W.D.N.C. 1999). In the course of the litigation, Commission attomeys were able to identify the operators of the scheme.

31. "Audiotext" services are telephone-based entertainment or information services.
32. *See* Bureau of Consumer Protection, Federal Trade Commission, *Anticipating the 21st Century: Consumer Protection in the New High-Tech, Global Marketplace*, iii (May 1996), and *Looking Ahead: Consumer Protection in the Global Electronic Marketplace* (September 2000).
33. *FTC v. J.K. Publications*, No. 99-000-44ABC (AJWx)(C.D. Cal. 1999).
34. In this case, the Department of Justice's Office of Foreign Litigation paid $50,000 up front, and the U.S. court ordered the defendants to pay the remaining $230,000 in fees. In other cases, the Commission may have to bear all or most of the cost of litigating in foreign court.
35. The Commission is increasingly cooperating with international colleagues in a number of venues. Among them is the International Marketing Supervision Network, a group of consumer protection agencies from the 30 countries that are members of the Organization for Economic Cooperation and Development.
36. The titles of the teaser sites are: Looking for Financial Freedom?; The Ultimate Prosperity Page; Nordicalite Weight Loss Product; A+Fast Ca$$h for College; EZTravel: Be an Independent agent; EZTravel: Certificate of Notification; EZToyz Investment Opportunity; HUD Tracer Association; CreditMenders Credit Repair; NetOpportunities: Internet is a Gold Mine; National Business Trainers Seminars; VirilityPlus: Natural Alternative to Viagra; ArthritiCure: Be Pain-Free Forever.
37. The original *consumer.gov* team received the Hammer Award, presented by the Vice President to teams of federal employees who have made significant contributions to reinventing government.
38. There has been an astonishing growth in page views of this publication in the past year: from 33,448 views in FY 1999 to 110,473 in FY 2000 .