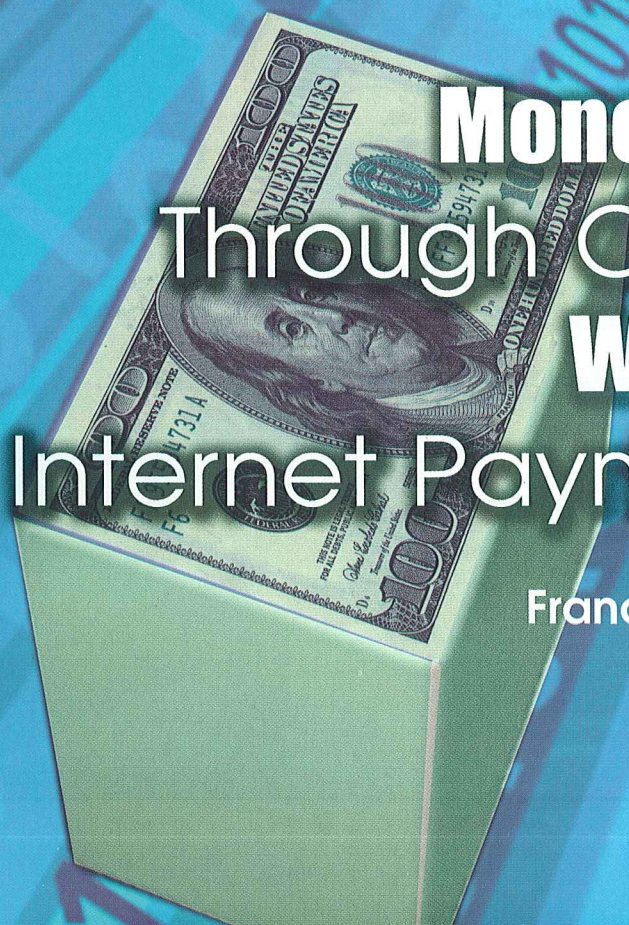
Lavado de dinero [1] a través de páginas Web comerciales y Sistemas de Pagos por Internet



Money laundering [1] Through Commercial Web Sites and Internet Payment System

Francisco Guadamillas Cortéz
Profesor Invitado de la UTE

Se sabe que el Internet es un medio o plataforma potencial para el desarrollo del crimen organizado, pero el Grupo de Acción Financiera (GAFI-FATF – Financial Action Task Force) identificó nuevas vulnerabilidades del sistema en uno de sus últimos reportes.[2]

El abuso de las páginas comerciales como "eBay" y de los sistemas de pago por Internet como "PayPal" es un método moderno de lavado de dinero, el cual va a ser considerado en este artículo muy detenidamente.

Los criminales usan una gran variedad de mecanismos para lavar las ganancias de sus actividades criminales e ilícitas y para financiar el terrorismo, e inclusive utilizando el sistema financiero formal, el movimiento físico del efectivo por correo y por movimiento de activos a través de negociaciones.

Al pasar de los años, el Grupo de Acción Financiera (GAFI-FATF) ha puesto mucha atención a estos mecanismos y su modus operandi. Con suerte, este esfuerzo se está desarrollando e incrementando aún más en la vigilancia y la experiencia de los sectores públicos y privados; y de esta manera se hace más difícil para los criminales lavar el dinero de las ganancias de sus actividades criminales e ilícitas y financiar el terrorismo utilizando los métodos ya identificados.

No obstante, los criminales han encontrado nuevas maneras y métodos para lavar el dinero de las ganancias de sus actividades criminales e ilícitas y para financiar el terrorismo. En este contexto las páginas comerciales y los sistemas de pago por Internet están sujetos a una gran variedad de vulnerabilidades que pueden ser explotadas por las organizaciones criminales y las personas que financian el terrorismo.

Al saber que este sector está en riesgo de ser utilizado como método de lavado de dinero o para financiamiento del terrorismo, los funcionarios de estado han sido alertados para comenzar a regular el comercio electrónico y en particular los sistemas de pago por Internet.

That the internet is a potential platform for organized crime is nothing new. But the FATF, Financial Action Task Force, has now identified some new vulnerabilities on one of their latest report.[2]

The misuse of commercial websites like "eBay" and of internet payment systems like "Pay Pal" is a modern method of money laundering which will be therefore considered in this article more closely.

Criminals use a wide variety of mechanisms to launder the proceeds of their criminal activities and to finance terrorism, including using the formal financial system, the physical movement of cash by couriers and the movement of value through trade.

Over the years, the Financial Action Task Force (FATF) has focused considerable attention on these mechanisms and their related typologies. Hopefully, this effort is increasing the vigilance and experience of both the private and public sectors, making it harder for criminals to launder the proceeds of their criminal activities and to finance terrorism, using identified methods.

However, criminals have shown adaptability and opportunism in finding new channels to launder the proceeds of their illegal activities and to finance terrorism. In this context, commercial websites and Internet payment systems appear to be subject to a wide range of vulnerabilities that can be exploited by criminal organizations and terrorist financiers.

Faced with the risk that this sector can be used to launder money or finance terrorism, government officials have been called on to start regulating electronic commerce and in particular Internet payment systems.

1.- Cp. Guadamillas Cortes, Francisco J.: Die potentielle Gefahr der Gelwasche durch Zahlungssystem e im Internet und kommerziellen Webseiten, 2008, Grin Verlag
2.- Cp. FATF-GAFI: Money Laundering & Terrorist Financing vulnerabilities of commercial websites and Internet Payment Systems, Report, 18.06.2008

"Pecunia non olet"[3] - El dinero no huele. Esta expresión del emperador romano Titus Flavius Vespasianus es totalmente cierta para este caso del Internet. El acceso global, el anonimato, la rapidez y las diferentes formas de pago son particularmente atractivos para el crimen organizado que utilizan las páginas comerciales y los sistemas de pago.

Las páginas comerciales pueden ser clasificadas en cinco categorías:[4]

1.- Por medio de cliente a cliente. Páginas que permiten a personas particulares vender por medio de mercados en línea.

2.- Por medio de negocio a cliente. Páginas que permiten que muchos comerciantes vendan a los consumidores por medio de mercados en línea.

3.- No directo - cliente a cliente (por ejemplo por medio de carteleras, diarios y clasificados en línea). Estas páginas permiten a los clientes hacer publicidad o anunciar los bienes que ellos quieren vender.

4.- Directamente negocio – cliente. Comerciante que venden bienes a clientes por medio de sus propias páginas Web.

5.- Directamente negocio – negocio. Páginas que permiten que los comerciantes vendan directamente a otros comerciantes.

La mayor diferencia está en la "oferta directa" por un lado y la "oferta por medio de la plataforma" por otro lado.

En este artículo nos vamos a enfocar en la primera categoría de las páginas comerciales. Las páginas de Cliente a Cliente son populares y de fácil acceso, abiertas al público y facilitan el gran volumen de las transacciones de negocios internacionales. Como tal, estas páginas y sitios Web son propensos y sensibles para un mal uso por parte de los criminales. Este tipo de páginas comerciales facilitan las transacciones entre los sectores privados en vez de dar solamente información del vendedor con cualquier transacción que tenga lugar sin estar en línea o conectados.

En su libro "The Shade of eBay" Walter Egon Glöckel dice:[5]

"Créanlo o no, los criminales ganan sus utilidades con una gran sonrisa en sus caras, gracias a la impotencia del sistema legal de eBay…"

Las páginas comerciales y los proveedores de sistemas de pago por Internet pueden ser utilizadas para transacciones ilegales, incluyendo la venta ilegal de drogas, armas, armas de fuego, productos falsificados y pornografía infantil o facilitar el fraude. Los proveedores de sistemas de pago por Internet pueden ser utilizados después de todo para lavar las ganancias de estas actividades ilegales.

"Pecunia non olet"[3] – money doesn't smell. This declaration of the Roman Emperor Titus Flavius Vespasianus is definitely true for the internet. Global access, anonymity, speed and the different forms of payment seems to be in particular attractive for organized crime dealing with commercial websites and payment systems.

Commercial websites can be divided into five categories:[4]

1. Mediated customer-to-customer, sites that allow private individuals to sell to one another via an online marketplace.

2. Mediated business-to-customer, sites that allow multiple merchants to sell to consumers via an online marketplace.

3. Non-mediated customer-to-customer (*i.e.* Bulletin board services and online classifieds), sites that only allow customers to advertise goods they want to sell.

4. Direct business-to-customer, merchants that sell goods to consumers via their own websites.

5. Direct business-to-business websites, merchants selling to merchants.

The main differentiator is the "direct offer" on one side and the "offer through a mediated platform" on the other side.

In this article we will focus on the first category of commercial websites. Mediated customer-to-customer sites are popular, easy to access, open to the public, and facilitate a high volume of cross border trade transactions. As such these sites are easily susceptible to criminal misuse. This type of commercial website facilitates transactions between private parties as opposed to simply providing seller contact information with any transactions occurring off-line.

In his book "the shade of eBay" Walter Egon Glöckel says:[5]

"… believe it or not, the criminals profit with a bride smile on her faces from the helplessness of the legal systems concerning eBay…"

Commercial websites and Internet payment service providers can be used for illegal transactions, including the sale of illegal drugs, weapons, firearms, counterfeit products and child pornography, or to facilitate fraud. Internet payment service providers can be used afterwards to launder the proceeds of these illegal activities.

3.- Note: Titus Flavius Vespasianus, Roman Emperor, reigned 69-79 a.C.
4.- Cp. FATF-GAFI: Money Laundering & Terrorist Financing vulnerabilities of commercial websites and Internet Payment Systems, Report, 18.06.2008 p.6
5.- Cp. Glöckel, Walter Egon: Der Schatten von eBay, in: www.der-chatten-von-ebay.com, last view 07.04.2009

En este artículo, el término de "Sistema de pago por Internet" en términos generales, es utilizado para describir a una compañía de Internet que proporciona servicios de transacciones financiaras a sus clientes. Además, en muchos casos, el sistema de pago por Internet consiste de una institución financiera, no necesariamente un banco y que pueda o no estar sujeta a una vigilancia reguladora, dependiendo de las jurisdicciones legales de donde dicho sistema provea de servicio a los consumidores. Los consumidores prefieren este sistema de pagos por Internet ya que son convenientes y sirven como una alternativa para hacer pagos por medio de cuentas bancarias o tarjetas de crédito que no todo el mundo tiene acceso.
Considerando el riesgo que afecta a las páginas comerciales de Internet y a los proveedores de sistemas de pagos por Internet, una distinción debe ser realizada entre las actividades económicas de las páginas comerciales de Internet y el pago relacionado con las actividades comerciales (Servicios de pago por Internet), a pesar de que algunas páginas comerciales son aparentemente proveedoras tanto de actividades comerciales como de servicio financiero asociado.

Las principales características de las páginas comerciales de Internet, que a través de una o todas pueden ser relacionadas, son las siguientes:[6]

- Una simple conexión de Internet es suficiente para abrir una cuenta de Internet con una página comercial y comprar y vender objetos en el Internet.

- Las páginas comerciales de Internet pueden ser fácilmente consultadas o visitadas en cualquier lugar del mundo.

- Un cliente puede tener acceso desde su propia conexión de Internet o por parte de terceros (por ejemplo: desde un café Internet o locales de llamadas telefónicas que proveen servicio de Internet) o cualquier otro punto de conexión en el cual el cliente no está registrado.

For purposes of this article, the term Internet payment system is used to broadly describe an Internet-based company that provides financial transaction services to consumers. Furthermore, in most instances, Internet payment systems consist of non-bank financial institutions that may or may not be subject to regulatory oversight depending upon the legal jurisdictions of where such systems provide services to consumers. Consumers are attracted to Internet payment systems because such systems often are convenient, and serve as an alternative to making payments via a bank account or credit card which may not be available to everyone.

Considering the risks affecting commercial websites and Internet payment service providers, a clear distinction must be made between the business activities of commercial websites and the payment associated with these commercial activities (Internet payment services), even if some commercial websites are apparently providing both commercial activities and the associated financial service.

The main characteristics of commercial websites, whereby they can show one or all, are the following ones:[6]

- A simple Internet connection is sufficient to open an Internet account with a commercial website and to buy and sell items on the Internet.

- Websites can potentially be accessed from any location in the world.

- A customer can gain access from his own Internet connection or from the Internet connection of a third party (*e.g.* cyber cafes or phone shops that provide Internet access) or another access point that is not registered to the customer.

6.- Cp. FATF-GAFI: Money Laundering & Terrorist Financing vulnerabilities of commercial websites and Internet Payment Systems, Report, 18.06.2008 p. 7-8

• Un cliente puede estar registrado en un país y conectarse de otro país.

• Registrarse o crear una cuenta es muy fácil y rápido (solo toma unos pocos minutos para crear una cuenta).

• Para crear una cuenta no existe la vinculación persona a persona.

• Muy poca información se necesita para abrir una cuenta.

• No se necesita verificar la identidad del cliente en algunos casos.

• Una cuenta de correo anónima puede ser utilizada para tener contacto con el cliente.

• Las transacciones comerciales son realizadas rápidamente. Los mensajes de correo electrónico son utilizados para informar al vendedor que el objeto que él puso en venta fue vendido.

• Los clientes tienen acceso a una gran variedad de páginas comerciales que se encuentran localizadas alrededor del mundo.

• Los bienes u objetos ofertados pueden ser vendidos por un precio fijo o de acuerdo a subasta. Por ejemplo, en páginas de subasta, el precio puede estar establecido por el vendedor o por los diferentes compradores, creando así, incertidumbre en el mercado acerca del verdadero valor de los bienes que son vendidos.

• A customer can register in one country and connect from another country.

• Registration is very easy and very rapid (only a few minutes are necessary to register).

• Registration is non face-to-face.

• A limited amount of information is required to register.

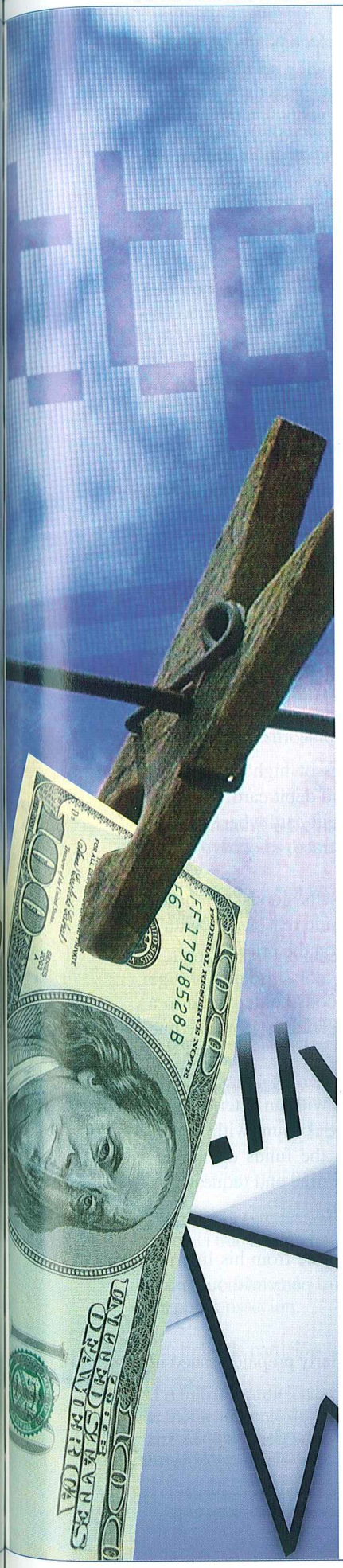
• No procedure to verify customer identification in certain cases.

• Anonymous e-mail addresses may be used as customer contact information.

• Commercial transactions are performed very rapidly. E-mail messages are used to inform the seller that the item he put on sale has been sold.

• Customers have access to a wide range of items (from small value items to high value items) on sale on a wide range of commercial websites located all over the world.

• Goods can be sold for either a fixed or variable price. For example, on auction sites, the price may be set by the seller or by different buyers, creating uncertainty over the true market value of the goods being sold.



• Las páginas comerciales pueden facilitar un convenio financiero o de venta, pero deja los arreglos de envío para ser discutidos por los compradores y vendedores. Normalmente, si no se envía algún producto o bien, es cuando el comprador tiene o presenta alguna queja.

Estas características pueden llevar al lavado de dinero, es así que, muchas nuevas leyes han sido establecidas internacionalmente, como en Alemania la nueva "Geldwäschereibekämpfungsergänzungsgesetz" (GwBekErgG) del 2008, la ley en contra del lavado de dinero, basada en la Ley número tres (3) de la Directiva Europea en Contra del lavado de Dinero del 26.10.2005.

Conocer a su cliente (KYC know-your-client) y verificación de la información suministrada por cliente (CDD Client-Due-Diligence), también para eBay y otras plataformas similares, es la clave que enfoca la directiva.

No sólo las páginas comerciales tienen un gran potencial de ser utilizadas de forma errónea para lavado de dinero, también los sistemas de pago por Internet son utilizados con el mismo propósito.

Antes un usuario del sistema de pagos por Internet podía hacer una transferencia de fondos por medio del sistema. Generalmente, primero el usuario debe consolidar la transferencia. El consolidar una transferencia por medio de un sistema de pago de Internet requiere que el usuario consolide o tenga una "cuenta" de la cual los fondos van a ser retirados para transacciones o transferencias posteriores o proporcionar al sistema de pagos por Internet una cantidad equivalente a los fondos que el usuario desea transferir. Esto dependerá de las operaciones de un sistema de pagos de Internet específico. El usuario puede tener varias opciones para consolidar la transacción y puede no estar limitado o no tener límites en el uso de su tarjeta de crédito o de su cuenta bancaria.

• Commercial websites may facilitate sale and financial settlement but leave delivery arrangement to buyers and sellers. Often, the only indication of non-delivery of goods will be if the buyer complains.

These characteristics could lead to money laundering; therefore, many new regulations have been put in place internationally, like in Germany the new "Geldwäschereibekämpfungsergänzungsgesetz (GwBekErgG) from 2008, the law against money laundering based on the 3. European Anti Money Laundering Directive from 26.10.2005.

Know-your-client (KYC) and Client-Due-Diligence (CDD), also for eBay and other similar platforms, is the key focus of the directive.

Not only the commercial websites have a big potential for being misused for money laundering, but also the Internet Payment Systems.

Before a user of an Internet payment system can do a transfer of funds through the system he generally must first fund the transfer. Funding a transfer through an Internet payment system may involve funding an "account" from which funds will be drawn for subsequent transactions or transfers, or providing the Internet payment system with the equivalent amount of funds the user wishes to transfer. Depending upon the operations of a given Internet payment system, the user may have several options for funding a transaction, and may not be limited to the use of the user's credit card or personal bank account.

De esta manera uno puede detectar actividades potenciales de lavado de dinero. Las siguientes características han sido identificadas como las utilizadas y son "indicadores de riesgo (red flags)":[7]

• El cliente abre una cuenta individual de Internet con sistema de pago en un país pero ingresa en su cuenta o a la página regularmente desde otro sitio u otros países.

• La cuenta que fue abierta por el cliente es manejada con fondos que son transferidos desde un tercer país.

• El cliente comienza a comprar objetos o bienes en el Internet por cantidades de dinero que no acostumbra o que son diferentes al perfil de transacciones que ha realizado anteriormente.

• El cliente deposita su cuenta de Internet con efectivo, si es que el proveedor del sistema de pagos por Internet permite que se deposite efectivo.

• Si a la cuenta del cliente con proveedor de sistema de pagos se le realiza depósitos que son transferidos por un tercero que aparentemente no tiene nada que ver con el cliente.

• Las transacciones del cliente de repente no tienen nada que ver con su perfil de transacciones previas después de que a su cuenta se ha realizado depósitos con dinero de un tercero.

• El cliente realiza compras de objetos de alto valor diariamente y con una tarjeta de débito prepagada, una tarjeta de crédito prepagada y anónima o una tarjeta de regalo de la cual el origen de los fondos es difícil de rastrear.

• El cliente aparentemente revende los bienes comprados con anterioridad sin ninguna razón económica o con un descuento significativo o sube el precio del objeto o del bien adquirido.

• El comprador pide que los objetos comprados sean enviados a una agencia de correos o a una dirección distinta a la que fue registrada en la apertura de cuenta.

• Un cliente abre una cuenta con un proveedor de sistema de pagos por Internet y hace depósitos significativos, y deja los fondos en la cuenta por un período de tiempo y solicita reembolso o amortización de los mismos.

• Un cliente que pide un estado de cuenta de su cuenta de Internet para ser transferido a una tercera cuenta sin que tenga ninguna relación con el mismo.

• El uso de tarjetas de crédito principalmente las prepagadas y expedidas en otro país.

• Un cliente que venda objetos o bienes ilegales que aparezcan en la lista de objetos prohibidos.

Here very often one could detect potential money laundering activities. The following so called "Red-Flags indicators" have been identified:[7]

• The customer opens his individual Internet account with the payment service provider in one country but logs in regularly on the website from a single or multiple third countries.

• The account opened by the customer is loaded with funds transferred from a third country.

• The customer starts to purchase items on the Internet for amounts not in line with his previous transactions profile.

• The customer loads his Internet account with cash, if the Internet payment services provider allows loading with cash.

• The customer account with payment service provider is loaded with funds transferred by a third party apparently not related to the customer.

• The transactions of the customer suddenly deviate from its previous transactions profile after his customer account had been loaded with money from a third party.

• The customer purchases items of high value items on a regular basis with a prepaid debit card, an anonymous prepaid credit card or a gift card where the origin of the funds is difficult to retrace.

• The customer apparently resells goods purchased beforehand, without any economic reasons, or with a significant discount or increase on the price.

• The buyer requests that the goods be delivered to a post office box or to a different address from the one registered to the account.

• A customer opens an account with an Internet payment service provider, loads the account with important amounts of money, leaves the funds on the account during a certain period of time and requests the redemption of the funds later on.

• A customer requesting the balance from his Internet account to be transferred to a third party without apparent relation with him.

• The use of credit cards, particularly prepaid, issued in a foreign country.

• A customer sells illegal items or the goods appear on a list of forbidden items.

7.- Cp. FATF-GAFI: Money Laundering & Terrorist Financing vulnerabilities of commercial websites and Internet Payment Systems, Report, 18.06.2008 p. 21-22

• Los productos comprados son enviados regularmente a otro país.

• El cliente usa una tarjeta de crédito expedida por un banco del exterior o en un país que no coopere con el Grupo de Acción Financiera (GAFI-FAFT).

• Los fondos son de un país que no coopera con el Grupo de Acción Financiera.

• Que el país de origen del cliente sea conocido como un país que no coopera con el GAFI-FATF y que no luche en contra del lavado de dinero y del financiamiento al terrorismo.

• Un cambio inesperado y dramático de una página comercial recientemente establecida o un crecimiento inesperado en el valor de la página comercial después de algunas ventas.

El comportamiento puede ser sospechoso cuando algunos indicadores se dan lugar. El Grupo de Acción Financiera ha pedido a todos los países miembros que pongan sus leyes en orden para prevenir el mal uso de estas páginas comerciales. Singapur es uno de los países que ya ha establecido sus leyes.[8]

Los riesgos del lavado de dinero basados en páginas comerciales de Internet y sistemas de pagos por Internet pueden ser también clasificados de acuerdo al Modelo de tres fases de los Servicios de Aduana de los EE.UU., Colocación, Distribución e Integración:

Colocación:

• Anonimato de los clientes en ciertas páginas comerciales y proveedores de sistemas de pagos por Internet.

• Las relaciones con los clientes cuando no existe una relación presencial.

• La posibilidad de tener algunas cuentas con diferentes registros e información.

• Acceso remoto a algunas páginas comerciales y sistemas de pagos por Internet.

• Anonimato "relativo" asociado con ciertos métodos de pago.

Distribución:

• La velocidad del movimiento o transacción.

• El carácter internacional y el problema jurisdiccional de donde la transacción tiene lugar.

• El gran volumen del número de transacciones y cantidades por transacción.

• La limitada participación del ser humano.

• La falta o insuficiencia de pistas para una auditoría, falta de mantenimiento de archivos de movimientos de la cuenta o de reporte de transacciones sospechosas por ciertos proveedores de sistemas de pagos por Internet.

• The purchased goods are regularly shipped to a foreign country.

• The customer uses a credit card issued by a bank in an offshore centre or in a FAFT non-cooperative country.

• The funds originate from a non-cooperative country.

• The country of origin of the customer is known by the FATF as a non-cooperative country in the fight against money laundering or terrorism financing.

• An unexpected turnover for a recently established commercial website or an unexpected increase in the value of the commercial website after a few sales.

Suspicious behaviour may result in particular when a set of indicators show up. The FATF has asked their member countries to put regulations in place in order to prevent the misuse. Singapore is one of the only countries which has already put regulations in place.[8]

The risks of money laundering based on commercial websites and Internet payment systems can be also classified according to the 3-phase money laundering model of the US Custom Services - Placement, Layering and Integration:

Placement:

• Anonymity of customers on certain commercial websites and Internet payment services providers.

• The relationship with customers is a non face-to-face relationship.

• The possibility to use multiple registrations.

• Remote access to commercial websites and Internet payment systems.

• Relative "anonymity" associated with certain methods of payment.

Layering:

• The speed of movement.

• The international character and the jurisdictional issue of where the transaction takes place.

• Volume - high number of transactions and amounts per transaction.

• The limited human intervention.

• The lack or inadequacy of audit trails, record keeping or suspicious transactions reporting by certain Internet payment services providers.

8.- Cp. Monetary Authority Of Singapore: "Prevention of Money Laundering and Countering of Terrorism – Holders of Stored Value Facilities", Notice PSOA-No. 2, 2007 In: www.mas.gov.sg/resource/legislation_guidelines, last view 12.12.2008

Integración

• La posibilidad de comprar objetos de gran valor.

Como resultado del alto riesgo detectado por el GAFI (FATF), han recomendado una lista de mecanismos para prevenir y luchar en contra del lavado de dinero y el financiamiento al terrorismo. Las recomendaciones son las siguientes:[9]

• Implementar grupos o equipos de seguridad que "patrullen" en el Internet a nivel mundial para detectar fraude y el mal uso de estos servicios.

• Aplicar la confirmación de datos entregados por el cliente.

• Dar una información de riesgo del cliente al momento de la apertura de la cuenta.

• Verificación de datos ingresada por los clientes (dirección de correo electrónico/ dirección IP, identificación del dueño de la tarjeta de crédito).

• Automatizar una llamada, hacer cargos al azar para verificar las identidades de los clientes.

• Enviar una carta para verificar la dirección de los clientes.

• Verificar la dirección de las tarjetas de crédito.

• Consultar bases de datos comerciales para confirmar la información entregada por los clientes.

• Hacer llamadas por el personal para obtener información adicional de los clientes.

• Límite de actividades, transacciones, envíos y retiros.

• Verificación de la fuente de los fondos.

• Tiempo real de exploración de la página comercial de los clientes, sus actividades y los objetos vendidos.

Integration:

• The possibility to buy high value items.

As a result of the high risk detected by FATF, they have recommended a list of mechanisms in order to prevent and fight against money laundering and terrorism financing. The recommendations are:[9]

• Implementing important worldwide security teams patrolling sites to detect fraud and misuse.

• Applying risk-based Customer Due Diligence.

• Scoring customer risk at opening of account.

• Risk-based verification of information entered by customers (e-mail address/IP address, identity of credit card holder …).

• Automated call, random charges to verify identities of customers.

• Sending a letter to verify customers address.

• Credit cards address verification.

• Consulting commercial databases to confirm information received from customers;

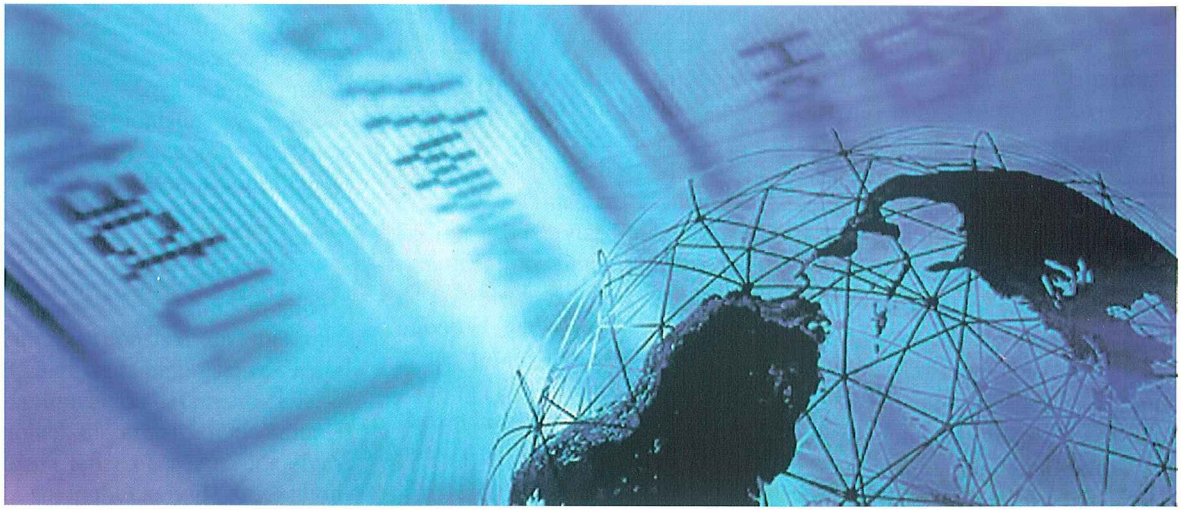
• Phone calls by staff to obtain additional information from customers.

• Activity limits, sending and withdrawals limits.

• Verification of funding source.

• Real time screening of customers, their activities and items sold.

9.- Cp. FATF-GAFI: Money Laundering & Terrorist Financing vulnerabilities of commercial websites



• Modelos de riesgo que detecten actividades anormales o de mayor volumen (con referencia a transacciones anteriores).

• Modelos de software que detecten actividades sospechosas (basados en los indicadores de riesgo "red flags").

• Revisión del manual de transacciones anormales o uso exagerado de las cuentas.

• Detectar actividades sospechosas o anormales en retiros de dinero.

• Rechazar transacciones en objetos prohibidos (drogas, armas de fuego, falsificación de productos...).

• Quitar o vedar productos ofensivos de las páginas comerciales.

• Cooperar con compañías comerciales que detecten productos falsificados y que los saquen de sus ventas.

• Analizar la evidencia física y electrónica dejada por los criminales en la red.

• Detener o posponer la transacción.

• Enviar mensajes a los clientes de las leyes que se aplican en ciertos países y transacciones.

• Promover y fomentar el reporte de objetos sospechosos que están a la venta, subastas sospechosas o comportamiento sospechoso de clientes (compradores o vendedores) – puntuar a los clientes (compradores o vendedores por cada uno).

• No aceptar o distribuir efectivo.

• Mantener pistas para auditar las transacciones comerciales y pagos.

Con el uso de los mecanismos recomendados, la lucha en contra del lavado de dinero puede tener éxito y ser efectiva, particularmente si se basa en la cooperación internacional incluyendo países "off-shore". Al implementar las reglas y mecanismos uno puede decir "El dinero no huele, el lavado de dinero sí!"■

• Monitor, using risk models built to detect bad activities:

• Risk models to detect abnormal (with regards to previous transactions) or high volume activity.

• Models/software to detect suspicious activities (based on various red flags and indicators).

• Manual review of abnormal transactions and of higher use accounts.

• Detect abnormal and suspicious activities in withdrawals.

• Refuse transactions on prohibited items (drugs, firearms, counterfeit products...).

• Remove offending items from the website.

• Cooperate with commercial company to detect counterfeit products and remove them from sales.

• Analyse the physical and electronic evidence left by criminals on the net.

• Delay a transaction.

• Display message to customers on regulation applying to certain countries and transactions.

• Encourages the reporting of suspicious items on sale, suspicious auctions or suspicious behaviour of customers (sellers or buyers) – scoring of customers (buyers and sellers by each other).

• Does not accept or distribute cash.

• Maintain full audit trails of commercial transactions and payments.

With the recommended mechanisms in place, money laundering could be fought effectively, in particular, based on international co-operation, including the off-shore countries. By implementing the rules and mechanisms one could then say: money doesn't smell, money laundering does!■