Financial Action Task Force

Groupe d'action financière

MONEY LAUNDERING & TERRORIST FINANCING VULNERABILITIES OF COMMERCIAL WEBSITES AND INTERNET PAYMENT SYSTEMS

18 June 2008

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. Criminals have shown adaptability and opportunism in finding new channels to launder the proceeds of their illegal activities and to finance terrorism. As the Internet becomes more and more a worldwide phenomenon, commercial websites and Internet payment systems are potentially subject to a wide range of risks and vulnerabilities that can be exploited by criminal organizations and terrorist groups.

2. The present study analyses money laundering and terrorist financing (ML/TF) risks associated with commercial websites and Internet payment systems with the focus on mediated customer-to-customer websites as the most vulnerable to abuse because of their popularity, accessibility (to the public), and high volume of cross border trade transactions. The analysis also provides a number of case studies that illustrate how mediated customer-to-customer websites can be exploited for ML/TF purposes.

3. The study highlights the following vulnerabilities of commercial websites and Internet payment systems: non face-to-face registration, possible anonymity of the users, speed of transactions, limited human intervention, high number of transactions, international presence, limited jurisdictional competences, difficulties for traditional financial institutions to monitor and detect suspicious financial transactions with the consequence that their abilities in the detection of suspicious financial transactions, when an Internet payment service provider is used, could be affected.

4. The study indicates that some of the ML/TF risks associated with trade-based money laundering[1] and non face-to-face business and financial transactions also apply to commercial websites and Internet payment systems. The financial transactions that are initiated from a bank account or a credit card (which is the majority of online payments) already involve a customer identification process as well as transaction record keeping and reporting obligations. While low value transactions do not necessarily equate to low risk, these transactions are subject to the regulatory controls already applicable to the financial sector and may be consequently less risky. Regarding the risks associated with the non-face-to-face registration and the possible anonymity of the users, the study highlights the need for online identity verification solutions (the electronic identity card used in certain countries for instance) to help commercial websites and Internet payment service providers mitigate the risk of criminal activity. The report also indicates that if Internet payment service providers adequately monitor the financial transactions of their customers, monitoring for and acting on deviations from the customer transaction profile, the lack of face-to-face contact at the beginning of the relationship with the commercial website and Internet payment service provider may not constitute a problem. Online and offline retail merchants and payment services should have comparable AML/CFT obligations.

5. It is also important that efforts to fight ML/TF by commercial websites and Internet payment service providers in different countries not be hampered by divergent privacy legislation, potentially interfering with the amount of customer information that service providers could exchange regarding suspected ML/TF.

---

1 FATF (2006b).

6. Although the challenges to identifying terrorist financing apply equally to Internet payment systems (the suspicions being mostly based on name matching with the names provided by the competent authorities), it is not always necessary for Internet payment service providers to identify TF in their suspicious transactions reports (STRs) in order to help counter terrorist financing. Any suspicious activity is important to report regardless of the type of activity. Some Internet payment service providers have put in place systems to detect, monitor and analyse suspicious transactions - even for small amounts.

7. Concerning the risk-based approach to combat ML/TF, we can refer to the June 2007 FATF Guidance which states that : "By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention." Applying this principle to online transactions, the private sector may be allowed to consider low value consumer payments initiated from a financial institution or credit card account (which require customer identification and verification procedures, as well as transaction record-keeping and reporting policies) to be of lower risk than transactions initiated through service providers without anti-money laundering and counter-terrorist financing (AML/CFT) obligations.

8. The risk of fraud and the sale of illegal goods are among the concerns of commercial websites and Internet payment systems. These concerns are among the motives for commercial websites and Internet payment systems to secure their communications, websites and payment systems. In some jurisdictions, online commercial websites are not as such required to detect or fight against ML/TF, but have a market incentive to detect fraud.

9. Some commercial websites and Internet payment service providers, aware of the risk of being used for illegal activity, have set up departments to screen and monitor the transactions of their customers, using a risk-based approach. In addition to monitoring for fraud, some Internet payment service providers have also set up AML/CFT mechanisms. Best practices in the sector, including customer due diligence, monitoring transactions, not accepting anonymous forms of payment (cash for instance) imposing transactions limits, maintaining transactions records, and reporting large or suspicious transactions to the competent authorities, could be helpful for other parties of the private sector.

10. The collaboration between commercial websites and Internet payment service providers to exchange information on commercial transactions underlying financial transactions is a factor which mitigates ML/TF risks, as well as risk of fraud. Legal dispositions encouraging such exchange of information could be very useful.

11. The report concludes that, as long as the sector and the relevant competent authorities understand the potential vulnerabilities associated with commercial websites and Internet payment systems and appropriate risk-based measures with regard to customer identification, record keeping and transaction reporting are taken, the mentioned issues may not necessarily constitute a higher risk for the online sector than for the offline sector.

12. The project team believes that even though awareness of ML/TF amongst major players in the online sector is increasing, due to efforts made by regulators and trade associations, efforts need to be made to increase this awareness, particularly regarding the mechanisms of ML/TF.

13. Looking ahead, the study identifies areas which could be the focus of future efforts in order to improve the capacity to cope with the identified ML/TF risks: *i)* building a better understanding amongst governmental bodies and the private sector of online ML and TF risks and related typologies and developing guidance for implementing mechanisms to detect suspicious transactions, *ii)* making traditional financial institutions aware that they still have an important role to play in the detection and

the monitoring of suspicious financial transactions, even when the payment is made via an Internet payment service provider, *iii)* given the international character of commercial websites and Internet payment systems, international cooperation is a key factor in the fight against ML and TF, *iv)* explore further ways Financial Intelligence Units (FIUs) can enhance the exchange of information and data pertaining to the criminal misuse of commercial websites and Internet payment systems. Finally, given the international character and presence of Internet, it is difficult to determine which jurisdiction has regulatory authority over an Internet payment service provider, and how enforcement action can be applied if there are violations. World based Internet payment service providers have locations and licences in different countries and regions. It is consequently important that governments impose similar regulations, requiring customer identification, due diligence, record keeping and transaction reporting, to avoid certain Internet payment service providers choosing the country with the poorest regulations or one that is not at all regulated.

INTRODUCTION

14. 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.

15. 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.

16. 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.

17. 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.

18. For the purpose of this study, commercial websites and Internet payment systems constitute the areas of study, with a focus on mediated customer-to-customer commercial websites. The overriding objective of this study is to increase public and private sector understanding of ML/TF risks associated with commercial websites and Internet payment systems and to raise global awareness of the methods used to launder the proceeds of crime or finance terrorism using these conduits. Largely based on case studies, an analysis of ML/TF risks associated with commercial websites and Internet payment systems constitutes a large part of the research.

19. The study does not want to replace or duplicate the FATF study on the New Payment Methods, but could be used within the framework of supplementing that report.

20. Ten countries have joined the project team and have contributed to the study: Australia, Belgium (as project leader), China, Hong Kong China, Finland, France, Luxembourg, the Netherlands, the United States and the United Kingdom. Several countries made presentations during the workshop held in Bangkok, Thailand from 28 November 2007 until 30 November 2007 in the framework of the typology exercise of the FATF. A questionnaire has been circulated to the members of the project team. The following other countries participated in the workshop and also contributed to the study: Bangladesh, Chinese Taipei, the Fiji Islands, Germany, India, Japan, New Zealand, the Philippines, South Africa, Russia, Spain, Sweden, Switzerland and Thailand. Various elements of the presentations and replies to the questionnaire have been incorporated into the report.

21. The study has also relied on the experience and cooperation of the private sector. Representatives of eBay and PayPal attended the workshop and participated to the study. The UK based company PrePay Technologies as well as the Electronic Money Association (EMA), a European trade association based in London representing a group of 33 e-money issuers and payment service providers, also participated to the project and contributed to the study.

22. The private sector has also been consulted on the report and the conclusions of the study. A meeting was organised by the project leaders with some members of the project team and the above mentioned members of the private sector, on 4 April 2008 in Brussels. The private sector which contributed to the study received a copy of the report and has been given the opportunity to comment. The comments of the private sector have been taken into account when considered relevant.

23. Finally, the risks and vulnerabilities identified by the study will be useful to the FATF study on Money Laundering Threat Analysis Strategies.

NATURE OF COMMERCIAL WEBSITES AND INTERNET PAYMENT SYSTEMS

Definitions

24. This section provides a functional definition of the different classes/types of commercial websites. Commercial websites can be divided into five categories[2]:

- Mediated customer-to-customer, sites that allow private individuals to sell to one another via an online marketplace.
- Mediated business-to-customer, sites that allow multiple merchants to sell to consumers via an online marketplace.
- 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.
- Direct business-to-customer, merchants that sell goods to consumers via their own websites.
- Direct business-to-business websites, merchants selling to merchants.

25. The present study focuses 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.

26. Online classified-advertising sites, bulletin boards and social networking sites often allow sellers to post items for sale with the transaction taking place offline. While these businesses facilitate the introduction and communication of buyers and sellers, they do not play a significant role in the final sale nor financial settlement. This type of "non-mediated" person-to-person website is therefore not often in a position to see any aspect of the transaction process after the introduction of buyer and seller.

27. "Mediated" websites, on the other hand, play an active role in the completion of underlying transactions, such as by setting the selling price through an online auction, providing some form of verification process for buyers and sellers (including aggregating feedback from other customers), or facilitating financial settlement of transactions (such as providing escrow, or similar intermediary, services). While non-mediated websites may be abused for illegal purposes such as fraud, this paper focuses on mediated businesses that play an active role in facilitating transactions that could be abused specifically for ML or TF.

28. Mediated business-to-customer websites are also subject to AML/CFT risks. A website can sell clothing much of the day, and appears legitimate to its Internet payment service provider, but the website address (URL) may in fact be used to sell child pornography material for several hours each night. In some cases, businesses may allow 3rd party merchants to sell their own goods and services through the business's online portal.

---

[2] It is worth mentioning that certain commercial websites belong to more than one category.

29. 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.

30. For purposes of this report, 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.

31. Considering the risks affecting commercial websites and Internet payment service providers, the project team considers that 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.

Main characteristics

32. This section lists the main characteristics of the type of commercial websites studied and the Internet payment systems linked to these websites.

Commercial websites

33. Commercial websites usually have some if not all of the following characteristics[3]:

- 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.
- 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.

[3] Some of these characteristics are characteristics of the Internet and also apply to Internet payment service providers

- 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.

34. Some commercial websites and Internet payment service providers apply a risk-based approach when identifying customers. If the risk profile of the customer and transaction are high, additional verification methods are applied (simplified Customer Due Diligence (CDD) vs. enhanced Customer Due Diligence (CDD). The mechanisms of verification can be adapted to the country of registration and changed as necessary to adapt to criminal techniques to bypass identification and verification processes. The private sector representatives who participated in the study indicated that criminals do attempt to circumvent these processes and although none of the methods had a zero-failure rate, they were effective on a risk-weighted basis. In certain countries, online customer identification mechanisms using an electronic identity card are used and reduce the risk of identity theft.

Internet payment systems

35. As with any type of online business, the structure and operations of a given Internet payment system may vary drastically. However, in most cases such systems usually require a consumer, or user, to register with the Internet payment system before any transactions can be effected by the system. This registration process typically involves the collection and verification of some identification and/or contact information. For example, an Internet payment system may require a user to input his or her email address, telephone number, street address, and information needed to create a password and user identification (User ID) that will be required for the user to log into the Internet payment system.[4] Other information may be required based upon the business practices of the Internet payment system largely depending upon the type of services provided and the risk management processes required by jurisdictional authorities. The information collected is then verified using a variety of methods, ranging from the examination of paper copies of identity documentation to the use of online identity verification solutions provided by third parties.

36. Before a user of an Internet payment system can effect 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. To avoid fraud or any form of criminal misuse, the Internet payment service provider may attempt to verify that the customer has control over and is authorised to use certain funding methods, such as a credit card or bank account. Once the user has successfully been verified, the user is free to conduct transactions through the Internet payment system.

37. It is important to note that in order for an Internet payment system to provide transaction services for their users, they oftentimes must intersect with traditional banking and settlement systems. For example, an Internet payment system that accepts major credit cards as a funding source from its users usually is required to maintain a merchant account at a financial institution. Through this merchant account the Internet payment system can receive funds from its users, via major credit card networks. Such funds can then be applied to a transaction instruction that has been initiated by a user within the Internet payment system. A similar type of relationship typically exists with an Internet payment system that accepts funds from its users via the user's personal bank account. Once again, the Internet payment system is typically required to maintain an operating account at a bank where the

[4] Note that at the time of registration an Internet payment system may not require a user to input their personal identification number (*e.g.* social security number, passport number, etc.) or date of birth. Based upon the best practices of a given Internet payment system such information may not ever be collected from a user.

transfer of funds from a user's personal banking account can be received. Typically these types of transfers are effected through clearing systems.

38. Internet payment systems may support various types of payment methods for consumers purchasing goods and/or services online from a business website (commonly referred to as Consumer-to-Business transaction or C2B transaction) and businesses purchasing goods and/or services online from another business (a Business-to-Business or B2B transaction)[5]. However, the type of transaction that is of concern for potential ML and TF vulnerability is a person-to-person (P2P) transaction, involving a transaction between two consumers, as when buyers and sellers interact via a mediated website.

39. Other types of funding could be provided directly by certain commercial websites (transactions not powered by an Internet payment provider) or requested by consumers selling items on P2P commercial websites:

- Credit cards.
- Prepaid scheme-branded cards[6] (anonymous in certain countries).
- Wire transfers (in favour of the bank account of the commercial website for further transfer to the seller).
- Wire transfers to the seller bank account (with a message accompanying the transfer and referring to a sale on the Internet).
- Gift cards or gift cheques (anonymous and transferable).
- Cheques (sent to the commercial website in certain countries, to the customers in other countries).
- Bank cheques.
- Postal orders/money orders in favour of the seller[7].
- Money transfers in favour of the seller.
- Cash is accepted on certain commercial websites.

Payment in cash can be made directly between buyer and seller, but this mechanism is not believed to be regularly used.

40. With Internet payment systems, the transaction takes place electronically very rapidly.

41. For global stakeholders (commercial websites and Internet payment systems available in different countries), the policies, practices, facilities (commercial and payments) made available to customers, may be different depending on the location of the parent company, local branch, or local website.

---

5 Some commercial websites and Internet payment service providers offer their customers the opportunity to use a more secured method of payment called the "third party of confidence". Using this facility (against the payment of a commission), the buyer knows that the funds for his purchases on Internet will be made available to the seller only if the goods purchased have been delivered and if he is satisfied that the goods correspond to the description on the commercial website.

6 Banks in certain countries offer prepaid scheme-branded cards (preloaded cards) to customers for whom banks do not want to open a credit limit (unemployed or persons without a regular income).

7 Certain commercial websites advise their users to be cautious when accepting money orders as payment facilities when purchasing items on the Internet, as experience has shown that money orders are often used by criminals who commit fraud (selling items they do not deliver for instance).

MONEY LAUNDERING AND TERRORIST FINANCING CASE STUDIES

42. The following section gives an overview of case studies involving the use of commercial websites and Internet payment systems. This section is divided into two subsections *i)* actual case studies and *ii)* potential vulnerabilities. Potential vulnerabilities are given to provide guidance to law enforcement agencies, financial intelligence units and the private sector.

Actual case studies

43. This subsection provides a number of case studies that illustrate various ways that commercial websites and Internet payment systems have been exploited for ML/TF purposes.

44. Commercial websites and Internet payment systems can be used to sell/purchase illegal products, like drugs or counterfeit goods. Sometimes, the sold/purchased dual-use or precursor products are not *per se* illegal but correspond to dual use goods such as products used to make explosive, weapons or other controlled goods. Postal and express freight are frequently used to distribute these goods.

45. Commercial websites and Internet payment systems can be used for committing illegal transactions, fraudulent transactions or illegal activities, activities outside of the FATF's remit. Nevertheless, various case studies indicate that commercial websites and Internet payment systems are also used to collect the proceeds of these illegal activities, and further to facilitate ML and TF transactions (by making the funds disappear: transferring the funds on a bank account in the country of the criminals or abroad, using them for other purchases on commercial websites,…).

Case study: The use of commercial websites and Internet payment systems to sell drugs

In one file, the bank account in Belgium of an individual was credited by wire transfers from an Internet payment service provider (small amounts for a total of EUR 4 700). The subject was under investigation in another European country for the sale of drug starters. Information from law enforcement confirmed that the subject was selling drug starters via a commercial website.

Source: Belgium.

46. In the above-mentioned case, the Internet payment service provider was used to collect the proceeds of the illegal activities and may afterwards be used to perpetrate the illegal activities and operations. The criminal could use the proceeds of his illegal activities to buy new drug starters and continue to carry out his illegal activities via the commercial website.

Case study: The use of commercial websites and Internet payment systems to sell counterfeit goods

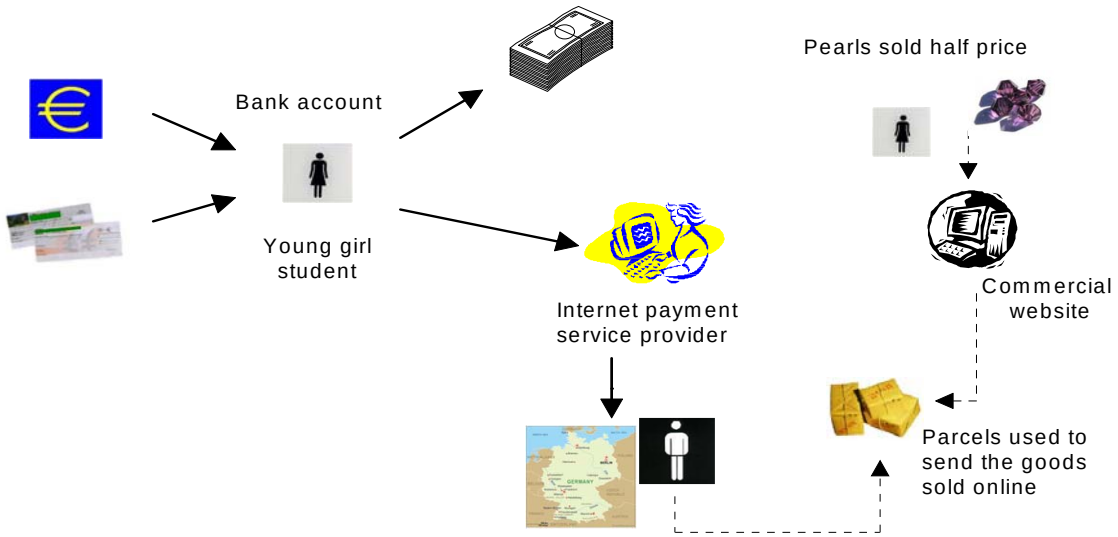
A bank reports the suspicious transactions of a young girl. From January 2005 to August 2005 (eight months), the bank account of the young girl, student, was credited by wire transfers and cheques written out by individuals located all over France. The amount of each cheque was rather small (EUR 20 to 40). Regarding the debiting operations, the girl made cash withdrawals and wire transfers bearing the mention "Internet payment provider bills". The purchases amounted to a total of EUR 6 340 split into 43 operations.

In September 2005, she began to use a credit card so that it became more difficult for the bank to understand and analyse her transactions. Only a global amount of payments is registered monthly on her bank account.

Investigations showed that, from September 2005 to March 2006 (eight months), she made 63 purchases online for a total amount of EUR 39 282.24.

The young lady was selling counterfeit pearls of a famous brand at half price. She was using a provider in another European country which sold her parcels used to send the goods she had sold online.

Over 16 months, she earned more than EUR 43 000, roughly more than EUR 2 800 a month.



Source: France

Case study: The use of commercial websites and Internet payment systems to sell explosive precursor products

A foreign FIU communicated/disclosed to the Belgian FIU that they received a STR from an Internet payment service provider concerning a national from a European country selling the following items on an associated commercial website: potassium, chlorate, barium nitrate, strontium nitrate, ammonium nitrate. These items are considered as dual-use goods, because, put together, they can be used to make explosives. The goods were sold to customers in Eastern Europe.

The criminals planned to collect the proceeds of their "illegal" sales on the Internet through the Internet payment service provider and consequently to launder these proceeds, also using the Internet payment service provider.

Source: Belgium.

Case study: The use of commercial websites and Internet payment systems related to weapons trafficking

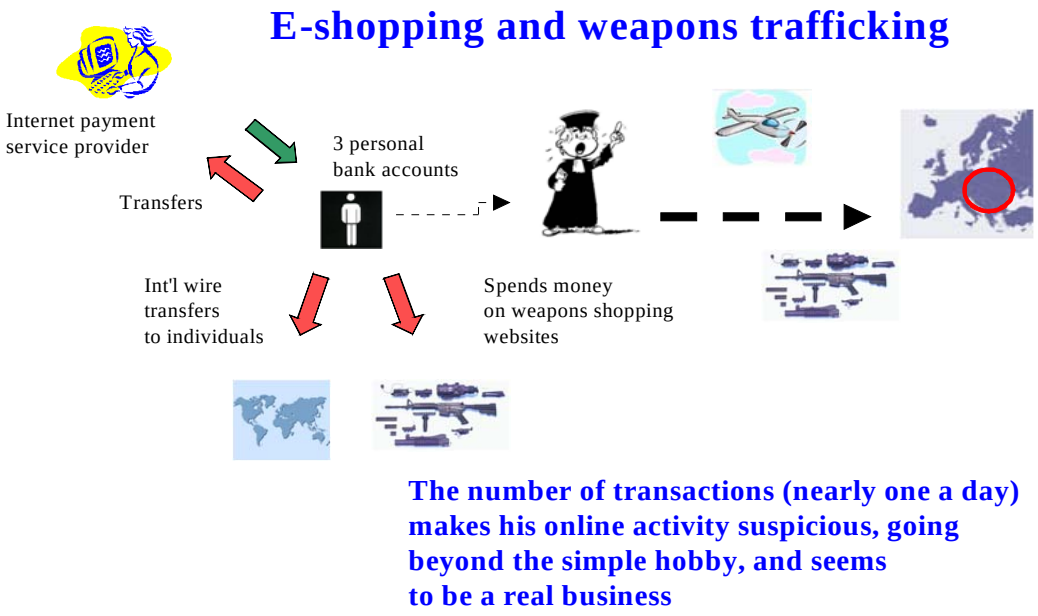
A case reported by a bank involves a lawyer receiving and initiating a lot of Internet payments on and from his three personal bank accounts, ordering international wire transfers to individuals, receiving cheques and making cash deposits with no apparent economic rationale.

From the message on his bank account accompanying the financial transactions with the Internet payment service provider (payment "gun X", payment "pistol Y") and the analysis of the wire transfers, it was possible to identify his online activity as related to weapons and elements of weapons sales transactions.

FIU's investigations revealed further that:

- over 4 years he made more than 1 600 selling operations, the frequency of this online activity revealing a potential illegal business activity related to the use of weapons commercial websites;
- he regularly travelled to countries from Central and Eastern Europe which are vulnerable to weapons trafficking and often stayed more than one week there, so that he might have smuggled weapons.

The case was transmitted to the judicial authorities for weapons trafficking.



Source: France.

47. Commercial websites and Internet payment systems can also be used for commercial activities performed without VAT registration and without paying taxes.

Case study: The use of commercial websites and Internet payment systems to sell goods illegally (avoiding tax obligations)

The persons on investigation were directors of a company involved in purchasing large quantities of duty free cigarettes and alcohol to sell on the domestic market contrary to their export-duty free status, thus avoiding tax obligations. Due to not paying any tax on the goods the company was able to markedly increase profits. The syndicate also generated false receipts that purported to come from an export company detailing their alleged cigarette exports. Investigations with the purported company confirmed that no such exports had ever been made. On arrival of the cigarettes, payment was made to the delivery driver on a cash-on-delivery basis.

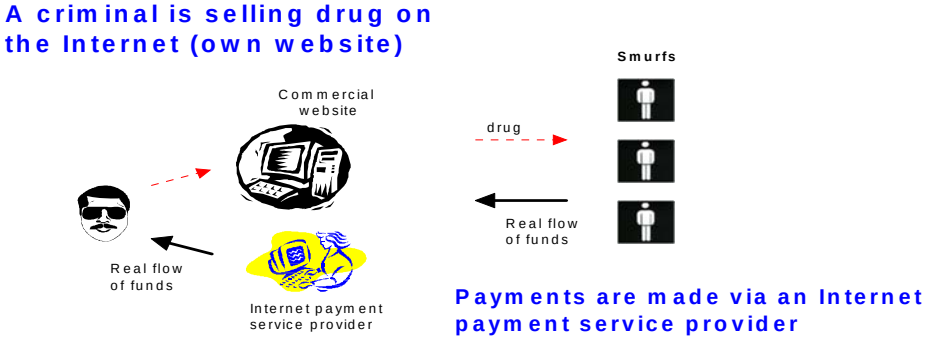
A large number of the company's sales occurred over the Internet from customers paying via credit card. A majority of the sales on the Internet were illegitimate and came from three different email addresses. Payments for these orders were made from one of two credit cards linked to Belize bank accounts. One of these cards was held in the company's name. The money in the Belize bank account was sent there by one of the directors using several false names from not only Australia but Belize, Hong Kong, and Vietnam. The director conducted structured wire transfers under false names and front company accounts. The funds were purchased at well known banks with multiple transactions occurring on the same day at different bank locations and all of the cash transfers conducted in amounts of just under AUD 10,000 to avoid the reporting threshold.

Source: Australia.

48. Criminals can develop their own commercial website to sell illegal products or perform illegal activities and use Internet payment service providers to collect the proceeds of these activities.

Case study: Criminals using their own commercial website to sell drugs and the use of an Internet payment service provider to collect the proceeds of their activities

An Internet payment system user owns a commercial website where he is selling cannabis, cannabis seeds and narcotics utensils. As he wishes to be paid via an Internet payment system, the buyers are using this payment system.



Source: Luxembourg.

Case study: The use of an Internet payment service provider account to collect proceeds of procurement on the Internet

The user of an Internet payment service provider receives payments from a website offering escort services or prostitution. This user is the registrant of the website and he gets the funds on an account from buyers. On the website, the use of the Internet payment system is indicated. The website is explicit, contains several prostitutes to be chosen by the client and is professionally set up. The commercial website and the IP logins are detected by the Internet payment service provider and the file transmitted to the FIU.

Source: Luxembourg.

49. As already mentioned in the FATF report on New Payment Methods, digital precious metals are a new online payment system that involves the exchange of options or the right to purchase an amount of precious metals at a specific price. These derivatives can be exchanged, like traditional commodity or securities derivatives, between account holders in a digital precious metal service. Consumers purchase a quantity of virtual precious metal holdings based on the current price of the metal on the world commodity exchanges. Once a purchaser has acquired a quantity of the virtual

precious metal, those holdings or a portion of them can be transferred either to another individual or a merchant in exchange for goods and services, also online. As a result, digital precious metal exchanges allow for the transfer of fixed "value" between unrelated 3rd parties, functioning as a money and value transmission business.

Case study: the use of e-gold as payment method

On 27 April 2007, a federal grand jury in Washington, D.C., indicted two companies operating a digital currency business and their owners. The indictment charges E-Gold Ltd., Gold and Silver Reserve, Inc., and their owners with one count each of conspiracy to launder monetary instruments, conspiracy to operate an unlicensed money transmitting business, operating an unlicensed money transmitting business under federal law, and one count of money transmission without a license under D.C. law. According to the indictment, persons seeking to use the alternative payment system E-Gold were only required to provide a valid e-mail address to open an E-Gold account – no other contact information was verified. The indictment is the result of a 2½-year investigation by the U.S. Secret Service with cooperation among investigators, including the Internal Revenue Service (IRS), the Federal Bureau of Investigation (FBI), and other state and local law enforcement agencies. According to Jeffrey A. Taylor, U.S. Attorney for the District of Columbia, "The defendants operated a sophisticated and widespread international money remitting business, unsupervised and unregulated by any entity in the world, which allowed for anonymous transfers of value at a click of a mouse. Not surprisingly, criminals of every stripe gravitated to E-Gold as a place to move their money with impunity."

Source: U.S. Department of Justice.

50. During the workshop, case studies were also presented where commercial websites and Internet payment services providers are used to facilitate the commitment of the underlying criminality (fraud in most of the cases) but not for the money laundering. These cases, even if they are not directly relevant in the framework of the present study, are given as they could be useful to traditional financial institutions for fighting against money laundering.

51. Commercial websites and Internet payment systems can be used by criminals to commit fraud. One of the mechanisms used is the sale of fictitious items which the seller will not deliver to the buyer after receiving the payment. If commercial websites are used to attract buyers (in this case the victims of the fraud), Internet payment systems are not necessarily used to collect the funds (the proceeds of these activities). Criminals frequently use bank accounts in traditional financial institutions or money transfers and postal orders to be paid for the goods they do not deliver. The same channels are thereafter used to launder the proceeds of these illegal activities by making the funds disappear.

Case studies: Transfers related to fraudulent sales on commercial websites (items never delivered)

The Belgian FIU received several STRs from banks in Belgium concerning bank accounts credited by wire transfers, apparently related to/justified by sales on commercial websites, and followed by cash withdrawals.

The majority of the wire transfers are of small amounts (maximum EUR 800), originate from various senders and, following the message accompanying the payment, should be related to sales on a commercial website, sometimes the sales of luxury goods. Payments are not made through an Internet payment service provider but originate from the bank account of the buyer and are credited on the bank account of the seller. The wire transfers are followed by instant withdrawals in cash.

The goods are never delivered to the buyer (victim of a non-delivery fraud).

In some reports the wire transfers are not followed by cash withdrawals but by transfers in a country known for producing counterfeit products (in cases related to the sale of counterfeit goods).

The fraudulent bank account is used only during a short period (because of buyer's complaints).

Investigation showed that false names are used on the commercial website (the name used by the seller on the commercial website (certainly a fictitious name) and the name of the bank account holder where the payment is made are different). In one file, information received from law enforcement indicated that the subject was known for using different names on the commercial website. In another file, the subject was using two different passports and different names.

Source: Belgium.

Case study: Sale of fictitious goods on commercial websites and the use of Western Union to collect the proceeds of these fictitious sales

The National Bureau of Investigation Money Laundering Clearing House investigates an aggravated fraud and money laundering case. The two main suspects in Finland were acting as Western Union agents in Finland. The offices of the agents were closed on 27 March 2007, and the suspects were taken into custody.

People from other countries than Finland were fooled into buying fictitious goods (in this case; cars or other vehicles) on commercial websites[8] and sending the payment to fictitious persons in Finland via Western Union.

The two Western Union agents in Finland picked up the money with the identities of the fictitious persons. Furthermore, the agents forwarded, again with fictitious identities, the money as Western Union transactions outside of Finland.

The two suspects in Finland received text messages from two persons (money flow managers) using mobile phone numbers including:

- information about the victims abroad (their name, the expected receiver of the money, the amount sent and the MTCN) as well as
- instructions for forwarding the money abroad (the name of the receiver, the amount and the country to which send the money).

The money flow managers are living in European countries.

The total number of victims is over 300 and the total loss for the victims is about EUR 1.07 million. The main source countries for the assets were the USA and the UK, but there were also a number of other source countries (about 25 countries).

The two Western Union agents in Finland say that they received 10 per cent of the money picked up by them. They also say that both the money flow managers visited Finland during the activity and took with them a significant amount in cash.

Based on the investigations, at least one of the money flow managers seems to have similar arrangements with local Western Union agents in a number of other European countries.

Searches at the Western Union offices and the homes of the agents and arrests were made on 27 March 2007.

The investigation of the phones, SIM cards and PCs gave good evidence. Hundreds of text messages as well as a few e-mail messages were found in which instructions were given to the Western Union agents concerning the fraud cases and the money transactions.

To support the investigation and the case in court, information is needed about as many predicate offences abroad as possible. Therefore, requests (FIU, Interpol or MLA) have been sent to 24 countries.
At the moment information was received about 181 fraud cases from 19 different countries.

[8] It is worth mentioning that on certain commercial websites, a seller cannot request potential buyers to pay by money orders. To avoid problem with fraud, these commercial websites do not allow their users to propose payments by money orders (this option is not available and a seller cannot request a payment by money orders when exchanging mails via the mail system of the commercial website).

Source: Finland.

52. It is worth mentioning that certain commercial websites propose mechanisms to their customers to avoid their site being used to commit such type of fraudulent activities: organizing rating systems to evaluate users' (buyers and sellers) reliability based on their previous transactions with the commercial website, advising their customers not to use money orders, encouraging the use of an Internet payment service provider associated with the commercial website because this is more secure, tracking and banning fraudsters.

Potential vulnerabilities

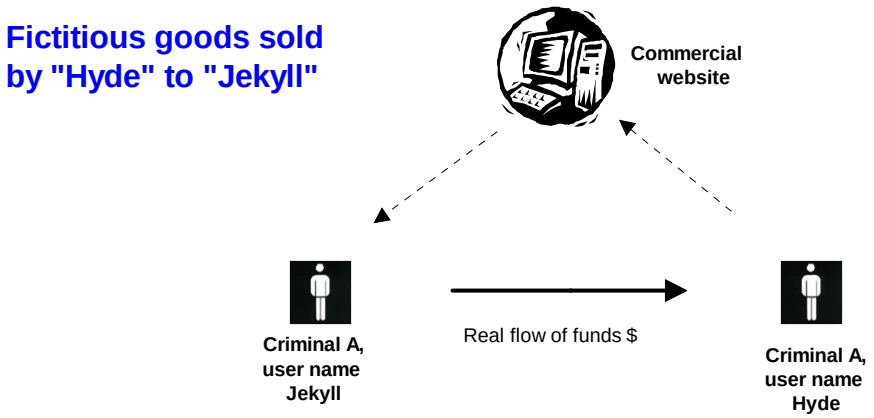
53. Potential vulnerabilities presented in this section are given to help the private sector stakeholders, not yet aware of possible ML or TF mechanisms, to detect possibly suspicious transactions. Some potential case studies present similarities with case studies analysed by FIUs and presented in the first subsection.

54. These potential vulnerabilities are considered feasible in reality by the private sector consulted during the study. However certain commercial websites and Internet payment services providers have developed monitoring and detection systems and mechanisms (cf. section "Risk management measures taken by the sector") in such a way that these transactions may be better detected and provide additional deterrence to criminals attempting to use these systems.

55. Criminals may use fictitious commercial transactions on commercial websites to justify movements of funds using traditional financial institutions or Internet payment systems. This typology shares many similarities with trade-based money laundering, where the transfer of funds for a transaction is disproportionate to the value of the goods delivered.

Potential case study: Fictitious sales on commercial websites followed by real payments

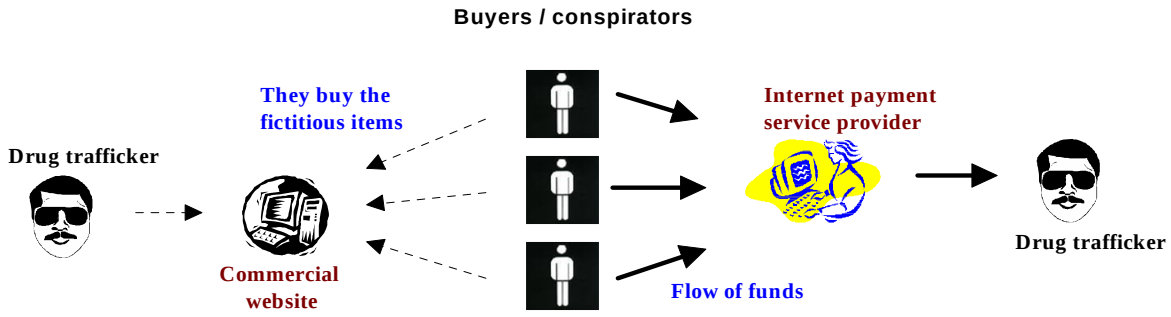
Buyer and seller know each other and may live in different countries or continents. No goods are delivered. Certain commercial websites between private individuals only put buyers and sellers in touch. They are not liable for the delivery, for checking the quality and/or the reality/existence of the goods offered for sale. The buyer will never complain for the non-delivery because seller and buyer are in league with each other. The buyer will pay the seller who will receive the funds on his bank account abroad. The beneficiary will have no difficulties justifying the origin of the funds received because the funds apparently come from sales on the Internet[9]. The buyer can also easily explain that he uses his credit card to buy something on the Internet. Commercial websites between private individuals allow the sale of goods of relatively high value, which will allow criminals to launder considerable amounts.



Source: Belgium.

Potential case study: The use of a commercial website to launder the proceeds of drug trafficking

A drug trafficker can use commercial websites to receive the payment of his illicit sales. Instead of raising his bank's suspicion with unjustified cash deposits, he publishes an announcement for whatever fictitious products. His drug clients then proceeds with an online immediate purchase. Once the drug trafficker receives the payment, he can deliver the drugs as well as justifying the credit operations on his bank account with "online sales operations". This implies that there is coordination between "seller" and "buyer".



Source: France.

[9] As also mentioned in the section "Considerations on second level of controls versus third level of controls", a statement or a printout of a screen of the commercial website showing an item on sale for instance must not immediately and unconditionally considered as an invoice or justifying a financial transaction on the bank account of the customer. Conversely, the presentation of such justification document could be used as a red flag or indicator for the financial institution.

56. If the item sold by criminals exists, it can happen that the price of the item sold is overrated by buyers and sellers who know each other and can consequently justify relatively bigger movements of funds. This is essentially the same typology used in trade-based money laundering.

Potential case study: The sale of goods at an overrated price

The mechanism is the same as in the above-mentioned example, except that the goods sold do exist and are sold at an overrated price through several fictive buyers. The net difference between the nominal sale price and the actual value of the goods delivered equals the value of money laundered. This type of transaction provides additional security for the launderers by creating a record trail of actual delivered goods, requiring law enforcement to prove that the value of the sale is grossly out of proportion with the actual market value of the goods.

Alternatively, value can be laundered in the reverse direction by having the buyer buy significantly less than the market value of the goods and then reselling the goods for a profit. The buyer would then be able to claim the difference in value was a profitable arbitrage deal while the seller would be to write off the difference as a market loss.

Many online businesses, particularly auction sites, sell goods that do not have a readily available market price. Also, overbidding is not unusual and could reflect legitimate transactions. In addition, since the items being sold remain in the possession of the seller throughout the auction process, the online auction company has little ability to ascertain the true market value of the item.

Source: Belgium.

57. As already mentioned above counterfeit products or stolen products could be sold on commercial websites, aka a "virtual fence". Internet Payment systems could be used to move and launder the proceeds of these sales.

Potential case study: The sale of counterfeit or stolen products using multiple identities and user names

A criminal sells via a Customer to Customer website stolen and counterfeit goods. By multiplying identities and user names, he reduces the risk of being identified by the monitoring unit of the shopping website. He can either use the proceeds generated by his illegal sales to buy other goods or services online or transfer it to his personal bank account, the crediting operations being justified by "online sales operations".

Source: France.

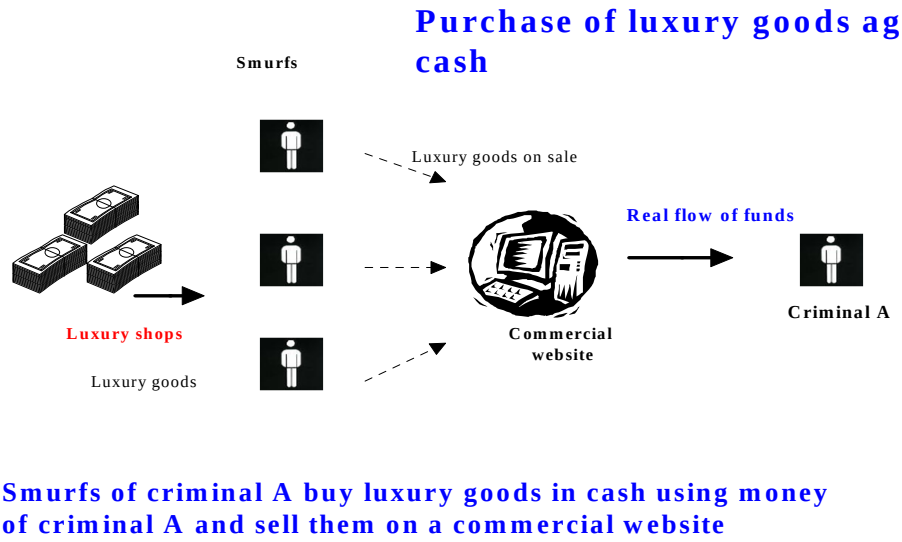
58. Not only counterfeit luxury goods could be sold on commercial websites, but also real luxury goods purchased with cash by smurfs recruited by criminals to launder the proceeds of their illegal activities.

Potential case study: The use of commercial websites to sell at a reduced price, of goods (not counterfeit) purchased by smurfs in luxury goods shops with cash

Criminals send smurfs to luxury goods shops to buy articles of relatively high value (handbags…) that they pay in cash. This first stage of the money laundering process allows criminals to inject cash, possibly in small denominations into the financial system. This stage takes place in luxury good shops, which are less aware of money laundering[10].

[10] The 3rd EU AML/CFT directive applies to natural or legal persons trading in goods, to the extent that payments are made in cash in an amount of EUR 15 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked. Merchants of high value goods accepting cash above EUR 15 000 are submitted the AML/CFT obligations (KYC, record keeping, cooperation with the FIU, adequate internal organisation). In certain countries, merchants in high value goods are not authorized to accept payments in cash if the value of the purchased goods exceeds a certain threshold (in Belgium: EUR 15 000).

The luxury goods are subsequently sold on commercial websites, at a lower price. Criminals accept to lose a lot of money to launder the proceeds of their illegal activities. The proceeds of the sale arrive on the bank account of the seller abroad.



Source: Belgium.

59. ML transactions not only take place in the first stage of the money laundering process (placement), but happen also during the two other ML stages (layering and integration). Criminals usually try to make the financial transactions more sophisticated for law enforcement authorities and investigators, using a combination of the different ML stages. Commercial websites and Internet payment services providers could be used at various stages of the ML process. Traditional financial institutions could be used during the placement stage and commercial websites and Internet payment services providers at later stages such as during the layering stage (the above mentioned potential case study) and the integration (the purchase of goods or items with illegal funds already injected in the financial systems). The two following case studies explained below provide examples of the use of the ML process at the integration stage.

Potential case study: The use of an electronic purse in conjunction with other ML methods

- An individual residing at the country border regularly imports tobacco and alcohol products exceeding the duty-free quantities from the neighbouring country.
- He sells them to individuals. The cash collected is used to credit a savings account opened in the name of one of his underage children. The justification given can be cash donations from the family to the child.
- The funds crediting the savings account of the child are regularly transferred to the bank account of the individual held in another bank. The origin of the funds appears to be legal – it comes from the savings account of one of his children; the justification for the transfers can be temporary financial difficulties, expenses made for the child like buying a scooter or paying driving lessons, etc.
- The funds transferred on the bank account of the individual can then credit an electronic purse to buy goods and services online.

Source: France.

60. Commercial websites and Internet payment systems can potentially be used to finance terrorism, taking into consideration the fact that terrorism financing may involve small amounts of money.

61. As already mentioned, commercial websites and Internet payment service providers depend on information they obtain from law enforcement and other authorities to facilitate the detection of suspicious transactions related to terrorist financing and it is not always necessary for Internet payment service providers to identify TF in their STRs in order to help counter terrorist financing.

Potential case study: The use of a commercial website and Internet payment service provider to finance terrorist activities also in conjunction with other ML methods

- Y, a well-known terrorist, under close watch of the intelligence services, residing in Germany, wants to send funds to Z, residing in France so that Z can buy cell phones or other items necessary to make explosive devices.

- Afraid of being detected if he uses funds transfer systems like Western Union or MoneyGram, he decides to use an alternative way to make his funds available.

- He asks a student to register on a C to C website and to open an Internet payment provider account. Y gives the student a prepaid card of EUR 799 to credit his Internet account.

- The student can then order a transfer from his Internet account to the Internet account of another student located in France.

- The student located in France can then credit his bank account with the funds received on his Internet account and buy prepaid cards to be handed over to Z.

- Z can use the prepaid cards directly or credit his bank account with them.

Source: France.

62. Front individuals or intermediaries such as the "students" in the example above are even recruited on the Internet, lured by the payment of a commission amounting from 5% to 10% of the funds to be transferred. Massive spams are sent, proposing to become the associate of a "financial company", the job consisting of receiving and transferring funds. These mules are used for ML/TF.

63. Other potential case studies :

Other potential case studies

- A criminal or a third party used by the criminal purchases goods on the Internet, using prepaid cards (anonymous).

- The purchase of prepaid cards against cash (from points of sales or third parties).

- The purchase from a third party (against cash) of assets/value held by the third party on an account opened on the Internet (Internet payment service provider).

- A money launder justifies movement of funds by a fictitious turnover from e-commerce activities.

- A criminal or money launderer detains assets on accounts opened on the Internet (Internet payment service provider).

Source: The Netherlands

64. If the above mentioned case study is feasible in reality, high standards of due diligence and computer software to detect suspicious transactions should detect such patterns as they are carried out on a multiple basis (multiple transactions is a prerequisite for criminals if they want their ML/TF transactions to be economically viable)[11]. On commercial websites and Internet payment service providers applying such due diligence mechanisms, a user multiplying transactions will be the subject of a "client verifying process", implying that the commercial websites will obtain more information on the seller (Memorandum of Association, VAT registration…). Commercial websites also work with companies selling luxury goods to identify individuals selling counterfeit luxury items.

Red flags – Indicators

65. This section, which resulted from the typological analysis, provides an overview of potential indicators of ML/TF. These red flags – indicators must call the attention of the Internet payment services providers when analysing suspicious transactions. An indicator is itself not sufficient to

[11] The commercial websites and Internet payment service providers consulted during the study apply these types of due diligence mechanisms and use monitoring software.

conclude that a transaction is suspicious and must be reported to the FIU. The Internet payment service provider has to collect additional information to analyse the suspicious transactions.

66. Certain Internet payment service providers already use these red flags – indicators to detect suspicious transactions/activities using risk models and computer software (cf. section "Risk management measures taken by the sector"). However, they are provided for Internet payment service providers which are not yet aware of the ML/TF risks and not yet familiar with such indicators.

67. This section is also provided for the private sector stakeholders to be added to their own developed indicators.

68. As mentioned below in the section "mechanisms used to mitigate ML/TF risks", Internet payment service providers have access to a range of information, inclusive information on the underlying commercial transactions, to analyse suspicious financial transactions.

69. Following red flags-indicators have been identified:

- 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, which could indicate that the customer does not live in the country from which he registered but in another country where he cannot register (not accepted by the website for security reasons) or that he registered in one country but commits illegal activities in a third country, or that he concealed the results of his illegal activities in 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[12], if the Internet payment services provider allows loading with cash[13].
- 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[14] or purchases middle high value items on a regular basis with a prepaid debit card, an anonymous prepaid credit card[15] or a gift card where the origin of the funds is difficult to retrace[16].

---

12 It is worth mentioning that the loading of an account or a card with cash is not sufficient in itself to give rise to a suspicion of ML/TF. Cash could have a legal origin. Confronted with cash, the Internet payment service provider needs to apply higher standards of control or due diligence (monitoring of transactions, limits and restrictions…).

13 It is worth mentioning that systems which do not accept cash may be less risky.

14 According to the private sector consulted during the study, on commercial websites and Internet payment services provider, the average value of a commercial transaction and the subsequent payment are very low. Consequently money launderers wanting to use commercial websites and Internet payment service providers for their criminal activities and the ML may need to carry out several consecutive small transactions if they want to avoid being detected. In case they carry out a large transaction they will be detected by commercial websites and Internet payment service providers using sophisticated computer software.

15 It is sometimes difficult for Internet payment service providers to distinguish between a normal credit card and a prepaid credit card as credit card companies use similar credit card numbers for both credit cards.

16 It is worth mentioning that Gift cards have generally low face values. Criminals need to purchase several gift cards to make their ML transactions economically viable. Issuers of gift cards have also internal control

- The customer apparently resells goods purchased beforehand, without any economic reasons, or with a significant discount or increase on the price (monitoring feasible if the Internet payment service provider cooperates with the commercial website involved when analysing suspicious financial transactions);
- 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 (facilities depending on the country of destination).
- A customer uses an account with an Internet payment service provider not to purchase items on Internet but to hide a sum of money obtained illegally. 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[17].
- 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.
- Abnormality with the proposed price on an auction site or during an auction sale indicating a possible complicity between buyer and seller (a customer offers to purchase an item at a price largely higher than the requested price). Additional factors could include multiple transactions between the same buyers and sellers.
- 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[18].
- 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 or transaction may result from one indicator or a set of indicators.

70. The private sector participating in the study confirmed, based on their experience, the accuracy and pertinence of this list of red flag – indicators.

---

mechanisms to follow the issuance of gift card at local shops or supermarket, which reduce but do not eliminate anonymity.

17 Some e-money devices are limited in time.

18 All the non-cooperative countries identified by FATF have been delisted. Certain countries are still under monitoring.

MONEY LAUNDERING AND TERRORIST FINANCING RISKS

71. The AML/CFT risks of trade-based money laundering and non face-to-face transactions apply also to commercial websites and Internet payment systems. The AML/CFT regulations of commercial websites could be comparable to the ones existing for traditional commerce (those regulations only apply to merchants accepting cash over a predefined threshold) and the ones of Internet payment systems to the common payments systems, even if the relationship is non face-to-face, because risk-based CDD and monitoring measures are taken to reduce and mitigate the ML/TF risks.

72. These risks can be classified according to the ML phases:

Placement:

- **Anonymity[19] of customers on certain commercial websites and Internet payment services providers.** Both the registration and transactions could in certain circumstances be performed anonymously (on certain websites an anonymous e-mail address is enough for registration).
- **The relationship with customers is a non face-to-face relationship**. Transactions are non face-to-face transactions, which makes it more difficult for the commercial websites and Internet payment services providers to be sure that they are working with the customer who has been identified at registration.
- **The possibility to use multiple registrations.** The use of multiple (anonymous) registrations to purchase and sell items could create problems when screening, monitoring and reconstructing transactions and flow of funds.
- **Remote access to commercial websites and Internet payment systems.** Connection to commercial websites and Internet payment systems is available everywhere in world. A criminal can connect himself to the Internet from web terminals not affiliated or registered to his or her identity, which makes more difficult for law enforcement to locate and to pursue criminals and money launderers.
- **Relative "anonymity" associated with certain methods of payment.** With prepaid credit cards, gift cards/gift cheques[20] and when cash is used, the origin of the funds cannot be (easily) retraced[21].

Layering:

- **The speed of movement**. Transactions via commercial websites and Internet payment systems can be done very rapidly as transactions between sellers and buyers are performed electronically.

---

19 A good identification is a prerequisite for detecting a suspicion related to an individual/company but also for a serious and effective investigation of a suspicious operation.

20 Even if anonymous gift cards are generally issued for relatively small amounts.

21 Even if measures of internal control exist to monitor and to supervise the issuance of gift cards at local shops or supermarkets and the purchase of prepaid cards and avoid or survey sudden increases in the number of gift cards issued and amounts loaded (analysis of purchase details, pattern of purchases and spending locations, IP addresses, physical monitoring of premises), anonymity can be reduced but cannot be totally avoided.

- **The international character and the jurisdictional issue of where the transaction takes place.** Transactions on commercial websites and Internet payment systems can be performed across international borders and the jurisdiction where the Internet payment service provider is located may not be competent to investigate and prosecute ML or TF. Likewise, no single jurisdiction has clear responsibility for regulating and monitoring activity.

The speed of movement, the international character of the transaction and the jurisdictional issue related to the use of the commercial websites and Internet payment systems may impact on FIUs and law enforcement who investigate cases of money laundering or terrorism financing.

- **Volume - high number of transactions and amounts per transaction**[22]. The high number of transactions and consequently amounts per transactions make it more difficult for Internet Payment services providers to define criteria to monitor and screen transactions (which types of transactions should be regarded as suspicious?)[23];
- **The limited human intervention**. As less human intervention is associated with transactions via commercial websites and Internet payment systems, traditional first level detection mechanisms which rely heavily on the face-to-face relationship with the customer, are no longer available and must be replaced by sophisticated second level detection mechanisms[24].
- **The lack or inadequacy of audit trails, record keeping or suspicious transactions reporting by certain Internet payment services providers.**

Integration:

- **The possibility to buy high value items.** Buying (high value) goods, precious metals, real estate or securities on commercial websites using an Internet payment system.

[22] By limiting the use of an account, the Internet payment service provider should be able to limit the potential risk.

[23] It is worth mentioning that it is also difficult for traditional financial institutions to define criteria to monitor the transactions of their customers using computer software.

[24] If Internet payment service providers adequately monitor the financial transactions of their customers by detecting deviations from their customer's known profile of transactions, the face-to-face contact at the beginning of the relationship with the commercial website and Internet payment service provider may not constitute a problem.

OVERVIEW OF REGULATIONS IMPOSED ON THE SECTOR

73. For the above-mentioned reasons, Government officials have been called on to start regulating the commercial websites and Internet payment systems fearing that criminals and terrorists could use them to launder money or finance terrorism.

General introduction

74. In general regulations are imposed to commercial websites mainly in the field of the protection of the consumer (better inform their users on their rights and duties, general terms of use and the use of electronic contracts, identification of the commercial website, advertising…), the prohibition to sell certain goods and the possibility to cancel a purchase made online.

75. For instance Electronic Commerce is regulated by means of several European Directives. The goal of the regulation is mainly to create transparency for consumers and thus give them the necessary protection. The main regulations stem from the E-Commerce Directive (2000/31/EC) and the Distance Selling Directive (1997/7/EC). The first Directive imposes several rules for transparency of the E-commerce company by obliging transparency about the nature and general information on the E-commerce company as well as transparency about the process of buying a product. The second directive states rules on revoking purchases (within certain time limits). Finally the European Regulation (2006/2004/EC) for coordination of cross-border requests for mutual assistance concerning consumer protection.

76. In the US, the Bureau of Consumer Protection of the U.S. Federal Trade Commission (FTC) works to protect consumers against unfair, deceptive, or fraudulent practices in the marketplace. The Bureau conducts investigations, sues companies and people who violate the law, develops rules to protect consumers, and educates consumers and businesses about their rights and responsibilities. The Bureau also collects complaints about consumer fraud and identity theft and makes them available to law enforcement agencies across the country.[25] The FTC's Division of Enforcement litigates civil contempt and civil penalty actions to enforce federal court injunctions and administrative orders in FTC consumer protection cases; coordinates FTC actions with criminal law enforcement agencies through its Criminal Liaison Unit; develops, reviews, and enforces a variety of consumer protection rules; coordinates multi-pronged initiatives to address current consumer protection issues; and administers the Bureau of Consumer Protection's bankruptcy programme.[26]

77. In most cases, there is no identification or STR-obligations in place for commercial websites. In The Netherlands, in case a commercial website provides payment services as well these obligations will be applicable.

78. This is consistent with the international AML/CFT standards which apply in the same manner to traditional commerce and do not require merchants to apply AML/CFT measures (CDD, cooperation with the FIU, adequate internal organization) if they do not accept cash over a preset threshold.

79. The AML/CFT obligation (among others the obligation to monitor and detect suspicious transactions) is an obligation imposed on financial institutions and e-money providers.

---

25 Federal Trade Commission (2007a).

26 Federal Trade Commission (2007b).

80. In the European Union, e-money issuers are required to be licensed, they are regulated in the country in which e-money is issued. With the European passport mechanism, an e-money issuer licensed in one European country is allowed to operate across the EU. E-money issued in one European country can be spent on a commercial website in another European country. E-money issuers are mainly located in the UK, Luxembourg, and Germany. In the US, Internet payment service providers are licensed as a money services business (MSB). Licences are also granted to Internet payment services providers in other countries such as Australia. There are apparently no regulations imposed to Internet payment services providers in China. The issuer can only issue the e-money and target customers of the country of issuance (the country where he gets the licence).

81. In the European Union, the prudential supervision of the business of e-money institutions is regulated by the EU Directive 2000/46/EC ("E-money Directive"). The directive introduces a legal framework that harmonises the prudential supervision of electronic money institutions for ensuring their sound and prudent operation and their financial integrity. The legal framework includes among others measures like the obligation to have an initial capital and requirements to own funds sufficient to cover their financial liabilities related to outstanding electronic money, limitations of investments, sound and prudent management, administrative and accounting procedures and adequate internal control mechanisms. For the purpose of the prudential supervision of electronic money institutions, the issuance of electronic money is not considered as a deposit-taking activity and subject to the supervisory regime applying to credit institutions if the received funds are immediately exchange for electronic money.

82. The EU AML/CFT Directives apply to electronic money institutions. Directive 2005/60/EC foresees simplified customer due diligence (CDD) where, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 150, or where, if the device can be recharged, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year by the bearer as referred to in Article 3 of Directive 2000/46/EC.

83. In regulated sectors like the sector of the Internet payment service providers, efforts have been made by regulators and by trade associations to develop guidance to the sector for the application of AML/CFT regulations and with fraud and ML/TF typologies exercises.

Overview by country

United Kingdom

84. The UK does not have a specific regulatory regime for electronic commerce, although the Financial Services Authority does regulate electronic money in the UK, as well as the sale of financial services by electronic means by firms in the UK.

85. E-money is defined in UK law as monetary value as represented by a claim on the issuer which is stored on an electronic device, issued on receipt of funds and accepted as a means of payment by persons other than the issuer. E-money is considered as an electronic surrogate for coins and banknotes, intended to effect payments of limited amounts.

86. The FSA's approach to regulating e-money is based on requirements of the EU's E-money Directive. E-money issuers also have obligations under the Money Laundering Regulations 2007 to, for example, apply customer due diligence measures and to undertake ongoing monitoring of their business relationships. In the event that potentially suspicious activity is detected, the firm has a legal obligation to report this to the authorities. The FSA would expect e-money issuers to be able to demonstrate that they deploy an adequate range of controls for the type of risks that they encounter. Discussion of steps that can be taken by e-money issuers to meet their legal obligations is provided by Guidance issued by the Joint Money Laundering Steering Group (JMLSG).

Luxembourg

87. The relevant Luxembourg legislation transposes the E-Money Directive and the EU AML/CFT Directives. Since July 2007 one Internet payment provider has established its EU Headquarters in Luxembourg. This entity is licensed as a bank by the Luxembourg financial sector supervisory authority, the *Commission de Surveillance du Secteur Financier* (hereafter the "CSSF"). Thus this Internet payment provider is submitted to the same AML/TF legislation and guidelines of the CSSF as any bank operating in Luxembourg. In particular it has the following obligations: costumer identification (CDD (simplified/enhanced) -on a risk based approach-), records keeping, adequate internal AML/CFT procedures, cooperation with the Luxembourg authorities (in particular with the FIU). The regime of administrative sanctions in case of breach of those AML/CFT obligations and the criminal offence in case of intentional breach of those obligations also apply.

The Netherlands

88. In the Netherlands the E-Money Directive (2000/46/EC) and Third Anti Money-Laundering Directive (2005/60/EC) apply. Payment methods on the Internet need an E-money license and a special regime will be applicable in that case. The regulatory response consists of: registration/licensing, (prudential) supervision, record keeping, suspicious transaction reporting, other specific AML policies & procedures (CDD-regulation). The providers who have a waiver have a less burdensome regime. The regulatory response consists of: record keeping, no suspicious transaction reporting, no other specific AML policies & procedures. Explicit waivers have been given for prudential purpose to five E-money institutions. Furthermore payment providers often have developed a self regulatory approach to a certain extent. The main goals for this approach are to protect the good name of the company, judicial liability issues and credit risks.

United States

89. Banking organizations that provide payment methods used for electronic commerce in the United States are subject to a full range of AML/CFT requirements, including among other things, requirements to: detect and report suspicious transactions; maintain records of funds transfers, and to implement AML compliance and customer identification programs. The cornerstone to this strong AML compliance program is the adoption and implementation of comprehensive customer due diligence policies, procedures, and processes for all customers. These processes assist U.S. banking organizations in determining when transactions are potentially suspicious.

90. When a banking organization within the United States determines a transaction is suspicious, it is required to file a Suspicious Activity Report (SAR) with the U.S. financial intelligence unit, known as the Financial Crimes Enforcement Network (FinCEN). Banking organizations within the United States are required to report transactions involving or aggregating to at least USD 5 000 that are attempted or conducted by, at, or through the institution in which the organization "knows, suspects, or has reason to suspect" the transaction: *i)* involves funds derived from illegal activities or is conducted to disguise funds derived from illegal activities, *ii)* is designed to evade the reporting or record keeping requirements of the Bank Secrecy Act (BSA) (*e.g.* structuring transactions to avoid currency transaction reporting), or *iii)* "has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the banking organization knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction."

91. The Federal banking agencies and the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) are the primary government agencies responsible for enforcing compliance with the relevant AML/CFT regulations.

92. The U.S. Federal banking agencies have been charged (under U.S. Federal banking laws 12 USC 1818(s) and 12 USC 1786(q) for banks and saving banks) with ensuring that banking organizations, subject to their respective jurisdictions, maintain effective Bank Secrecy Act/Anti Money Laundering compliance programs.

93. Several other regulations apply to electronic funds transfer activities. They concern the rights, liabilities, and responsibilities of parties in electronic fund transfers (EFT) and protect consumers using EFT systems, such as ATMs and debit cards.

Singapore

94. E-money is broadly referred as Stored Value Facility (SVF) in Singapore. Under Singapore law, a SVF is a form of prepaid electronic cash or card that can be used within the system of the SVF issuer. The SVF issuer is also known as the holder of the SVF.

95. The issuance and management of SVFs are governed by the Payment Systems (Oversight) Act 2006 (PS(O)A) and its related regulations[27]. Any entity can issue a SVF and hold the stored value. However, SVF with total outstanding stored value exceeding SGS 30 million will require approval from the Monetary Authority of Singapore (MAS) and a bank licensed by the MAS to be fully liable for the stored value. SVFs whose aggregated stored value falls below the prescribed SGD 30 million do not require MAS' approval to operate but are required to provide disclosure to advise potential users that such SVFs are not subject to MAS' approval.

96. In addition to the PS(O)A regulatory requirements, any holder SVF which issues a SVF that has a load limit of more than SGD 1 000 has to adhere to and apply the MAS AML/CFT Notice to holders of SVF on the prevention of money laundering and countering the financing of terrorism[28].

97. The Notice imposes preventive measures to holders to limit the risk of SVFs being used for illegitimate purposes. The Notice sets out obligations which require holders to take measures to mitigate money laundering and financing of terrorism risk in the following fields; *i.e.* due diligence measures (simplified, enhanced), identification of users (customers), verification of identification of users, identification and verification of identities of Beneficial Owners, non face-to-face verification, review of relevant transactions, record keeping, suspicious transactions reporting, internal policies, audit and training.

98. Any holder of SVF which fails or refuses to comply with the requirements under the Notice shall be liable on conviction to a fine not exceeding SGD 1 000 000 and, in case of a continuing offence, to a further fine of SGD 100 000 for every day during which the offence continues after conviction (under section 27B of the MAS Act[29]).

99. The MAS has also issued SVF Guidelines[30] which recommend sound principles and risk mitigating factors for all holders of SVFs. These principle-based recommendations address issues such as transparency, disclosure, public confidence, stored value protection, prevention of money laundering and countering the financing of terrorism.

---

27 *Payment Systems (Oversight) Act 2006 (PS(O)A).*

28 Monetary Authority of Singapore, (2007).

29 *Monetary Authority of Singapore Act (Chapter 186).*

30 Monetary Authority of Singapore, (2006).

China

100. There are no regulations in place addressing Electronic Commerce or Internet payment systems in China. Nevertheless, on 13.12.2007, the Chinese Ministry of Commerce issued an opinion on Enhancing the regularised Development of Electronic Commerce. The objectives of the guidance are to help the third-party electronic payment service providers to improve the reputation of the industry, operate in a prudent and stable manner, prevent blind business expansion and out-of-order competition, and ensure the safety of users' funds. The guidance encourages measures like standardised operation and management, overseeing business flow, secure electronic payment, keeping transaction data, and prevents online illegal financial transactions …

Hong Kong, China

101. Hong Kong, China does not have licensing systems for e-money and Internet payment service providers. In Hong Kong, China, 'e-money' is very much represented by Multi-purpose stored value cards. Institutions in Hong Kong China issuing or facilitating the issuance of Multi-purpose stored value cards must be authorised by the Hong Kong Monetary Authority (HKMA) under the Banking Ordinance, Cap. 155 (BO)[31]. These institutions are called authorised institutions (AIs) and are subject to supervision of the HKMA.

102. Internet payment service providers, in Hong Kong, China, only provide a platform for the users to settle various types of payment through transferring money from their designated bank accounts to that of the vendor of goods or services. Nevertheless, when such service providers carry on a business of taking deposits and cash, they have to get a licence from HKMA to conduct business as an AI.

103. The HKMA has set out various supervisory policies and requirements to be observed by AIs in the form of supervisory guidelines. The supervisory guidelines issued by the HKMA with respect to AML/CFT are the "Guideline on Prevention of Money Laundering" and the "Supplement to the Guideline on Prevention of Money Laundering". These guidelines are issued in the form of a statutory guideline pursuant to section 7(3) of the BO. These guidelines impose obligations on AIs to put in place effective systems and procedures for combating money laundering and terrorist financing and are developed based on the latest international standards including the current 40 Recommendations on anti-money laundering and 9 Special Recommendations on countering the financing of terrorism of the FATF. The requirements in these guidelines apply to AIs which issue Multi-purpose stored value cards.

104. Under the AML/CFT guidelines, AIs are required to *i)* conduct the customer due diligence process to identify and verify the identity of their customers and the beneficial owners of their customers using reliable, independent source information, *ii)* obtain information on the purpose and intended nature of the business relationship, and *iii)* conduct on-going due diligence and scrutiny of transactions throughout the business relationship. AIs are required to adopt a risk-based approach in their CDD process. AIs should develop customer acceptance policies and procedures that aim to identify the types of customers that are likely to pose a higher money laundering/terrorist financing risk. For those customers identified with higher ML/TF risk, AIs should adopt a more extensive customer due diligence process and subject them to close monitoring. In undertaking the CDD

---

[31] A Multi-purpose stored value card is defined in the BO as a card on which data may be stored in electronic, magnetic or optical form and for or in relation to which a person pays a sum of money to the issuer of the card (directly or indirectly) in exchange for *i)* the storage of the value of that money, in whole or in part on the card; and *ii)* an undertaking by the issuer (express or implied) that the issuer or a third party will, on production of the card, supply goods and services (which may include money). There is currently only one issuer of Multipurpose stored value cards (*i.e.* Octopus Cards Limited) in Hong Kong, China. The Octopus Cards Limited is authorised as a deposit-taking company under the BO. Octopus cards are designated for small amount retail payments and there is a maximum storage limit of HKD1 000 per card.

process, AIs should, whenever possible, conduct a face-to-face interview with a new customer to ascertain the customer's identity and background. In cases where a face-to-face interview is not conducted, they should apply equally effective customer identification procedures and on-going monitoring standards to mitigate the risk. The AML/CFT guidelines also require AIs to keep proper account and transaction records.

105. Section 25A of the Organised and Serious Crimes Ordinance, CAP 455, (and similar provisions under Hong Kong's anti-terrorist financing legislation) provides requirements for reporting of suspicious transactions by all persons in Hong Kong to Hong Kong's Joint Financial Intelligence Unit, (JFIU). Failure to report a suspicious transaction is a criminal offence. All parties engaged in financial transactions of any kind must have systems in place to detect suspicious transactions to comply with this law, but the exact methods used are the responsibility of each company. Moreover, under the HKMA's AML/CFT guidelines, AIs should put in place effective management information systems to enable them to identify and report suspicious transactions. The Organised and Serious Crime Ordinance and Drug Trafficking (Recovery of Proceeds) Ordinance, (and similar provisions under Hong Kong's anti-terrorist financing legislation) makes provision for reporting of STRs to the JFIU. The reporting obligations apply to any person who knows or suspects that any property represents any person's proceeds of an indictable offence, or the property was used in connection with or is intended to be used in connection with an indictable offence, he shall disclose that knowledge or suspicion to an authorised officer (*i.e.* JFIU officer) as soon as practicable.

106. The HKMA ensures compliance of AIs with its AML/CFT guidelines through its on-going supervisory process. If an AI fails to comply with a requirement under the AML/CFT guidelines, the HKMA will require the AI to take appropriate remedial actions to rectify the situation. The HKMA will follow up with the AI to ensure that the deficiency has been satisfactorily addressed. Where the non-compliance is considered to be serious, the HKMA will impose supervisory measures against the AI[32].

Australia

107. Payment methods are regulated largely by a combination of the Payments System (Regulation) Act 1998, the Payment Systems and Netting Act 1998, and the Electronic Funds Transfer (EFT) Code. The Reserve Bank of Australia (RBA) administers the Payments System (Regulation) Act 1998, and the *Payment Systems and Netting Act 1998* with the goal of achieving efficiency, competition and stability. The Australian Securities and Investments Commission administers the EFT Code with the goal of providing consumer protection.

108. Australia's primary anti-money laundering and counter-terrorism financing (AML/CTF) legislative package includes the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) and Anti-Money Laundering and Counter Terrorism Financing Rules. The AML/CTF Act sets out general AML/CTF principles and obligations. With the details of how these obligations are to be carried out being set out in subordinate legislative instruments known as the AML/CTF Rules.

109. The AML/CTF Act covers the financial sector, gambling sector and bullion dealing and any other professionals or businesses that provide particular designated services. Being activities-based,

---

[32] There is a broad range of supervisory measures available to the HKMA. They include for example issuing a statement of warning to the senior management of the AI, imposing restriction on the AI's business, downgrading the supervisory ratings of the AI and commissioning an external auditor to review the AML/CFT system of the AI. In the event that the AI fails to take appropriate remedial actions, the HKMA will consider exercising its formal powers under the BO, which include withdrawing the consent given to the responsible directors and chief executives, attaching conditions to the AI's authorisation, requiring the AI to seek advice from an Advisor appointed by the HKMA and suspending or revoking the authorisation of the AI. The supervisory measures to be taken in each case will depend on the seriousness of the deficiencies identified in the AI and are considered to be effective, proportionate and dissuasive.

under the AML/CTF, it does not matter how designated services are provided (*i.e.* electronic, paper or face to face).

110. The AML/CTF Act imposes a number of obligations on businesses (called reporting entities) when they provide these designated services. These obligations include: customer due diligence (identification, verification of identity and ongoing monitoring of transactions); reporting (suspicious matters, threshold transactions and international funds transfer instructions); record keeping, and establishing and maintaining AML/CTF program.

111. The AML/CTF Act implements a risk-based approach to regulation. Businesses are able to determine the way in which they meet their obligations based on their assessment of the risk of whether providing a designated service to a customer may facilitate money laundering or terrorism financing. The AML/CTF Rules specify how the obligations may be complied with by a reporting entity putting in place appropriate risk-based systems and controls. When determining and putting in place appropriate risk-based systems and controls, the reporting entity must have regard to the nature, size and complexity of its business and the type of ML/TF risk that it might reasonably face. In identifying its ML/TF risk a reporting entity must also consider the risk posed by the following factors: its customer types, including any politically exposed persons, the types of designated services it provides, the methods by which it delivers designated services; and the foreign jurisdictions with which it deals.[33]

112. The Australian Prudential Regulation Authority (APRA) authorises certain e-commerce payment mechanisms to be a Purchased Payment Facility (PPF). PPFs, such as smart cards and electronic cash, are facilities which consumers pay for in advance and use to make various types of payments. Consumers rely on the holder of the stored value redeeming that value on demand.

113. APRA's prudential standard regarding PPF's seeks to ensure that those who provide PPF facilities are subject to prudential requirements commensurate with their risk profile. A PPF provider is not authorised to conduct general banking business. Under the prudential standard, a PPF provider is required to comply with AML/CTF requirements as administered by AUSTRAC (under the Anti-Money Laundering and Counter-Terrorist Financing Act 2006).

114. APRA also authorises those who carry on a credit card issuing and/or acquiring business in Australia as a "specialist credit card institution" (SCCI). SCCIs are a special class of authorised deposit-taking institutions (ADIs) that are authorised to perform a limited range of banking activities. SCCIs may only perform credit card issuing and/or acquiring business and any other services related to credit card issuing and/or acquiring. SCCIs are not permitted to accept deposits (other than incidental credit balances on credit card accounts).

[33] [Australian] Attorney-General's Department (2007).

RISK MANAGEMENT MEASURES TAKEN BY THE SECTOR

Introduction

115. As with any type of business, commercial websites and Internet payment systems are confronted with various types of risks ranging from the technical safeguards of their websites from computer hackers and viruses to the outright criminal misuse of their systems by criminals for purposes of facilitating fraud, and Internet payment systems for money laundering and other financial crimes. Risk management is therefore an ongoing process that may be developed by commercial websites and Internet payment systems to minimise their exposure to various risks. This may include the establishment of customer user agreements and policies by a company that set strict rules and policies for the use of their respective system by a user. In addition, commercial websites and Internet payment systems may also establish "best practices" designed to set internal standards for how a company may safely operate while at the same time providing effective services to their users. Risk management may also encompass Anti-Fraud and Anti-Money Laundering/Terrorist Financing (AML/TF) programs that may have been implemented by commercial websites and Internet payment systems. Finally, a risk-based approach may also integrate other initiatives that are undertaken by a commercial websites and Internet payment systems that are required under the regulatory regime of a specific country or jurisdiction where a commercial websites and Internet payment systems may provide services, *e.g.* reporting requirements (for Internet payment systems), etc. Other stakeholders (such as the tax authorities and authorities supervising payments) are or must be involved in the fight against ML or TF and the mitigation of ML or TF risks. If commercial websites have no reporting obligations they are controlled by these stakeholders.

AML/CFT mechanisms used to mitigate fraud, money laundering and terrorism financing risks

116. Internet Payment service providers, subject to regulations from a supervision authority, mitigate the above mentioned ML/TF risks by applying different mechanisms. During the study the project team obtained confirmation on the use of such mechanisms by consulting, as mentioned in the introduction, one of the most important mediated customer-to-customer commercial websites and Internet payment service provider as well as a smaller electronic money issuer and the Electronic Money Association representing a range of e-money issuers and payment service providers. The project team also obtained confirmation that AML/CFT regulations imposing similar mechanisms apply to Internet payment service providers in the most industrialised countries.

117. A non-exhaustive list of these mechanisms is provided in this section:

- Implementing important worldwide security teams patrolling sites to detect fraud and misuse.
- Applying risk-based Customer Due Diligence (simplified CDD vs. enhanced CDD).
- 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, stolen credit cards …).
- 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.
- Monitor, using risk models built to detect bad activities, information:
  - obtained from customers (identity, address, e-mail and IP addresses used, About Me page, …)
  - collected from customers (phone call to sellers, …)
  - obtained internally (previous transactions, item country location, customer location, shipping methods used, behaviour of customers during auction processes, accepted payments, …)
  - obtained from external sources (countries at risk for certain forms of criminalities, check listings of presumed terrorists or terrorist groups, …)
- 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.

118. The most organised Internet payment service providers collect a range of data and information about movements of funds between buyers and sellers, located in different countries all over the world but customers of the same Internet payment service provider, commercial transactions between buyers and sellers, data and information accumulated over a long period of time and available centrally.

119. Consequently, they have a global view of the movements of funds and the commercial transactions between buyers and sellers internationally, information that the banks of buyers and sellers do not have. They can easily reconstruct commercial transactions and movements funds between different countries and persons in the world.

120. Certain Internet payment service providers have the opportunity to access data and information on the commercial transaction underlying a financial movement of funds because they provide payment facilities to commercial websites belonging to the same financial group. Nevertheless, certain Internet payment service providers providing payment facilities to commercial websites not belonging to the same financial group can also obtain but in a more limited way information on underlying commercial transactions.

121. An easy data sharing of information with commercial websites reduces the risks of misuse and the risks of ML/TF.

122. If Internet payment service providers adequately monitor the financial transactions of their customers by detecting deviations from their customer's known profile of transactions, the non face-to-face contact at the beginning of the relationship with the commercial website and Internet payment service provider may not constitute a problem.

123. Nevertheless, it is worth mentioning that an Internet payment service provider will be able to build a better and much accurate customer's profile of transactions if the number of transactions performed by a customer is significant.

124. Exchange of information between commercial websites and Internet payment services providers possibly located in different countries is sometimes not easy because of the differences in the privacy legislation.

125. As already mentioned in the subsection regarding regulations, AML/CFT reporting obligations are applicable to Internet payment service providers in the country in which they are physically located. Certain commercial websites and Internet payment service providers work closely with law enforcement. They encourage regulators and law enforcement to play an active role in the fight against the use of commercial websites and Internet payment service providers for criminal activities.

CONSIDERATIONS ON "SECOND LEVEL OF CONTROLS VERSUS THIRD LEVEL CONTROLS"

126. Internet payment service providers, licensed as e-money providers or as a bank, have several obligations in the field of identification of customers, detection, monitoring and reporting of suspicious financial transactions. As explained in the section above, they have access to a wide range of information for monitoring the transactions of their customers and certain Internet payment service providers have implemented ongoing due diligence mechanisms which include: scrutiny of transactions undertaken throughout the course of the relationship to ensure the transactions conducted are consistent with their customer's known profile. In many cases, the profile of a customer can only be deducted from previous transactions with the payment service provider.

127. When services of Internet payment services providers are used, banks of buyers and sellers do not have a global view of the flow of funds between buyers and sellers, as this information is only known by the Internet services provider itself. A customer of a bank may order his bank to transfer funds from his bank account to his account with an Internet payment service provider. Afterwards the customer will request the Internet payment service provider to transfer funds for a purchase on a commercial website. The bank can be totally unaware of this purchase and the reasons for funding the account with the Internet payment service provider. In the United States, similar cases have been identified with payments requested by customers of banks in favour of Internet payment service providers and used thereafter by these customers on gambling websites, without the bank knowing the funds were used for this illegal activity in the United States.

128. But banks still have an important role to play in the monitoring and detection of suspicious transactions, even if the funds are transferred to or originate from an Internet payment service provider. For instance, a transaction with an Internet payment service provider can be abnormal or disproportionate to the bank with regards to the known profile (professional activities, professional revenues, customer bank transactions profile) of its customers.

129. It is also important that financial institutions, such as the banks, do not exonerate themselves from their AML/CFT responsibilities, in particular the detection of suspicious financial transactions, when the funds originate from an Internet payment service provider, and even if the transactions concern relatively small amounts. A statement or a printout of a screen of the commercial website showing an item on sale must not immediately and unconditionally considered as an invoice or justifying a financial transaction on the bank account of the customer. Conversely, the presentation of such justification document could be used as a red flag or indicator for the financial institution.

POLICY IMPLICATIONS

130. ML/TF risks associated with commercial websites and Internet payment systems have been analysed and the focus has been put on the type of electronic commerce identified for various reasons (increasing popularity, easy access, available to private individuals, high volume of cross border trade transactions …) as the most susceptible to be used by criminals for ML/TF: mediated customer-to-customer. The work of the project team has led to the following key findings with respect to ML/TF vulnerabilities of commercial websites and Internet payment systems.

Key findings

131. Criminals have shown adaptability and opportunism in finding new channels to launder the proceeds of their illegal activities and to finance terrorism. As the Internet becomes more and more a worldwide phenomenon, commercial websites and Internet payment systems appear to be subject to a wide range of risks and vulnerabilities that can be exploited by criminal organizations and terrorist groups.

132. Various vulnerabilities of commercial websites and internet payment systems have been highlighted: the non face-to-face registration which may lead to identification problems; the speed of transactions, the limited human intervention and the high number of transactions, which may cause problems concerning audit trails, monitoring and detection of transactions; the international character, which is inherent to the Internet, which may create issues concerning jurisdictional competences; difficulties for traditional financial institutions to monitor and detect suspicious financial transactions with the consequence that their abilities in the detection of suspicious financial transactions, when an Internet payment service provider is used, could be affected.

133. Some of the ML/TF risks associated with trade-based money laundering and non face-to-face business and financial transactions apply also to commercial websites and Internet payment systems. The financial transactions that are initiated from a bank account or a credit card (which is the majority of online payments) already involve a customer identification process as well as transaction record keeping and reporting obligations. While low value transactions do not equate to low risk, these transactions are subject to the regulatory controls already applicable to the financial sector and may be consequently less risky. Regarding the risks associated with the non-face-to-face registration and the possible anonymity of the users the study highlights the need for online identity verification solutions (the electronic identity card used in certain countries for instance) to help commercial websites and Internet payment service providers mitigate the risks of criminal activity. The report also indicates that if Internet payment service providers adequately monitor the financial transactions of their customers, monitoring for and acting on deviations from the customer transaction profile, the lack of face-to-face contact at the beginning of the relationship with the commercial website and Internet payment service provider may not constitute a problem. Online and offline retail merchants and payment services should have comparable AML/CFT obligations.

134. It is also important that efforts to fight against fraud and ML/TF by commercial websites and Internet payment service providers in different countries not be hampered by divergent privacy legislation, potentially interfering with the amount of customer information that service providers could exchange regarding suspected ML/TF.

135. Although the challenges to identifying TF apply equally to Internet payment systems (the suspicions being mostly based on name matching with the names provided by the competent authorities), it is not always necessary for Internet payment service providers to identify TF in their

STRs in order to help counter terrorist financing. Any suspicious activity is important to report regardless of the type of activity. Some Internet payment service providers have put in place systems to detect, monitor and analyse suspicious transactions - even for small amounts.

136. Concerning the risk-based approach to combat ML/TF we can refer to the June 2007 FATF Guidance which states that : "By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention." Applying this principle to online transactions, the private sector may be allowed to consider low value consumer payments initiated from financial institutions or credit card account (which require customer identification and verification procedures, as well as transaction record-keeping and reporting policies), to be of lower risk than transactions initiated through services providers without AML/CFT obligations.

137. The risk of fraud and the sale of illegal goods are among the concerns of commercial websites and Internet payment systems. These concerns are among the motives for commercial websites and Internet payment systems to secure their communications, websites and payment systems. In some jurisdictions online commercial websites are not as such required to detect or fight against ML/TF, but have a market incentive to detect fraud.

138. Some commercial websites and Internet payment service providers, aware of the risk of being used for illegal activity, have set up departments to screen and monitor the transactions of their customers, using a risk-based approach. In addition to monitoring for fraud, some commercial websites and Internet payment service providers have also set up AML/CFT mechanisms. Best practices in the sector, including customer due diligence, monitoring transactions, not accepting anonymous forms of payment (cash for instance) imposing transactions limits, maintaining transactions records, and reporting large or suspicious transactions to the competent authorities, could be helpful for other parties of the private sector.

139. The collaboration between commercial websites and Internet payment service providers to exchange information on commercial transactions underlying financial transactions is a factor which mitigates money laundering and terrorism financing risks, as well as risk of fraud. Legal dispositions encouraging such exchange of information could be very useful.

140. The report concludes that, as long as the sector, and the relevant competent authorities, understand the potential vulnerabilities associated with commercial websites and Internet payment systems and appropriate risk-based measures with regard to customer identification, record keeping and transaction reporting are taken, the mentioned issues may not necessarily constitute a higher risk for the online sector than for the offline sector.

141. The project team believes that even though awareness of ML/TF amongst major players in the online sector is increasing, due to efforts made by regulators and trade associations, efforts need to be made to increase this awareness, particularly regarding the mechanisms of ML/TF.

142. Given the international character of commercial websites, international cooperation is a key factor. Cooperation between, for example, FIUs, law enforcement and other parties involved is therefore important. Internet payment service providers report in the country where they are established (got a license) and not in the country of residence of the individuals involved in the suspicious financial transactions, which for FIUs and law enforcement may lead to identification and follow-up problems (it is difficult to confirm the true identity of the parties involved in the transactions in the country of the disclosure given that the individuals do not live in the country and the transactions are difficult to explain / justify as they does not take place in the country where the Internet service provider is located and reports.

Issues for consideration

143. Looking ahead, there appear to be a number of areas that could be considered to improve the capacity to cope with ML/TF risks associated to commercial websites and Internet payment systems.

144. **Building a better awareness:** Creating an understanding of the ML or TF risks amongst governmental bodies and the private sector is critical. Making the traditional financial institutions aware of their role in the detection and the monitoring of suspicious financial transactions. Therefore it is necessary to raise awareness by identifying red flags and typologies. Awareness could also be raised by training programs and outreach sessions to the private sector. The regulators and trade associations which have already contributed to the issuance of AML/CFT guidance to the sector and the development and issuance of ML/TF typologies could be of great help.

145. **Imposing similar regulations**: Given the international character and presence of Internet, it is difficult to determine which jurisdiction has regulatory authority over an Internet payment service provider, and how enforcement action can be applied if there are violations. World based Internet payment service providers have locations and licences in different countries and regions. It is consequently important that governments impose similar regulations, requiring customer identification, CDD, record keeping and transaction reporting, to Internet payment service providers all around the world, to avoid certain Internet payment service provider choosing the country with the poorest regulations or not at all regulated.

146. **Exploring industry best practices**: The high standard for customer due diligences and the sector best practices (monitoring of transactions, non-acceptance of certain forms of payment (cash for instance) considered as high risk for ML/TF, limits imposed to transactions, …) identified during the workshop and presented in the report could be helpful for other players in the private sector and could be an important part of the training programs and outreach sessions to the private sector.

147. **Bearing in mind that international cooperation is a key factor**: International cooperation is a key factor in the fight against ML and TF given the international character of the Internet and commercial websites activities. Countries need to work cooperatively to identify and combat the use of commercial websites and Internet payment systems for ML/TF purposes. International cooperation to ensure that entities operating in multiple jurisdictions are being properly regulated and monitored somewhere is also important.

148. Approaching the Egmont group in order to discuss the awareness raising amongst FIUs in view of combating ML/TF via commercial websites and Internet payment systems: There is a need to explore ways FIUs can enhance the exchange of information and data pertaining to the criminal misuse of commercial websites and Internet payment systems.

REFERENCES

[Australian] Attorney-General's Department (2007), *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*, accessed through: *www.comlaw.gov.au*.

FATF (2006a), *Report on New Payments Methods*, FATF, Paris, *www.fatf-gafi.org*.

FATF (2006b), *Trade-based Money Laundering*, FATF, Paris, *www.fatf-gafi.org*

FATF (2007), *Guidance on the Risk-Base Approach to Combating Money Laundering and Terrorist Financing, High Level Principles and Procedures*, FATF, Paris, *www.fatf-gafi.org*.

Federal Trade Commission (2007a), "*About the Bureau of Consumer Protection*", Federal Trade Commission web site, *www.ftc.gov/bcp/about.shtm.*

Federal Trade Commission (2007b), "*Division of Enforcement*", Federal Trade Commission web site, *www.ftc.gov/bcp/about.shtm.*

Monetary Authority of Singapore, (2006), "*Stored Value Facilities Guidelines"*, accessed at: *www.mas.gov.sg/resource/legislation_guidelines.*

Monetary Authority of Singapore (2007), *Prevention of Money Laundering and Countering of Terrorism – Holders of Stored Value Facilities*, Notice PSOA-No.2, Singapore, accessed at: *www.mas.gov.sg/resource/legislation_guidelines*.

Monetary Authority of Singapore Act (Chapter 186), http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED-186&doctitle=MONETARY%20AUTHORITY%20OF%20SINGAPORE%20ACT%0a&date=latest&method=part.

Munro, Neil (2001), "*Internet-Based Financial Services: A New Laundry?*", *Journal of Financial Crime*, Henry Stewart Publications, Vol. 9, No. 2, pp. 134-152, Henry Stewart Publications.

Philippsohn, Steve (2001), "*The Dangers of New Technology – Laundering on the Internet*", *Journal of Money Laundering Control*, Henry Stewart Publications, Vol. 5, No. 1, pp. 87-95.

[Singapore] *Payment Systems (Oversight) Act 2006 (PS(O)A)* accessed at: *www.mas.gov.sg/legislation_guidelines/payment_system/payment_act2006/Payment_Systems_Oversight_Act_2006.html.*

***