IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITB12639

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Money Laundering Using Electronic Payment Systems

Juergen Seitz, Department of Business Information Systems, University of Cooperative Education Heidenheim, Schmelzofenvorstadt 33, 89520 Heidenheim, Germany, P +49 7321 38-1906, F: +49 7321 38-1915, seitz@ba-heidenheim.de

Krzysztof Woda, Department of Business Information Systems, European University Viadrina, August-Bebel-Strasse 12, 15234 Frankfurt (Oder), Germany, P +49 335 5534-2927, F +49 335 5534-2357, kwoda@euv-frankfurt-o.de

ABSTRACT

Electronic payment systems are not only an appropriate medium of exchange on electronic markets. They can also make easier illicit dealing, among them money laundering. The purpose of this article is the identification of key features for money laundering transactions and an analysis of potential attractions and the suitability of single payment systems for money laundering. The article concludes with an overview on possible measures against money laundering and a short summary and a short summary.

IMPACTS AND PHASES OF MONEY LAUNDERING IN E- AND M-COMMERCE

Money laundering in the definition of the European Parliament and the Council of the European Union means intentional committed actions whose purposes consist in concealing or disguising "the true nature, source, location, disposition, movement, rights with respect to, or ownership of property" (Directive 2001/97/EC of the European Parliament and of the Council, Art. 1 (C)). The properties themselves are derived from criminal activity or from an act of participation in such activity. The committed actions must have been done in knowledge of the fact such of the illicit origin. The conversion, exchange, transfer, transport, acquisition, possession or use of assets for the purposes of concealing their illicit origin belong to these illegal committed actions in terms of § 1 (C) of the Directive 2001/97/EC (also in § 1956 Money Laundering of USA Patriot Act). The regulations of the US complement an other purpose of concealing or disguising of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity or avoiding a transaction reporting requirement under State or Federal law [§ 1956 (a) (1) (B), USA Patriot Act]. Properties are each kind of assets, tangibles and intangibles that can fulfill the functions of an exchange medium and storage of purchasing power (e. g., gold and paper money).

The concealment or disguise of the origin, location, nature etc. of property takes place as a result of a complicated and multistage process that can consist of a lot of single transactions. The transactions can be furthermore carried out by credit and financial institutions supported by transaction systems for international payments (e. g., Target, SWIFT). The illicit assets are legalized within the scope of money laundering by a process that consists of three main phases: (Madinger, Zalopany (1999)).

- **Placement:** Assets from illicit dealings are converted in this phase into other forms of properties to allow their investment or movement in legal properties. Examples are deposits, checks, prepaid cards with electronic chips, gold, virtual currencies and securities instead of cash.
- **Layering:** It will be tried by a set of transfers of assets between accounts of different financial institutions and other economic subjects to cover up the identity of the true owner or the money launderer. The determination of the origin of the property becomes more and more difficult and expensive on accounts of numerous transfers. Besides, different legal restrictions, like the transaction reporting obligation for transaction amounts higher than a legally defined amount (e. g. money changes, owner of foreign bank accounts), are avoided by the money launderers.
- **Integration:** Legal as well as illicit properties are combined with each other and integrated into the economic cycle. These already inseparably booked properties will often hand over back to the owner—now, nevertheless, as legalized properties—e. g., in form of paid back loans or paid claims of falsified invoices for goods deliveries or services which have never been performed.

It is crucial for the assessment of money laundering to consider the consequences of such deals for the participants of an economic cycle. The conversion of illegally acquired properties into the financial and economic system exposes such transaction systems to many risks. The potential losses result from money laundering transactions, which are carried out e. g., with sight deposits generate operational and legal risks for banks, if the affected bank cannot satisfy their liabilities or cannot fulfill the liquidity principles (Basel Committee on Banking Supervision (1998)). Farther risks arise, e. g., the reputational risk, that results in a potential trust loss for the bank and the whole financial system. Money laundering is often connected with tax evasion, corruption (e. g., of bank employees), terrorism financing as well as increased crime that can result on the basis of integrated assets from money laundering (Department of Justice Canada (1998); FATF (2004)). Also other properties, like securities (e. g., life insurance policies), which arouse the interest of money launderer, can lead their legal offerer to the collapse or jeopardize their financial stability.

The dimensions of potential risks for a provider of properties suitable for the money laundering depend on several factors like the easy access to the assets, the complexity of potential investments, the suitability for international transfers. (FATF (2004)). The more complex and advanced products on the one hand are and the greater their international mobility on the other hand is, the more difficult is the detection of illicit dealing and simpler at the same time is the integration of the property from the money laundering in existing financial systems. The factors that are crucial on the suitability of a property for the money laundering are to be defined in relation to electronic marketplaces (E- and M-Commerce) anew.

ELECTRONIC AND MOBILE PAYMENT SYSTEMS—CRUCIAL FEATURES FOR MONEY LAUNDERING

Electronic payment systems for electronic and mobile commerce can be used as potential properties for money laundering as well as a medium of exchange in a phase of the money laundering process (e. g., layering) (Escher, et all (1999)). Nevertheless, the suitability of e-payment as a property potentially used for money laundering is limited in comparison to other assets with distinctive long-term maintenance of value like gold, diamonds, life insurances, and stocks. Also, some system specific

qualities, like time-limited certificates and restrictions like maximum amount limits per transaction (e. g., 200 Euro for GeldKarte, 10 Euro for m-pay or simpay), recording of transactions (shadow accounts, e. g., GeldKarte) and serial number archiving or connections with the bank checking account with direct debit procedure (e. g., paybox) are responsible for the limited suitability of electronic payment systems as a property used in money laundering. Such restrictions authenticate the committer clearly and therefore limit the dimension of illicit money laundering transactions. Hence, electronic payment systems can be used rather as an exchange medium for money laundering transactions for concealing or disguising the origin or the transaction operations efficiently.

An essential problem is the traceability of transaction streams in open networks like the Internet, that itself exists as a decentralized meshed communication network without controlling authorities. Transactions can be carried out internationally also in countries which do not cooperate with organizations for combating money laundering.

Electronic payment systems enclose the electronic transfer of money with different payment instruments (smart card, software for electronic money, mobile devices, debit and credit cards) and through several infrastructures from the payer to the recipient (EZB (2003)). Electronic and mobile payment systems differ in access methods on accounts (on-line versus off-line), the purpose of use (business-to-business, consumer-to-business, person-to-person), billing methods (prepaid, post-paid, pay now) and transaction costs (macropayments and micropayments) (McKitterick, Dowling (2003)).

Some payment systems distinguish themselves by certain qualities, e. g. anonymity, that can be for the suitability of such payment systems for the money laundering of particular importance (Stickel, Woda (2005)).

Analysis of the money laundering risk in selected electronic money schemes

For the analysis of the money laundering risk some electronic payment systems are selected that allow a quick, convenient and also cost-effective realization of money laundering transactions. The suitability of the single payment system for money laundering will be assessed referring to different phases of a money laundering process.

Traditional Payment Methods: Credit Cards, Debit Cards and Online Money Transfers

There are a lot of examples demonstrating how the traditional payment methods could be exploited by money launderers. Structured cash payments (the transferred amounts are below the known value with mandatory reporting) are a typical representative of the uncomplicated order of illicit money placing (see FATF (2004)). Payments with credit cards will not often carried out by their owner directly but on behalf of his name. Then the primary owner opens merely a bank account at a loan institute or orders directly a credit card. Within the on-line money transfer system large amounts can also be transferred fast by bank transfer to foreign payees. In interbank payments by SWIFT, messages about payments are exchanged. Nevertheless, they need not contain the data of the origin of a payment and the payer. Indeed, there exists a form text field about the originator of payment, its completion remains voluntary (FATF (2001)). Only the payee is identified clearly in the SWIFT system.

Traditional payment methods are rather unattractive for money laundering because of some specific qualities. The transactions are not anonymous and often account-based that requires the archiving of the transaction data and provides a good traceability. The payment amounts are not transferable between private customers directly and may be spent with an appointed dealer only. The transaction costs vary as a function of the transaction value and the fees and charges policy of the issuer of a card strongly. Also with regard to the flexibility these payment instruments are not interesting for the money laundering, because they require a registration and verification by opening a bank account. In comparison with other traditional payment methods the credit cards can be distinguished regarding the mobility or worldwide acceptance of that payment method. Only a theft and abusive use of a credit card would be interesting for criminal money laundering activities with the credit card on the Internet.

Also money transfer orders can pass several accounts at different banks and in that way be laundered quickly. Due to the obligation to report and the archiving of transactions such money transfers are only practicable using banks in offshore countries in order to launder money without consequences like criminal proceedings. The transfer of transactions through countries that do not cooperate on combating money laundering bear a risk for potential committers, because such transactions are eyed automatically of other national authorities and bank supervision authorities.

Nevertheless, the traditional payment methods can be used together with other money laundering activities successfully. Charity organizations can be founded, for instance, by terrorist organizations or money laundering committers to collect the money through the Internet (U.S. Treasury, (2003)). In such cases traditional electronic payment systems are suited merely for the layering phase of the money laundering process. Summarizing, electronic payment instruments are interesting for money laundering only in very small number of cases (e. g., structured cash payments, card transactions on behalf of the true card owner, etc.) because of the accounted character of the payments.

Mobile Payment Systems

Mobile payment systems distinguish themselves in general by their high flexibility with application possibilities and by high reachability of the customers as well as of the on-line providers. Other qualities, as for example anonymity, security, transaction costs efficiency or convenience are specific for system and often depend tightly on the transport medium used in a system for transferring the payment units (credit cards and prepaid cards), as well as on the account methods (flat rate versus fees dependent on volume or time) (McKitterick, Dowling (2003)).

For the potential use of mobile payment systems for money laundering is the differentiation between server-based and local mobile payment applications of great importance. In case of server-based payment systems the payment applications are located on a server of the system provider which requires an on-line connection and thereby in each case an authenticity check for every transaction. In local systems working in the off-line mode the data is often sent in aggregated form for the clearing and verification process to the system provider at the end of a predefined commercial period. Then the data is stored on a storage medium integrated in the mobile end device locally. While server-based payment systems carry out a strict customer and bank account authentication, the local payment systems are often not linked with bank accounts, instead, they are equipped with a prepaid function (payment guarantee for merchants). The integration of the payment function directly in the mobile end device (anonymous prepaid cards) can guarantee to the users in certain cases the unlimited anonymity, because the payer who is not bound by a contract to a bank or mobile service provider could not be identified (only with the help of the IMSI number for a phone). And the flexibility secures that the cards with stored payment applications can be exchanged between different mobile end devices or in general between readers unrestricted (e. g., in dual slot or dual chip end devices). The systems already operating at the market represent particularly the server-based solution with registered user accounts and often with the on-line authorization of the transactions.

Mobile payment systems operating today are rather inappropriate for the money laundering because of their central server-based character with definite identification and registration requirements for the customers. The international character of payment systems, high flexibility of application possibilities (also person-to-person transfers) as well as the direct payment opportunities by local prepaid cards increase, together with an enormous mobility of the users, the suitability of mobile payment systems for potential money laundering in the future.

Electronic Money—Network-Based Money Systems

Electronic money is a prepaid holder based payment instrument for payments in electronic commerce, in stationary trading and for person-

to-person money transfers. The customer's bank account will not be directly debited during or after the transaction like in "access products" (debit cards) in the way of transferring sight deposits by a bank. Instead, the prepaid money stored on a medium belonging to the customer (previously uploaded from a bank account) will be transferred during the payment from one bearer instrument (customer's wallet) to another (e. g., merchant's wallet). The European Parliament and the European Council distinguish in their definition of electronic money (Directive 2000 /46/EC) three functional aspects: the storage function (on a customer data storage medium), the redeemability function always to the nominal value (the possibility for an user to re-convert the electronic money in central bank money as a necessary condition for ensuring customer confidence in electronic money, (see European Commission (2004)) and the multipurpose function of electronic money (open payment systems).

In the USA the electronic money is not a subject to so restrictive regulations like in the EU. The American Uniform Money Services Act (UMSA) corresponding to the European directive 2000/46/EC has no duty character but rather a recommendation character for the legislation in the U.S. federal states (Ramasastry (2001)). Hence, the issue and redemption of electronic money is not only limited to the financial institutes as in the EU and therefore is not subject to the central bank supervision. In the USA the so-called MSB (Money services businesses) institutes may issue electronic money, but no redeemability has been guaranteed. Thus electronic money could be also exchanged for prepaid coupons or for other purchase items.

The suitability of electronic money for the money laundering is questionable. In general, Ecash guaranteed the perfect anonymity of payments for their users. Other systems require the registration or the certification of users to the system provider or directly to the merchant. Coins have often a unique character and cannot be transferred to private persons without involvement of a bank authority (extremely short payment cycles). Also the submitted coins may not be used by merchants for further transactions, but they have to be exchanged at the issuer for new valid coins first. The coins can also not be stored, because they have a very limited period of validity to limit the time and effort of the verification process. Therefore, the present and previous network based payment systems pose only a small suitable payment instrument for money laundering.

Prepaid Money Cards

Prepaid customer smart cards, where the electronic value is stored on and are used as a general and multipurpose payment system, are summarized to card based electronic money. Nowadays, card based money is the only widespread form of electronic money and can be used in stationary trade, for person-to-person transfers as well as for electronic commerce (using special card readers). Prepaid cards differ enormously regarding to their characteristic attributes. The properties interesting for potential money laundering like anonymity, international operability etc. are mostly represented individually in case of a each payment system.

Prepaid cards that can be purchased in stationary trading companies are suited for the placement phase of the money laundering. With prepaid cards the customer can pay in electronic commerce for goods or services, because the system provider checks merely the credit balance of the card with the help of PIN that is printed on the card and is rubbed off by the customer. More difficult will be the realization of the further money laundering phases, i.e. the layering and the integration phase, because the merchants must be registered at the system provider and no person-to-person transfers will be admitted. Nevertheless, also in this case techniques, like money laundering by charity organizations, foundations, online casinos or payment for pseudo-consultation services is a proven method for the integration of successfully placed money.

In connection with terrorism financing the aspect of the transferability of such loaded cards on third parties is also important. The unaccounted cards can be purchased in bulk and be transferred to a third party. Many card projects support the multi-currency function and are suited for international operations.

MEASURES AGAINST MONEY LAUNDERING

A lot of international organizations, as for example the Financial Action Task Force on Money Laundering (FATF), the Basel Committee on Banking Supervision (BCBS) and institutions like the European Commission etc. which have worked out different regulations, recommendations and standards, e. g., 40 FATF Recommendations as an international standard, for national supervisory authorities and economic subjects, e. g., financial institutions, that deal with combating of the international money laundering. Such regulations concern national legislation (Directive 2001/97/EC of the European Parliament and the Council or Section 311 of the USA PATRIOT Act), as well as bank-usual practices especially with customers, e. g., know your customer policy. Nevertheless, they should be considered only as a minimum standard for combating money laundering at a international level and under inclusion of electronic markets. Such measures can be implemented directly by the system provider without waiting for suitable regulations.

A large number of national supervisory authorities see no danger of money laundering in newer electronic payment systems if the following measures are undertaken (Committee on Payment and Settlement Systems, (2004)):

- Smart cards or wallets may be uploaded only up to a certain value (e. g., GeldKarte up to 200 euros).
- Payment systems are accounted and require the involvement of a bank in each transaction (no person-to-person transfers).
- Recording of all transactions.
- Restriction of the application possibilities on a national level (no cross-border transfers).

Such measures are often neither realistic (e. g., restriction on national use) nor innovative (accounted smart cards) and contradict the idea of efficient (e. g., off-line payment systems), secure, interoperable and the private sphere of a customer respecting payment system. Rather technically adequate solutions should be introduced which allow protecting the customer's authentication internationally and carrying out the transaction also in the off-line mode efficiently. Such a technical solution arranges the unique certification of users of payment systems by a trust center that guarantees the non-repudiation of transactions worldwide. The certificates may be stored after the successful registration already today in many payment instruments (prepaid cards) and software wallets. The trust centers can be identified mutually on the basis of their certificates and their own certification can be undertaken by suitable national authorities (roots). Up to now, certification systems represent rather isolated solutions. However, they can be integrated relatively fast into a complete certification infrastructure. This is the consequence of the hierarchical construction principle of certification with asymmetrical cryptographical methods. The introduction of the certification and thereby of the digital signature as a functional part of electronic payment systems will create not only the non-repudiation of transaction, but also international interoperability and verification possibilities of transactions that will be again an efficient measure against the international money laundering on electronic markets.

REFERENCES

Basel Committee on Banking Supervision (BCBS) (1998). Risk Management for Electronic Banking and Electronic Money Activities. Received January 3rd, 2006 from http://www.bis.org/publ/bcbs35.pdf.

Basel Committee on Banking Supervision (BCBS) (2003). Initiatives by the BCBS, IAIS and IOSCO to combat money laundering and the financing of terrorism. Received January 3rd, 2006 http://www.bis.org/publ/joint05.pdf.

Committee on Payment and Settlement Systems (CPSS) (2004). Survey of developments in electronic money and internet and mobile payments. Received January 3rd, 2006 from http://www.bis.org/publ/cpss62.pdf.

Department of Justice Canada, Solicitor General Canada (1998). Electronic Money Laundering: An Environmental Scan, October

1998. Received January 3rd, 2006 from http://ww2.psepc-sppcc.gc.ca/publications/crim_jus/money_laundering_e.asp.

Escher, et al. (1999). Aktuelle Rechtsfragen bei Zahlungen im Internet. Received January 3rd, 2006 from http://www.gassner.de/escher/zvi.html.

Europäische Zentralbank (EZB) (2003). Elektronisierung des Zahlungsverkehrs in Europa. Monatsbericht Mai 2003, S. 65-78.

European Commission (2004). Application of the E-money Directive to mobile operators, Consultation papers of DG Internal Market. Received January 3rd, 2006 from http://europa.eu.int/comm/internal_market/bank/docs/e-money/2004-05-consultation_en.pdf.

Financial Action Task Force on Money Laundering (FATF) (2001). FATF-XII Report on Money Laundering Typologies 2000-2001. Received January 3rd, 2006 from http://www.fatf-gafi.org/dataoecd/29/36/34038090.pdf.

Financial Action Task Force on Money Laundering (FATF) (2004). Report on Money Laundering Typologies, 2003-2004. Received January 3rd, 2006 from http://www.fatf-gafi.org/dataoecd/19/11/33624379.pdf.

Madinger, J. & Zalopany, S. A. (1999). Money Laundering: a guide for criminal investigators. Boca Raton: CRC Press LLC.

McKitterick, D. & Dowling, J. (2003). State of the Art Review of Mobile Payment Technology. The University of Dublin, Trinity College, Technical Report. Received January 3rd, 2006 from http://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-24.pdf.

Ramasastry, A. (2001). E-Money Regulation in the United States. In: Electronic Payment Systems Observatory- Newsletter, ePSO-Newsletter, No. 11, December 2001. Received January 3rd, 2006 from http://epso.jrc.es/newsletter/vol11/7.html.

Stickel, E. & Woda, K., (2005). Electronic Money. In: Petzel, E. (Ed.). E-Finance. Technologien, Strategien und Geschäftsmodelle - Mit Praxisbeispielen. Wiesbaden: Gabler Verlag.

U. S. Treasury (2003). The 2003 National Money Laundering Strategy. Received January 3rd, 2006 from http://www.treas.gov/offices/enforcement/publications/ml2003.pdf.