MONEY LAUNDERING TECHNIQUES WITH ELECTRONIC PAYMENT SYSTEMS

Krzysztof WODA

Abstract: In case of terrorist actions, the main emphasis lies on the security aspect. Nevertheless, the financial aspect, as for example the collection, transfer and withdrawal of money from the payer to the payee plays an equally important role for preparation of terrorist actions. Besides, the techniques of money laundering are often used to conceal or disguise the origin, nature, source, location, disposition or ownership of assets financing terrorist actions. The Financial Action Task Force (FATF) organization has identified many activities and typologies used for money laundering or terrorist financing, e.g. with shell companies and nominee, through unofficial money transfer systems, "smurfing" practices (through dividing of large payment sums into multiple deposits under the threshold value), transfers, money smuggling, etc. Many of these activities are carried out by means of electronic payment systems, which transfer the monetary values over telecommunication networks. Customer instruments such as Internet software (electronic purse), smart cards, mobile devices, debit and credit cards could be applied as payment instruments. The suitability of an electronic payment system for financing of illegal activities depends to a great extent on such supported characteristics as anonymity, mobility, etc. It can be furthermore assumed that payment systems differ with regard to their suitability for a single money laundering phase (and thereby for terrorist financing). The multi-process character of money laundering is typical for terrorist financing and often contains a series of transactions from collection of money to money withdrawal in order to conceal the origin, nature or disposition of money.

Keywords: Money Laundering, Terrorist Actions, Electronic Payment Systems.

Introduction and Definitions

Money laundering is an intentionally committed offense that signifies the conversion and transfer of assets of an illicit origin. The objective of this action consists of disguising the true origin, location, nature, disposition, movements and transfer of assets that are derived from illegal activities.[1] Participation, support or facilitation of the realization of illegal activities, such as transfer of money of illicit origin to several

INFORMATION & SECURITY. An International Journal, Vol.18, 2006, 27-47.
© ProCon Ltd. This article cannot be reprinted, published on-line or sold without written permission by ProCon.

bank accounts and afterwards their conversion into legal financial products, are regarded also as money laundering actions.

Different goods are considered as potential assets for money laundering; they can to a different degree fulfill the functions defining money ("medium of exchange," "store of value," and "unit of account"). The assets with distinctive "medium of exchange" function include highly liquid funds like cash, sight deposits, checks and electronic currencies, as for example prepaid bearer payment instruments (e-money) and virtual gold currencies. The gold currencies support particularly the "store of value" function, while they are based on real gold reserves with current market value. Besides, gold acts as an internationally exchangeable property with simply calculated prices in various currencies ("unit of account") as well as a direct payment instrument (bearer instrument) without identification features as for example credit card number or bank account number. Typical finance products and real estates as well as products and services of certain commercial branches could also be considered as other assets for money laundering, such as those coming from restaurants, casinos or shops in e-commerce.

The transformation of liquid funds or cash into finance products is often a crucial moment for detection of illegal activities.[2] This could be accomplished often as checking the business activities of suspects by state authorities (e.g., related to tax payments), audit companies and banks (following some money laundering guidelines); however, the origin and disposition of assets must be determinable in case of legal activities.[3] The money launderer can use the anonymous funds or generally accepted money currencies functioning as medium of exchange for any intended purpose (also terrorism financing) only if this money has left the business cycle successfully, i.e. without disclosure of its illicit origin. Such stepwise introduction, movement through several cash transaction systems and business cycles and, in the following, legal use of the laundered money is called in general *placement*, *layering* and *integration* of assets in the money laundering cycle.[4] In the placement phase, assets from criminal activities are mostly deposited (on a bank account, e.g., against checks), invested (in finance products) or smuggled (cash, diamonds). The layering phase consists of transfers of the placed assets between several accounts in different institutions and other business participants with the purpose to conceal the identity of the true owner or the trading person. Besides, the illegally trading persons try to avoid different legal restrictions, as for example the report obligation for transaction amounts above legally defined level (currency change, owner of foreign bank accounts). In the integration phase, the legal as well as the illegal assets are combined together and integrated into the business cycle. The already inseparably booked assets will be often transferred back to the owner, now as legalized possessions.

The money laundering techniques and the laundered money are often used for terrorist financing. The planning, logistics and acquisition of objects for terrorist actions often require a cross-border transfer of funds to the country of destination. Direct importing of cash will be avoided for the reason of strict border control; more sophisticated techniques will rather be applied for quick and mostly complex transfer of funds through existing legal and illegal transfer systems and financial instruments. Electronic payment systems are generally characterized by high performance and mobility; some of them have also such important features as for example anonymity of transfer, cross-border payment possibility, cost efficiency, as well as high security of communication (confidentiality) due to the use of cryptographic procedures. Therefore, the electronic payment systems are quite suitable for the conduct of money laundering operations in every phase of the money laundering cycle.

The aim of this article is to analyze the possible techniques for money laundering and terrorism financing, which can be carried out with electronic payment systems. Furthermore, the article will identify the most important characteristics of the particular payment systems, which predetermine such systems as especially suitable for illicit activities. Finally, solutions will be presented to reduce the risk of illegal money transfers with electronic payment systems.

Money Laundering Techniques with Electronic Payment Systems

The money laundering techniques involve direct use of electronic payment systems for terrorism financing or their use only as a transporting instrument in one of the three phases of the money laundering cycle. In what follows, the typical techniques for money laundering involving the use of electronic payment methods and identified by the Financial Action Task Force (FATF) organization will be presented.

Transfers

Money wire transfers can be characterized as the easiest transfer method within the money laundering activities. Transfers are financial transactions by which value unities are transported from the payer to the payee electronically over telecommunication networks. In case of money laundering, often the sender and the receiver of the transferred money is one and the same person who tries to conceal the origin of money by several money movements (transfers).[5] In general, there exist legal transfer systems and illegal ones, often called parallel bank transfer systems. The legal transfer systems comprise, in the private customer area above, all electronic banking and, in the corporate clients area, the international large value payments through SWIFT or TARGET. The illegal transfers take place through systems such as Hawala for example, which are based on informal or trust connections and effect money transfer without using official bank accounts. The legal transfers can be well traced due to ar-

chiving of the transaction data by the financial institutions. Exceeding some legally fixed threshold values for money transfers or deposits, as for example 15,000 Euros in the EU (Directive 2001/97/EC, Article 3) or $10,000 in the U.S. (Section 326, the U.S. Patriot Act), automatically triggers reporting and checking of the origin of money by bank employees and then, in suspicious cases, by supervisory authorities. Even opening an account in a bank or a financial institution (on-line broker, mutual funds, and insurance companies) requires an extensive customer identification (e.g., the Customer Identification Program in the U.S.) and investigation, as for example in the U.S. through comparison with the lists of private individuals or organizations whose assets were frozen by the Treasury Department.[6]

Despite the electronic tracking, investigation possibilities and identification requirements, the transfers are an efficient money transferring method for terrorist financing. The following cases can be considered as possible abuse cases:

- *The use of falsified or false identities* (front men, letterbox companies). Customers with good reputation, often on the basis of ethnic, religious or cultural affiliation with the money launderers or terrorists, let the transfer of money through their official bank accounts internationally. The legal account holders can further guarantee to the money launderers access to their bank accounts by disclosing their PIN or password. Therefore, it would be difficult to distinguish bank accounts for a suspicion of money laundering (assuming that the transfers would not contain extraordinary large amounts of money), due to the fact that they combine legal transfer(s) with the illegal ones. Also, email accounts are often opened with false identity at public places (e.g., library, university) to conceal the real identity.[7]
- *Structured payments* also called "*smurfing*." Large payments are split and transferred always in smaller sums that lie under the legal threshold value required for checking on suspicion of money laundering. Such payments are conducted through several channels (phones, online-banking, chip cards with electronic purse function, mobile payment systems) to complicate the detection of structured payments.
- *Transfers through banks in offshore countries* with customer identity protected from jurisdiction. The opening of bank accounts as well as the transfers can occur only on the Internet, so the investigation have to rely solely on electronic evidence like the visited IP addresses, the computer cache, as well as the information about the conducted transactions stored on the server of the Internet Service Provider (ISP). However, the Internet Service Provider would often be chosen from countries without restrictive bank regulation or countries not-cooperating with organizations like FATF that prevent cooperation between service providers, banks, and the authorities. Furthermore,

the relevant information about the transactions could be encrypted symmetrically or asymmetrically by cryptographic software programs (containing known algorithms as RSA, AES, Triple-DES, etc.) and, therefore, it can be confidentially exchanged between the participants (e.g., terrorists) without risk of disclosure by the authorities. A report of the U.S. Treasury points to another technique for hiding information – the technique of email drafts.[8] All the terrorists receive the password and the user name for a given email account. If one of them writes a draft, without sending it, then this draft remains on a provider server for this email account. All the terrorists could then access the account and read the draft.

- *Transfers as a result of criminal actions*, as for example hacking of bank systems or attacking private computers (the man-in-the-middle-attack). Such attacks can be used mainly for fundraising for terrorism financing, but not for money laundering since money laundering is a multistage and often a long-term process that goes also through legal transaction systems and business cycles with the objective to legalize the funds.
- *Informal money transfer systems*, such as Hawala, enable a special category of transfers in the Far and Middle East. Money is deposited at a Hawala representative in the country of the payer and is paid by another Hawala representative in the country of the payee. The Hawala representatives calculate their demands and liabilities often mutually or balance the difference through their bank accounts. The payments in the Hawala system are predominantly cash-based, while the communications and the payment confirmation occur often electronically (e.g., email, fax, chat). Hence, the Hawala transfer system combines the advantages of the traditional cash systems (anonymity, no registration of the transactions, and transferability to other private individuals (person-to-person)) with the advantages of electronic communication (high speed and cost efficiency).

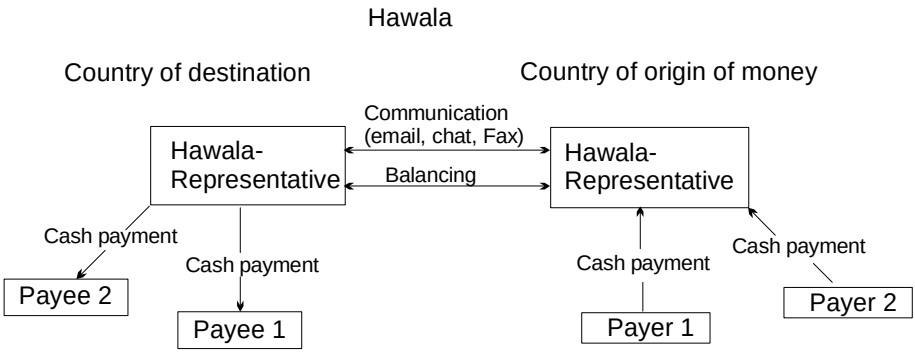

Figure 1: The Hawala System.

The electronic wire transfers are the easiest method for terrorism financing, nevertheless, with high risk for detection. Prior to the terrorist attacks in America on September 11, 2001, the transfers were considered less suitable for terrorist financing because of the risk for electronic tracking (the money for performing the attacks on the WTC were transferred mostly with legal wire transfers and illegal Hawala transfers).[9] The possible combination of wire transfers with the Hawala system as well as the use of the Internet for communication determine the transfers as ideal instruments for short-term illegal activities such as terrorist actions. The transfers are also suitable for money laundering, however, only to a limited degree, mainly during the layering phase for multiple movements of money between accounts.

Shell Companies, Offshore Corporations, Nominees, and Charities

While the wire transfers have a one-time character and a high risk of detection mainly when transferring large sums, different business activities are used for long-term money laundering and sophisticated terrorist financing. Registered companies or non-profit organizations like charities can transfer larger amounts over borders than private individuals. The charities often operate in crisis areas where also the terrorists are active. Even if the enterprises or organizations are supervised by the authorities (e.g. bank supervisory or tax authorities), it leads mostly to no indications for terrorist financing. Also, the on-line check of the WWW contents or the check of logs can often deliver no direct indication of suspicious cases. In such cases, it should be rather looked for the list of charities' contributors; however, the contributors commit no crime if they have no idea of the illegal financing activity of the charity. Raising money for humanitarian purposes could generally not be distinguished from the financing of illegal activities. Therefore, key role in detecting illegal financing activity of a charity may play the use of the means or the history of the conducted transfers. Unfortunately, the charities or the other money raising organizations often operate on informal basis in quite closed groups, such as ethnic or religious groups, and afterwards can transfer money also informally, e.g. through the Hawala system, so there is no track of transfers or fundraising in official transaction systems.

The charities can themselves operate as informal transfer system if, for example, their employees are in several countries (also in the countries where terrorists operate), and carry out illegal transfers. Then transfers take place without transferring the money physically; rather internal accounts are balanced without leaving a track in the legal bank system. In addition, the charities are often linked organizationally with each other or are represented by the same persons what complicates at last the later investigation of the cases.

The use of the so-called shell and offshore corporations (or from offshore territories) offers another method for big money transfers. The shell corporations are enterprises

without usual business activity, assets, and liabilities. They are rather used only as an intermediary for the transfer of capital. They become often linked or pyramided to disguise the track of moved and laundered money. Generally, the shell companies have merely an address (e.g., a letterbox company), a manager (nominee like attorney or manager of the offshore corporation) and often many bank accounts. The funds are sent electronically through bank accounts and between different places worldwide. Hence, shell corporations can function as ideal camouflage for illicit money mainly in the layering phase of the money laundering process.[10]

An indication of potential illegal activity of a shell corporation provides the owner's structure and activity profile of the company. The owners of the shell corporations often become the actual owner of the bearer shares or unregistered stock, thus no private person or shareholder is registered in the commercial register.[11] Such omitted regulation appears in some offshore centers with restrictive bank secrecy law, also for enterprises, allowing the owners of shell corporations not to be identified. Other advantages from the offshore location of a shell corporation are the possible tax exemptions and the strict protection of customer privacy by the attorney-client relationship, e.g., in case of investigation by supervisory authorities of another country.

Shell corporations in offshore countries are well suited for the integration phase of money laundering. After the money has been moved to an offshore center (e.g., by structured payments through several bank accounts, charities or by transfer of virtual gold currencies), it can return to the owner already in a legal form. A known method is the loan-back schema. The placed money is transferred in form of a loan, e.g., from a shell corporation or an offshore bank to the domestic company (furthermore, no taxation on the loan or laundered money is due). The loan is paid back with laundered money and officially appears as an origin of the money to the borrower (money launderer). In reality, often in the money laundering case, the borrower as well as the credit grantor is the same physical person who conceals his real identity using companies (shell corporations), nominees, etc.

Other schemas include manipulations with invoices for delivered or ordered goods and services. In case of under-invoicing, the beneficiary (seller) gets a very low amount of money, far below the usual market price for a delivered product (e.g., computers, cars); while the payer (buyer) can resell the product and can thereby register big profits (laundered money).[12] The seller pays in reality, e.g., an illicit goods delivery (drugs, weapons), or acts as a shell corporation which conceals the identity of the contractor (in money laundering cases the seller and the buyer is one and the same physical person). With the over-invoicing schema, exorbitant prices for goods and services are paid by contractors resulting in extraordinarily high profits (laundered money) for the seller. Such transactions are often characterized by fictitious deliveries of goods and services or have hardly determinable values (e.g. market

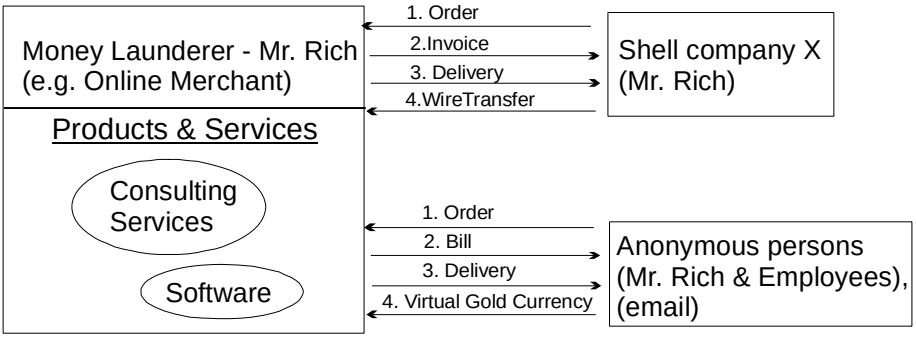

Figure 2: Over-Invoicing on the Internet

analysis, consulting services, and software products on the Internet). The transactions with software programs on the Internet, for example, can be carried out by shell corporations from offshore territories and anonymous persons (merely with email address or IP number identifiable), or with anonymous electronic payment systems, which makes the retracing from the payee to the payer practically impossible. Thus, the transferred money for goods or services is legalized and can be reintegrated in the business cycle (e.g., real estate purchase or business activities of a legal enterprise).

The role of the electronic payment systems in the traditional money laundering techniques with companies is very important. Most transfers take place electronically using electronic banking (e.g. electronic fund transfers (EFT)), through SWIFT, TARGET or by the involvement of virtual currencies such as gold currencies on the Internet. Many providers of virtual gold currencies are located in offshore centers whereby the transfers in the layering phase of money laundering may be anonymous.[13] The transfers are often final (no chargeback risk) and leave no information at the providers of private currencies or transfer systems. Without electronic payment systems, the money laundering models with shell corporations (or from offshore countries) would be not so effective since it would require transporting of the physical cash by a courier to an offshore centre in the placement phase of money laundering (with the concomitant high risk of detection).

Financial Products

The financial products are ideal instruments in the integration phase of the money laundering process given the size of the market, the easy access and the availability as well as the diversity of products. Primarily, insurance policies are bought to legalize the laundered money, e.g., through income from life insurance policies.[14] The advantage of the insurance products for possible money laundering transactions lies in the

free access to such products given that broker and external agents are rather interested in profits than in the due diligence of the customers. In addition, another party could benefit from payment of insurance policies. Detecting money laundering activities is clearly complicated if the insurance policies were bought in offshore-centers or through trustees or nominees.

Other financial products could also become investment objective of money launderers as, for example, share certificates, bonds or not-standardized derivatives such as swaps and futures. Not-standardized securities could mainly be used in deals between a money launderer and a shell corporation that belongs to him and could be the origin of high-level-speculative profits or losses. Such high-level-speculative trading between the members of a criminal network can be conducted especially in the placement phase of money laundering. Nevertheless, security trading requires the involvement of a licensed security broker; however, such trading can be carried out on the Internet and by offshore brokers quickly and efficiently. Furthermore, the securities bought can act as security for loans in the loan-back schema for money laundering. In this way, the cycle of money laundering activities closes (eliminating possible suspicions) with the appearance to have only legitimate transfers of money and securities in circulation.

Money Laundering with Electronic Payment Systems

Electronic payment systems are characterized by large diversity in terms of access methods (off-line or on-line), transport methods (access to bank account, to card with electronic chip or to virtual currency account, etc.), charging methods (flat, pay per use, variable fees dependent on volume), and time of the payment settlement (prepaid, post paid, pay now). Differentiation criteria such as access to payment application often determine the other features of a payment system. During payment, the on-line payment systems are characterized by an on-line connection to the system provider who authorizes the transaction. Relevant access data such as passwords as well as currencies are stored on a central server of the system provider. Hence, requests (e.g., for PIN) and answers (authorization) between the participants (client, server of system provider) are exchanged on a real-time basis. In case of off-line procedures, the end devices of users guarantee not only data transportation and authorization, but they often act also as storage medium for currencies. Therefore, the currencies or payment orders flow directly to the receivers without involving the bank or the transaction system of the system provider. Authorization of an off-line transaction is not possible on a real-time basis (only, e.g., at the end of a specified period of time if the turnovers were submitted to the bank (acquirer)), and bears a high risk of fraud. The on-line as well as the off-line payment systems can be distinguished by certain special features that sometimes position the systems against each other in a conflict. These

conflicts are often irresolvable and, hence, determine the character of a payment system as well as its potential use for illicit actions.

Key Features of Electronic Payment Systems

Many empirical studies have shown that the most important reasons for the use of an electronic payment system from the point of view of the end users are its flexibility (e.g., the use of existing end devices for new payment systems), convenience (e.g., an easy entry to the payment system, possibly without registration, as well as quick settlement), and security.[15] Low availability, high transaction costs as well as a nescience in dealing with the electronic payment systems were named as the most important reasons that obstruct the adoption of such systems. High significance is often given to the security of these systems; however, this is rather based on an uncertainty or on nescience than on acknowledgement of the concrete risks and security mechanisms.

The most important reasons for the adoption or the refusal to use electronic payment systems often coincide with the most important reasons to adopt or refuse the use of such systems by the money launderers. Indeed, the money launderer has specific goals of use and strategies (e.g., for disguising the origin of the money); however, the choice of concrete technologies and in this case of a suitable payment system for a money laundering operation often depends on the features supported by an electronic payment system as well as on the knowledge and ease of handling of the system by the money launderers. The money launderer would have to decide on a specific profile of the supported features, taking in consideration the fact that between the features already mentioned irresolvable conflicts exist. And to date no electronic payment system supports even approximately the majority of the desired features by the consumers (or in the narrower sense by the money launderers).

Conflict between Security and Cost Efficiency

High security is guaranteed mainly to centralized on-line payment systems applying many cryptographic mechanisms. Costly mathematical procedures are used for encoding and decoding of data, which should satisfy the well-known requirements of security: confidentiality of the data and transfer; integrity of the data as protection from manipulations (by generating hash sums); authentication of the communication partners on the basis of passwords, PINs, digital signatures, etc.; and non-repudiation, e.g., owing to digital fingerprints. The cryptographic operations are very costly especially in the case of on-line payment systems with high security level since they are based on asymmetric procedures (long keys), with multiple on-line communication generating high costs (for computational costs, on-line connections, storage capacities). Contrary to the on-line procedures, the off-line payment systems, as for example

Millicent, use only the highly cost-effective check sums (hash value) and digital signatures.

Transaction costs represent principal costs in the total cost of a transaction. In general, the electronic payment systems are more efficient than the traditional paper- or account-based payment systems owing to the lower transportation and storage costs (no significant costs for transport or insurance policies, only communication and storage space costs). The settlement costs often vary as a function of the value of a transaction, the risks of non-repudiation as well as the costs for the infrastructure, e.g., for clearing and verification of turnovers by payment system provider (e.g., costs for the card evidence and control centers of the German GeldKarte chip card-based payment system).[16] For the customers, searching costs appear in the form of search efforts for acceptance places, virtual brokers, banks, change agents, etc. For money launderers, these searching costs are often an integral part of the layering phase of money laundering, while money circulates through several accounts, shell companies or offshore centers. Some payment systems also offer certain profit possibilities (besides lower transaction costs), as, for example, virtual gold currencies in case of increasing market prices of gold.

Conflict between Anonymity and Non-Repudiation

Anonymity means secrecy of customer identity as well as hiding of transaction data. The primary purpose of anonymity is protection of customer's private area in order to prevent the creation of customer profile for unauthorized marketing actions. Besides, no relationships/ associations would be possible to be established between customers, traders and related data. As back as in 1987 had David Chaum referred to the possibility of linking computer data of different organizations with the help of certain key data for unauthorized actions and as a response suggested the use of unique digital pseudonyms for each transaction.[17] The idea of Chaum, which is in the form of an anonymous digital signature (the so-called blind signature), was used in an electronic money system known as Ecash (the identification characteristics, as for example the serial number of an electronic coin, are covered with a blinding factor before sending to the issuing bank for digital signing. Perfect anonymity is guaranteed only if the customer does not identify, e.g., by giving information about his physical address for delivery).[18] Other mechanisms—such as dual signatures with SET (the clearing centre as well as the trader gain access only to the data part relevant to them, e.g., the payment information or the order data), special alias number instead of telephone number for mobile payment systems (e.g., Paybox), anonymous prepaid telephone cards or coupon cards (e.g., Paysafecard)—guarantee anonymity of transactions to a large extent. Such anonymous technologies are also used by the money launderers helping them to avoid the identification procedures (e.g. resulting to the "know your cus-

tomer" rule in the banks). Furthermore, other Internet technologies are also used, such as IP-Spoofing (modifying packet headers of Internet messages to make them appear to have originated from a trusted site) or generating anonymous IP by anonymous hosting (also from offshore countries).[19]

Anonymity is supported only by a small number of electronic payment systems. Nearly all electronic payment systems are characterized by extremely short payment circulations (unique coins or transfers), no transferability of the coins or the checks to private persons without the involvement of a bank (protocol and verification of the payment data) and the existence of many identity characteristics (as for example serial number of a coin, bank details, telephone number for a mobile transaction, shadow accounts for cards with electronic chip as for example GeldKarte, etc.). Excluding anonymity is often done in order to maintain consistency of the payment systems in case of unauthorized copying of the electronic coins or checks (the so-called double spending) as well as in case of potential use of such anonymous payment systems for illegal actions such as money laundering, tax evasion, and terrorism financing. For this reason, authentication mechanisms will be adopted for unique customer identification (e.g., PIN for debit cards, transaction random numbers for on-line transfers, telephone number or alias for Paybox and Mpay, digital signatures and fingerprints for Ecash, card and terminal serial numbers for GeldKarte, "passphrase" for e-gold account of e-gold Ltd., etc.) which should guarantee non-repudiation at the same time.

Conflict between Convenience, Mobility, and Security

Convenience for the users of an electronic payment system implies time and location freedom, access possibilities to other integrated applications as for example electronic banking and brokerage, free transferability of the assets between private users as well as an easy and comfortable use, possibly without any registration (physically in the branch, on-line on Internet or WAP).[20] The requirement for convenience is clearly in the interest of money launderers who use, for example, person-to-person transfers primarily in the layering phase. Besides, protocol of transactions and hence traceability would be avoided. Electronic payment systems would rather reach in such cases cash functionality and be suitable, therefore, for terrorist financing.

For money laundering activities, mobility of payments is of great importance as another characteristic bringing convenience. In the ideal case for money laundering, transfers will be carried out trough countries with bank secrecy laws, with allowed anonymous accounts and customer identity protecting policy, generally with the help of notaries and attorneys (most of all during the layering phase). Mobility of payments is predictable considering the international character of e-commerce (e.g., sup-

plier's ordering systems or auctions) and, therefore, meets the requirement of money laundering operations for cross-border transfers.

Many electronic payment systems (e.g., ecash, CyberCoin, SET, Paybox in Germany) have not been accepted by the customers due to insufficient convenience, flexibility, and mobility. Also, in spite of the developed mature security technologies (digital, blind signatures) for confidentiality and authentication of the customer, the systems could not reach the critical mass of customers. Instead, payment methods spread as, for example, transfers and debit procedures per SSL protocol, which does not guarantee non-repudiation of the transaction or authentication of the payer (potential money launderer) (simply the server of the payment provider will be authenticated with appropriate certificates), even though it allows to carry out the transfer fast, easy, and without additional software (only Internet browser) or hardware.

Suitability of Electronic Payment Systems for Money Laundering

Choosing an electronic payment system for illegal activities such as money laundering or terrorist financing depends on many factors as, for example, the duration of the operation, the amount of money to be transferred, the international or local character of the transfer and, furthermore, it also depends on such individual preferences of the money launderers or smugglers as their attitude to new technologies, risk aversion to electronic payment methods, and many others. Therefore, an electronic payment system cannot be analyzed by means of a universal pattern or matrix containing specific features, but rather intuitively and considering the definition of money laundering (concealing or disguising the origin, location, use, nature of assets, etc.). Hence, a number of payment systems were selected for the analysis, which posses such characteristics that make possible to carry out with them international money transfers in a convenient, fast, and flexible way, through anonymous accounts.

Virtual Gold Currencies

Virtual gold currencies (e.g., e-gold, Goldmoney, e-Bullion, AnonymousGold) are account-based electronic payment systems whose value is backed by 100%-golden deposits in a physical form (bullions, bars or specie). The gold reserves are in a private storage of the system provider who often operates from an offshore country (e.g., e-gold Ltd., Nevis Corporation).[21] In the case of gold currencies, only certain weights of gold are booked to accounts of receivers. While the possession of gold reserves changes constantly, the gold in the treasury vault remains untouched.

For exchange or purchase of gold currencies, the user opens an account for a virtual gold currency at a system provider. The identification requirements are negligible in comparison to opening a bank account and are often limited only to a request for information such as name, email address and occasionally physical address to which

then a "verification code" is sent. Furthermore, also a copy of an ID could be required to be faxed or sent. Nevertheless, such verification will be often omitted if, for example, the transactions do not exceed the value of 15,000 euros or $15,000.[22] Structured payments for money laundering or terrorist financing can be made by opening several accounts at a system provider or accounts at many different providers without the need for identification (only the email address). Similar verification obligations are also required by the exchange agents who exchange gold currencies for national currencies worldwide (e.g. Gold-cash.biz informs that in the case of a foundation of an offshore enterprise in Delware no copy of the real ID is required).[23]

Person-to-person transfers between users of virtual gold currencies are allowed (which shows suitability for the layering phase); the transfers are conducted very fast worldwide and with no chargeback risk. For cash withdrawal and the integration phase of money laundering, the special payment cards for Automated Teller Machines (ATM) are very appropriate. Such anonymous ATM cards are often issued by offshore banks without name, addresses or credit investigation (any addressing information is accepted) and can be used worldwide for cash withdrawal from ATM from a gold currency account.[24]

In special cases, the golden bars can be transferred physically to the customer (redemption) or are sent by the customer to the provider also physically (bailment, exchange, e.g., by e-gold).[25] Nevertheless, the exchange of gold mostly occurs against a central bank currency through an exchange agent on the Internet. The new customer pays an amount in national central bank currency on the account of a change agent (on the Internet) who credits an amount on the customer account at a provider of gold currencies (after deduction of a commission). Besides credit cards or bank wire transfers, other payment methods are also accepted by many exchange agents, which are hardly controllable again by the supervisory authorities – cash payment, money or postal transfer orders. Some exchange agents try to avoid possible risks of transfers for money laundering or terrorist financing and determine clear policy for the transfers (e.g., E-forexgold.com accepts no checks and money orders for the purchase of virtual gold currencies. Also the payments directly on the accounts from e-forexgold.com are rejected before confirmation of the payment form. E-forexgold.com stresses thereby its role as exchange agent and not as a trustee or nominee for anonymous transfers. The Paybox customers have to be registered before participation in the system by SSL, sending their bank account details to the system provider. Mpay of Vodafone requires no registration; nevertheless, the customers are identified by the contract with the mobile phone company).

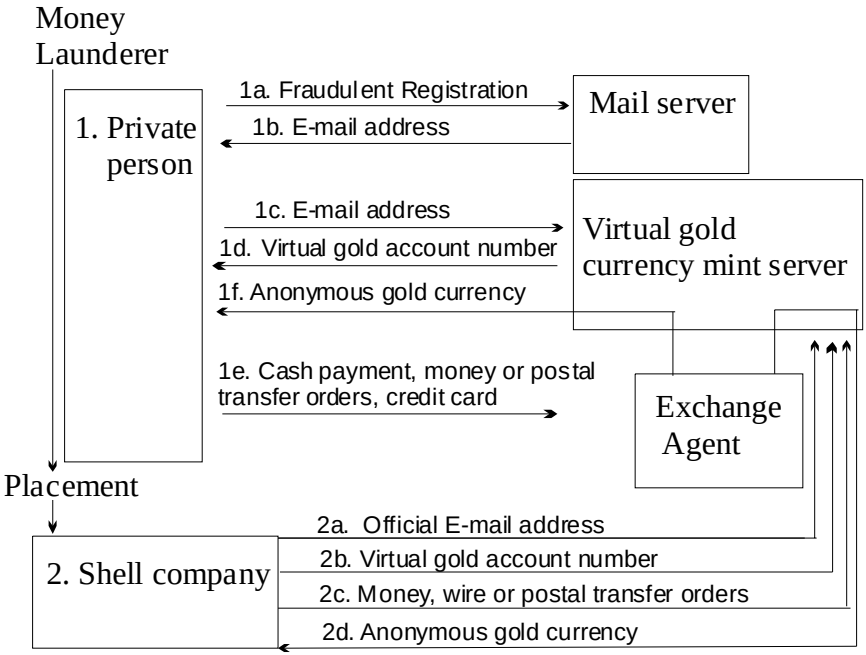

Figure 3: Gold Currencies and Shell Corporations.

The gold currencies can be an attractive electronic payment system for money laundering and terrorist financing taking into consideration their features and their suitability for realization of each phase of money laundering. In the placement phase, the laundered money can be deposited with the help of an exchange agent on the Internet, shell corporations, a trustee or a private transfer system (e.g., Hawala) in form of postal orders, checks, charity payments or payments of other already existing anonymous users of, for example, virtual gold currencies (person-to-person transfers). The network of numerous providers and agents on the Internet creates ideal conditions for the movement of money between private persons and corporations, also from offshore countries (layering phase). Cash withdrawals with the so-called Gold ATM cards, re-exchange with gold currencies and central bank currencies, or paid dividends, e.g., from an e-commerce (business) activity of the money launderer, allows reintegration of the laundered money back into the legal transaction systems (integration).

Prepaid Cards

Prepaid customer smart cards with a rewriteable memory storing electronic currencies are a multipurpose payment instrument that can be used in stationary trade, for person-to-person transfers as well as for e-commerce (using special devices connected to

the computers). Most card products are suitable for money laundering only to a limited extent due to the maximum fixed loading amount for a card (e.g., 200 euros for the GeldKarte) or the account-based character of payments (in this case the customer becomes clearly authenticated). Hence, for terrorist financing the account-unlinked products (with just e-purse functionality) are more attractive; they allow loading of currencies, e.g., in exchange of cash. Example of such a card is the so-called "white GeldKarte" primarily developed for young people without bank account. In spite of the guarantee for perfect anonymity for the users, only approximately 5 to 6 % of all loading processes in the GeldKarte system were conducted with cash.[26] The marginal acceptance of the "white GeldKarte" prevents the wide use of these payment instruments for money laundering since fast increase of transactions with the account-unlinked GeldKarte could immediately trigger a suspicion alert for illegal activities. Nevertheless, in the future such prepaid cards (assuming their wide acceptance) could be used by the money launderers as a possible placement instrument.

Other prepaid cards, such as the coupon card Paysafecard that can be purchased in stationary trade in Austria as anonymous prepaid telephone card, are also suitable for the placement phase of money laundering.[27] With Paysafecard the customer can pay in e-commerce applications for goods or services, while the system provider merely checks the credit balance of the card with the help of the 16-figure PIN (it is printed on the card and is rubbed off by the customer for payments). It would be more difficult to carry out the other money laundering phases, i.e. the layering and the integration phases, because the on-line merchants have to be registered at the system provider and no person-to-person transfers are permitted.

Other prepaid cards with electronic chip, which function as electronic purse, are characterized only by a few features suitable for money laundering – only for a single phase. The transactions are stored by the system provider and can be linked together on the basis of certain identification features such as serial number of payment unities, card number, account number or terminal number. The projects with electronic payment systems are often only of a national character, making them not suitable for international transfers. Nevertheless, to a limited extent, certain characteristics of the electronic payment systems can be used mainly in the layering phase as for example the possibility of person-to-person transfers in the off-line mode with Mondex or interoperability of Proton and VisaCash systems.

Mobile Payment Systems

In general, mobile payment systems are characterized by high flexibility in many application domains (mobile commerce, electronic commerce, stationary trade, as well as for person-to-person transfers) and by high reach-possibility both for customers and on-line suppliers. Other characteristics, such as anonymity and convenience, are

system-specific and often depend closely on the transportation medium used in the system (direct debit or prepaid cards), the charging methods (e.g., telephone bill) or the access methods of the payment application (off-line versus on-line). The on-line and server-based payment systems have payment applications on the server of the system provider and require authentication of the users on a real-time basis. In the off-line systems, the data is stored in the mobile end device (chip card). Therefore, the off-line payment systems are usually not account-based, with prepaid character (payment guarantee for receiver) and anonymous (anonymous prepaid cards; payment occurs when currency units are transferred from the customer prepaid card to the receiver card on a real-time basis as in IrDA, Bluetooth, etc.). The flexibility of mobile cards with stored payment applications guarantees that the cards can be widely exchanged between any different mobile end devices or, in general, between card readers (e.g., dual slot or dual chip end devices).

Nowadays, the off-line mobile payment systems with integrated payment functions in the mobile end devices are supported mainly by many initiatives for development of a universal payment system (e.g., Mobey Forum, Mobile Electronic Transaction). The systems, which are already operating on the market, represent mainly the server-based solution with registered user accounts and with on-line authorization of the transactions.

Furthermore, the on-line payment systems have features that attract the money launderers as for example suitability for cross-border transfers. Paybox has already been implemented in several countries (Austria, Spain, and the Middle East);[28] Simpay plans its first implementation in Belgium, Great Britain, and Spain. Simpay has the highest potential among all mobile payment systems to achieve quickly the critical mass of users and thereby to become target of illegal money activities. The customers of Simpay are identified by their signed contract with a mobile phone company. However, the complex structure of the Simpay chain value with many participants could make difficult a future investigation of money laundering activities. This complex structure is based on the business connections between the Simpay's joint company with Orange, Telefonica Moviles, T-Mobile and Vodafone, the merchants and the new intermediary authority, Mobile Merchant Acquirer (MMA), which can operate after the positive certification by Simpay as a real service provider.[29] The MMA receives the request for payment of the content provider and passes it on through Simpay to the customer. As a response, the payment authorization of Simpay is sent through MMA, after payment confirmation by the customer, to the content provider. The MMA acts as an important administration and contacting center in the Simpay system, which in addition guarantees a high scalability. Account debiting is done through the customer telephone bill (post-paid; theoretically no money laundering risk, only through the involvement of shell companies) or directly by debiting cus-

tomer prepaid card (high risk of money laundering). Later, the wallet function will also be added to the user phone card with several payment options (debit and credit card) which again increases the exchange and disguising combinations for the potential money launderers in the layering phase.

Solutions

The actions/ measures for limiting and combating money laundering can be categorized as organizational, legislative, and technical. The legislative measures include the regulatory measures at national and international level. Many standards and recommendations were already established worldwide for national legislation (e.g., Forty Recommendations of FATF, Risk Management Principles for Electronic Banking of the Basel Committee on Banking supervision), which define the concrete measures against money laundering or for detection of suspicious activities. Nevertheless, the regulatory solutions remain ineffective so far as countries or territories exist without regulation of the money laundering activities. The FATF organization publishes at certain time intervals a list of the not-cooperating countries and territories, which act as a shelter for many criminal networks.[30] The list of the not-cooperating countries is an important indication for the supervisory authorities investigating possible involvement of suspected persons in criminal activities. Unfortunately, the fact that a country is in the list is often only informative and does not limit the dimension of money laundering (shell companies in offshore territories). A regulatory solution for this problem could be an administrative restriction of the economic relations with a non-cooperating country. However, it seems unrealistic that such restrictions or sanctions will be efficient due to the unlimited communication possibilities of the Internet (closing of one location is followed by opening of another location through Internet).

The organizational measures include different methods for testing (checking all transactions that exceed a threshold value) or some calculation methods as for example the net value (worth) measuring the difference between assets and liabilities of a suspected person (its increase has to be a result of legal income), supervision systems (e.g., Suspicious Activity Reports filed by financial institutions in the U.S. and EU), and early warning systems of potential fraud risks according to the risk management methodology.[31] Record keeping of transaction and customer data at the system providers also belongs to the organizational measures and solutions. Traceability of transfers and net traffic often present a significant problem for the supervisory authorities due to the fact that the data of the customers and consequently their privacy are protected by the Internet Service Providers (the ISP can also operate from not-cooperative countries). Other postulated measures against potential money laundering activities, such as setting a maximum loading value for a prepaid card, demand for bank involvement in each transaction (no peer-to-peer transfers) or restriction of the

use to national level (no international payments), are neither realistic (e-Commerce) nor innovative or efficient.

The technical solutions represent the most interesting and, at the same time, efficient part of the solution approaches regarding authentication of users or traceability of transactions, for example. Many technical solutions that could limit money laundering have already been developed:

- Digital signatures and certificates based on the Public Key Infrastructure (PKI) – This is a hierarchical certification technology based on asymmetrical cryptography for authentication, confidentiality and integrity of data, as well as for non-repudiation of electronic transactions. The generation of key pairs and the confidential distribution of public keys with certificates are also important for combating money laundering conducted by means of different electronic payment systems due to the fact that it secures practically a worldwide authentication of the transaction participants (worldwide interoperability).
- Special cryptographic protocols such as for example the off-line payment protocol of Chaum, Fiat and Naor, developed on the basis of the "blind signature" for an anonymous off-line payment procedure. In contrast to the online payment procedures, where the verification processes and payments should be processed between the merchants and banks in real time, the electronic checks and coins are collected in off-line payment protocols by the merchant first and then are submitted in aggregated form at the bank of the merchant in the end of a given period. A fraudulent case (e.g., double spending) enhances enormously the probability of disclosure of customer identity.

Conclusion

Based on the supported features, the gold currencies are often favored for potential application in money laundering. Other electronic payment systems have characteristics attractive to money laundering to a different degree. Being suitable for a single phase of money laundering, a combination of different payment systems would enhance their suitability for the whole money laundering process – prepaid cards for the placement phase, mobile payment systems for the layering phase and virtual gold currencies for the integration phase. The number of possible combinations for illegal activities increases enormously when other traditional techniques are involved (e.g., transfers through Hawala, intermediation of shell companies and nominees or investment in legal financial products). Hence, money laundering is a complex and continuously changing process; however, the dimension of illegal money activities can be limited by suitable measures and approaches (primarily technical solutions) or detected by early warning and supervision systems.

Notes:

[1] "Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering," *Official Journal of the European Communities*, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_344/l_34420011228en00820082.pdf> (05 September 2005).

[2] John Madinger and Sydney A. Zalopany, *Money Laundering. A Guide for Criminal Investigators* (Boca Raton, FL: CRC Press, 1999).

[3] Madinger and Zalopany, *Money Laundering. A Guide for Criminal Investigators*.

[4] Madinger and Zalopany, *Money Laundering. A Guide for Criminal Investigators*.

[5] *Report on Money Laundering and Terrorist Financing Typologies 2004-2005*, FATF-XV (Financial Action Task Force on Money Laundering (FATF), 10 June 2005), <http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf > (05 December 2005).

[6] *2003 National Money Laundering Strategy* (U.S. Treasury: The Office of Terrorism and Financial Intelligence (TFI), 2003), <http://www.treas.gov/offices/enforcement/publications ml2003.pdf> (05 September 2005).

[7] *2003 National Money Laundering Strategy*.

[8] *2003 National Money Laundering Strategy*.

[9] *2003 National Money Laundering Strategy*.

[10] Madinger and Zalopany, *Money Laundering. A Guide for Criminal Investigators*.

[11] Madinger and Zalopany, *Money Laundering. A Guide for Criminal Investigators*.

[12] Madinger and Zalopany, *Money Laundering. A Guide for Criminal Investigators*.

[13] e-gold Ltd. is a Nevis Corp. and the bullion backing the e-metal currencies is held by the e-gold Bullion Reserve Special Purpose Trust in the Iceland of Bermudas, <http://www.e-gold.com/contracts/egold-spt-111899.htm> (05 September 2005).

[14] *Report on Money Laundering and Terrorist Financing Typologies 2003-2004*.

[15] Karl-Heinz Ketterer, *Internet-Zahlungssysteme aus der Sicht der Verbraucher – Ergebnisse einer Online-Umfrage IZV6* (Erhebung des Instituts für Wirtschaftspolitik und Wirtschaftsforschung der Universität Karlsruhe, May 2003), 1-13, <http://www.iww.uni-karlsruhe.de/izv/pdf/izv6_auswertung.pdf> (14 July 2004).

[16] Eberhard Stickel and Krzysztof Woda, "Electronic Money," in *E-Finance*, ed. Erhard Petzel (Hrsg.) (Gabler Verlag, 2005), 831-860.

[17] David Chaum, "Sicherheit ohne Identifizierung: Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen - Zur Diskussion gestellt," *Informatik-Spektrum* 10, no. 5 (1987): 262-277.

[18] Chaum, "Sicherheit ohne Identifizierung: Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen."

[19] Anonymous hosting (e.g. <http://www.katzglobal.com/hosting/hosting.html> (05 September 2005)).

[20] Susanne Leist and Krzysztof Woda, "Analyse der Erfolgsfaktoren mobiler Zahlungssysteme," (Frankfurt (Oder): Europa-Universität Viadrina, Arbeitsbericht Nr. 217, July 2004), 1-23.

[21] e-gold, "What is e-gold?" <http://www.e-gold.com/unsecure/qanda.html> (05 September 2005).

[22] Gold-cash.biz., FAQ, <http://www.gold-cash.biz/faq.php> (05 September 2005).

[23] Gold-cash.biz., FAQ.

[24] Gold-ATM, Debit and Prepaid Cards for Digital Currencies Users, <http://www.gold-atm.biz/cards.php> (05 September 2005).

[25] e.gold, "e-gold Account User Agreement," (last modified on 20th December 2003), <http://www.e-gold.com/unsecure/terms.htm> (05 September 2005).

[26] Stickel and Woda, "Electronic Money."

[27] Stickel and Woda, "Electronic Money."

[28] Paybox Austria AG, FAQ, <http://www.paybox.at/238.php#> (05 September 2005).

[29] Simpay, FAQ's, <http://www.simpay.com/faqs.php> (05 September 2005).

[30] The Financial Action Task Force on Money Laundering (FATF), "Annual Review of Non-Cooperative Countries or Territories," 2 July 2004, <http://www.fatf-gafi.org/dataoecd/3/52/33922473.PDF> (05 September 2005).

[31] *2003 National Money Laundering Strategy*.

KRZYSZTOF WODA received his Ph.D. degree in Economics from the Viadrina University in Frankfurt (Oder), Germany, in 2003. His current research area interests include modern techniques for money laundering and terrorism financing, the role of electronic payment systems in supporting illicit money transfers as well as the development of quantitative methods for detecting illicit money transfers and financial computer crime. *Address for Correspondence*: Dept. of Information Systems, Viadrina University, Postfach 1786, 15207 Frankfurt (Oder), Germany; *E-mail*: kwoda@euv-frankfurt-o.de