
# Financial Action Task Force

## Groupe d'action financière

## REPORT ON NEW PAYMENT METHODS

13 OCTOBER 2006

# Executive Summary

New and innovative methods for electronic cross-border funds transfer are emerging globally. These new payment tools include extensions of established payment systems as well as new payment methods that are substantially different from traditional transactions. New payment methods raise concerns about money laundering and terrorist financing because criminals can adjust quickly to exploit new opportunities.

The present study analyzes prepaid cards; Internet payment systems; mobile payments; and digital precious metals in order to: (1) Identify trends in the adoption of new payment technologies; (2) Assess money laundering (ML) and terrorist financing (TF) vulnerabilities; and (3) Determine whether the Financial Action Task Force (FATF) Forty Recommendations and Nine Special Recommendations (40 + 9) adequately address any potential vulnerabilities.

The study found there is a legitimate market demand served by each of the payment methods analysed, yet potential money laundering and terrorist financing vulnerabilities do exist. Specifically, offshore providers of new payment methods may pose additional money laundering and terrorist financing risks compared with service providers operating within a jurisdiction.

While it is believed that the FATF 40 + 9 provide the appropriate guidance to address the vulnerabilities associated with these new methods of payment, the study does suggest further examination of the effect these evolving technologies may have on cross-border and domestic regulatory frameworks in order to ensure their compatibility with the FATF 40 + 9.

# Table of Contents

# 1. Introduction

Payment innovations that use the Internet, wireless devices, and even well-established payment networks are appearing globally. Both domestic and offshore service providers may offer these new payment methods (NPMs). While a few NPMs operate or are used in multiple countries or even globally, most are limited in their operational reach or use to specific geographic markets or for specific types of transactions involving the purchase of goods and services. Some NPMs also support domestic, and in some instances, cross-border fund transfers between individuals.

The present study analyzes prepaid, cards; Internet payment systems; mobile payments; and digital precious metals to: (1) Identify trends in the adoption of new technologies; (2) Assess actual money laundering (ML) and terrorist financing (TF) vulnerabilities; and (3) Determine whether the Financial Action Task Force (FATF) Forty Recommendations and Nine Special Recommendations (40 + 9) address any vulnerabilities identified.

This report updates a review of NPMs that FATF members conducted in 1996-1997.[1] Most of the specific payment tools described in this report were not yet in use when the previous FATF study was conducted, which was at the dawning of the Internet era. Accordingly, the previous FATF study of new payment methods concluded: "It is premature to consider prescriptive solutions to theoretical problems."[2] Many of the concerns of ten years ago, however, no longer appear to be theoretical.

More recently, in the FATF 2004-2005 Typologies Exercise, participants re-examined new payment methods as part of the Alternative Remittance Systems (ARS) typologies project.[3] The ARS report stated: "[T]his study very briefly touches on the issue of new payment methods including e-money. Although many of these systems might also be included in the term *alternative remittance systems*, their characteristics are so atypical that they would almost deserve a separate study." Some of the tools and techniques identified in that report are considered in more depth in this study.

The research underlying this report began with a questionnaire that attempted to identify the new payment methods appearing around the world and to estimate market size; how or if those payment tools were subject to regulation, supervision, or licensing; whether there was evidence of ML or TF activity associated with those new payment methods; and whether there were relevant law enforcement cases. Thirty-eight jurisdictions responded to the questionnaire.

The results of the questionnaire show in general that it is not always easy to identify new payment methods (NPM). As a consequence, these results may not mirror the real supply of NPM around the world, but only the perceived supply in the jurisdictions which have provided responses to the questionnaire. The periodic surveys of NPMs conducted by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements (BIS)[4] are a useful complement to this report. However, these surveys on developments in

---

[1] The first formal FATF study of the emerging payment methods discussed in this report is found in the 1996-1997 Report on Money Laundering Typologies, February 1997, Section V and Annex 1. See http://www.fatf-gafi.org/findDocument/0,2350,en_32250379_32237235_1_32247552_1_1_1,00.html.

[2] February 1997 Typologies Report, p. 14. These conclusions were subsequently updated and generally re-endorsed in two later annual FATF typologies reports of 10 February 1999 and 1 February 2001.

[3] 10 June 2005, section I, see http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf

[4] The CPSS, under the auspices of the BIS, regularly publishes reports analyzing developments in domestic and cross-border payment, clearing, and settlement systems. See "Survey of developments in electronic money and internet and mobile payments," CPSS publications no. 62, March 2004, at http: www.bis.org/publ/cpss62.htm. For the most recent statistical information on payments and settlement systems (including certain NPMs), see CPSS, "Statistics on payment and settlement systems in selected countries—Figures for 2004," BIS, CPSS #74, March 2006, at http://www.bis.org/publ/cpss74.htm.

payments market do not focus on anti-money laundering (AML) or countering the financing of terrorism (CFT) as they apply to NPMs, which is the purpose of this study.[5]

The project team, which included representatives from Asia, the European Union member countries, and the United States, conducted additional primary research by consulting public and private sector experts. At the 2005-2006 Typologies Experts Meeting on ML and TF in Rio de Janeiro, the project team heard Mr. Joshua Peirez of MasterCard and Mr. Allen Love of PayPal describe their respective company's payment tools and markets; Mr. Vicente S. Aquino, Executive Director of the Philippines' Anti-Money Laundering Council Secretariat, described that nation's mobile payment systems; and Ms. Sheri Dunlop of the United States Secret Service presented a ML case study involving the use of digital precious metals. At other times, core project team members met with representatives from Visa and American Express and prepaid card program management firms in the United States.[6] Finally, project team members reviewed a variety of related media articles and public sector reports.

This report reflects the contributions of payment system and anti-money laundering and regulatory experts from a variety of countries. In many cases, the definitions and terminology used to describe similar payments systems or payments activities vary from country to country. To provide clarity and consistency within this report, the members of the working group have chosen to adopt, as much as practical, the terms and definitions applied to payments systems by the CPSS.[7] Whenever the terms or definitions used in this report diverge from this source, the variation is highlighted and explained.

The report is divided into six sections. Sections 1 and 2 provide an executive summary and a brief introduction. Section three describes how the new payment methods addressed in this study operate and are used.[8] Section four introduces a ML and TF risk matrix developed by the project team to assess the potential ML/TF risk of each NPM in this study. Section five addresses how the FATF Forty Recommendations and Nine Special Recommendations apply to NPM, and presents selected jurisdictional regulations. Section six summarizes the 38 responses to the FATF NPM questionnaire prepared by the project team.[9] Section seven offers conclusions and highlights areas for further consideration by the FATF.

# 2. Background

How payment system innovations emerge is associated with a number of factors specific to each country, including the underlying economic environment, technology, preferences, actual and perceived costs, along with regulations, policies, and practices of government and private entities with significant influence on the payments system. The fundamental trend, however, across all nations is the migration from paper to electronic payments.

Moving away from paper payments to standardized electronic transaction processing has had the effect of breaking down the payment system into distinct business segments. Hardware, software, communications lines, systems management, accounting, marketing, and distribution have all emerged as distinct business lines for distinct payment services. This segmentation, and the specialization that has resulted, has led to the entry of

---

[5] Another reliable source of information about the development and the state of the market of NPM's is the website of the electronic payment systems observatory (ePSO), managed by the European Central Bank: www.e-pso.info.

[6] NetSpend, Green Dot, and Wild Card Systems (now eFunds).

[7] See CPSS, "A Glossary of terms used in payments and settlement systems," BIS, March 2003, at http://www.bis.org/publ/cpss00b.htm.

[8] A detailed presentation of traditional credit and debit payment methods (on which most new payment methods are based) is contained in Appendix A.

[9] A detailed summary of the questionnaire responses can be found at Appendix B.

nonbanks as both outsourced service providers to the banking industry and sometimes competitors in the market for clearing services.[10]

While banks remain the core providers to end-users for most retail payment instruments and services, payment applications are now available from a wider range of service providers. The move from paper to electronic transactions has enabled non-bank service providers to customize their payment instruments and to package them with complementary products in order to serve niche markets.

Nonbanks now serve as Internet payment portals, transferring payments between payers, payees and their account-holding institutions. Nonbank intermediaries also transfer payments between buyers and sellers who transact through Internet retail storefronts and through online auction sites. Nonbanks, in fact, pervade the payments industry, processing transactions, maintaining databases, and even operating as value providers in e-money schemes. The result is that "the line between the direct provision of retail payment services to end users by non-banks and the provision of related support services to users and payment providers is much less clear than in the past."[11]

## Traditional and Non-traditional Retail Payments

Traditional retail payments are generally low-value, consumer payments that do not require immediate settlement.[12] Traditional electronic payments include bank payment products and services and money transfers that are carried out through nonbank intermediaries such as Western Union, which generally work as credit transfers but do not rely directly upon the transfer of funds between bank accounts.

The FATF defines a money or value transfer system as a "financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money/value transfer system belongs."[13]

Supplementing these traditional retail payments are newer, innovative payment products, or non-traditional retail payments. For the purposes of this report, we refer to these types of payments as "new payment methods", although they are also often referred to as "e-money" by international payments system experts. NPMs include a variety of innovative products that involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems. NPMs also include products that do not rely on traditional payment systems to transfer value between individuals or organizations.[14] This report considers the following NPMs: prepaid cards, electronic purses, mobile payments, Internet payment services, and digital precious metals. Table 1 below provides for a schematic distinction, amongst NPMs, between those that are an extension of traditional payment instruments and those which are *strictu senso* new payment methods.

---

[10] Clearing and Settlement Arrangements for Retail Payments in Selected Countries, Committee on Payment and Settlement Systems, Bank for International Settlements, September 2000 (CPSS #40)

[11] Policy Issues for Central Banks In Retail Payments, Committee on Payment and Settlement Systems, Bank for International Settlements, March 2003 (CPSS #52)

[12]Paper non-cash retail payment instruments include checks, demand drafts, cashiers checks, money orders, traveler's checks, and other related bank drafts. Electronic non-cash retail payment instruments include credit and debit cards as well as credit transfers and direct debits completed through systems such as an automated clearinghouse (ACH). See Appendix A for detailed descriptions of traditional debit and credit card systems.

[13] Interpretative Note to FATF Special Recommendation VI: Alternative Remittance, February 2003.

[14] For the purposes of this study, we have excluded from consideration any non-traditional means of clearing and settling paper check payments or bank drafts through the use of electronic information or electronic check images, including their conversion to electronic funds transfers via ACH systems.

## *New Payment Methods (NPM)*

| Extensions of traditional retail electronic payment systems | New non-traditional retail electronic payment systems |
|---|---|
| Prepaid payment cards | Electronic purse |
| Internet payments based on bank accounts[15] *(not covered in this report)* | Internet payments not based directly on a bank account |
| Mobile payments based on bank accounts | Mobile payments not based directly on a bank account |
| | Digital precious metals |

**Table 1**

### Prepaid cards

Prepaid payment cards provide access to monetary funds that are paid in advance by the cardholder. While there are many different types of prepaid cards that are used in a variety of ways, they typically operate in the same way as a debit card and ultimately rely on access to an account. There may be an account for each card that is issued or, alternatively, there may be a pooled account that holds the funds prepaid for all cards issued. The cards may be issued by, and accounts may be held at, a depository institution or a non-bank organization; pooled accounts would be normally held by the issuer at a bank.

Prepaid cards can be issued for limited or multiple purposes. Limited-purpose or *closed system* prepaid cards can be used for only a limited number of well-defined purposes and their use is often restricted to specific points of sale or for specific services. Examples include merchant-issued gift cards, prepaid long distance service, and mass transmit system cards. These cards may either be limited to the initial value posted to the card (non-reloadable) or may allow the card holder to add value (up to a certain limit) and reuse the card (reloadable). The issuer of the card or its service provider typically operates the network on which the cards can be used. The value on the cards generally is linked to a prepaid account established by the issuer or service provider. Transactions are processed in a similar fashion to transactions involving debit or credit cards.

Multipurpose or *open-system* prepaid cards can be used across a broader range of locations for a wider range of purposes. Such cards may be used on a national or international scale but may sometimes be restricted to a certain geographical area. Multipurpose cards may be used by the person who purchased the card or by someone else. Examples include payroll cards and general purpose "cash cards" for individuals without bank accounts or a credit card. These cards are usually associated with a card payment network, such as Visa or MasterCard, which permits them to be used in the same manner as a debit card to make purchases or to get cash from an automated teller machine (ATM). Some issuers do not require the cardholder to have a depository account. These cards are distributed by merchants, depository financial institutions, and money/value transfer (MVT) systems for a variety of purposes. Most are reloadable.

[15] The expression "bank account" used in this box refers to accounts held at financial institutions that are subject to AML requirements.

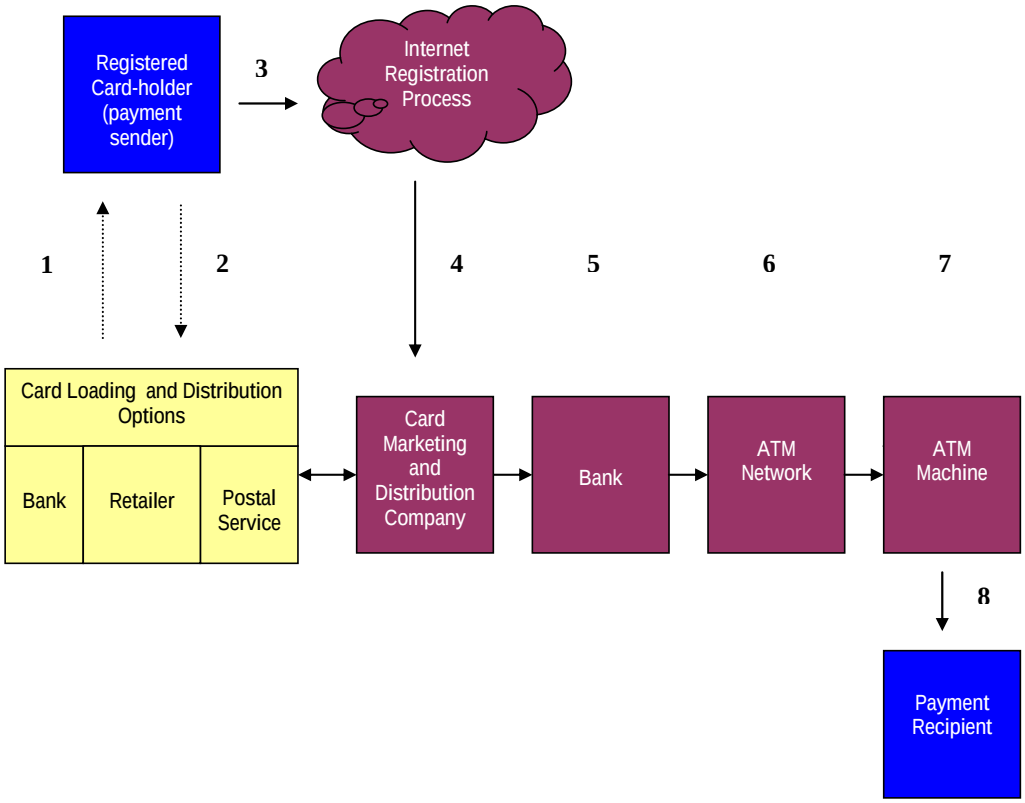



**Figure 1 The** process of issuing an open-system, magnetic strip, prepaid card varies by issuer. Steps (1), (2), and (3) above may occur in any order. In those three steps an individual completes the registration process for a prepaid card, prepays funds into the card account, and receives the card. Step (4) is the transfer of registration information to the service provider. When a card carries a bank association service mark (as in the case of MasterCard- or Visa-branded cards), the service provider must contract with a bank (5) in order to have access to the global ATM networks (6). Individual ATM machines (7) connect to local networks and often global networks allowing individuals in one country (8) to access funds held in another country.

## Electronic purse

An electronic purse, or e-purse (also referred to as a "stored value card" as the value is stored on the card), is value stored electronically in a device such as a card with an integrated circuit chip (called a smart card or chip card).[16] Unlike a card with a magnetic stripe, which stores account information, an e-purse actually stores funds on the card's memory chip. The user is literally carrying his funds with him on the card (hence the name electronic purse).

In some e-purse programs value can be transferred from the card directly to participating merchants or another individual without the transaction going through an account at an intermediary. This may limit the amount of

[16] This definition augments slightly the normal CPSS usage of the term "electronic purse" to also encompass the term "electronic money". For the purposes of this report, the term electronic purse is "a reloadable, multi-purpose prepaid card which may be used for small retail or other payments instead of coins" where the "value is stored electronically in a device such as chip card."

identifying information available with such transactions. To obtain funds from an e-purse payment, however, the merchant or individual must redeem the value from an account held by the e-purse provider at the e-purse issuing institution. As the funds are on the card, no online connection and no cardholder identification are needed to make a payment. The electronic purse function was designed to substitute for cash in everyday situations. Today, electronic purses are mainly used for micropayments such as for public transportation, parking tickets or vending machines.

The development and use of card-based e-purses has declined considerably over the past decade so that very few e-purse systems remain in existence. In addition, these few remaining e-purse solutions are generally not interoperable regardless of the market in which they operate. Only one system, the German GeldKarte that operates in the border area of Germany and Luxemburg (See Figure 2), is known to be used in multiple national jurisdictions. Furthermore, e-purses usually have a limited storing capacity for funds (e.g. the German GeldKarte has a load limit of EUR 200).


**Figure 2**

## Mobile Payments

Mobile payments refer generally to the use of mobile phones and other wireless communications devices to pay for goods and services. Payments are initiated from a mobile communications device using voice access, text messaging protocols (such as short/single messaging service or SMS), or wireless application protocols (WAPs) that allow the device to access the Internet. Authorization often occurs by keying in a unique personal identification number (PIN) associated with the customer or mobile device. Adoption of mobile payments varies from country to country. Use of mobile phones as a means to initiate payments is relatively widespread in Southeast Asia and in some European countries.[17]

Most mobile payment services simply use the phone as an access device to initiate and authenticate transactions from existing bank accounts or payment cards.[18] This is the equivalent of using the Internet to initiate a direct debit or credit transfer from a bank account, or a credit or debit card transaction. This is an extension of traditional payment methods.

New mobile payments: Where mobile payment services are not based on an underlying bank or payment card account, the telecom operator typically acts as a payment intermediary to authorize, clear, and settle the payment.[19] Telecom companies engaged in these activities may not be overseen by a country's central bank or other banking regulator but may be subject to AML/CFT measures.

The telecom operator may either allow the phone owner to charge certain transactions to the phone bill (post-paid) or may permit the phone owner to fund an account held by the telecom operator or other service provider for the purposes of making payments (prepaid). Prepaid mobile payments accounts operate in the same manner

---

[17] See CPSS, "Policy issues for central banks in retail payments," BIS, CPSS #52, March 2003, at http://www.bis.org/publ/cpss52.htm.

[18] See CPSS, "Survey of developments in electronic money and internet and mobile payments," BIS, CPSS #62, March 2004, at http://www.bis.org/publ/cpss62.htm.

[19] Telecom companies offering mobile payment services provide for the settlement of the payment transactions completed via their systems through normal banking channels.

as a prepaid card or an electronic purse. When the phone is used in the same manner as a prepaid card, the phone owner uses the phone as a payment system access device to authorize the deduction of value from the prepaid account. When the phone functions as an e-purse, the prepaid value is stored on the subscriber identify module or SIM card within the mobile phone.

Post-paid and prepaid card-like mobile payments are much more common than e-purse mobile payments. In the case of prepaid mobile payments, telecom providers often offer this service in conjunction with a bank. For example, in the Philippines two telecom companies offer mobile payment services, Globe Telecom and Smart Communications. Smart Communications' Smart Money is co-branded with Banco de Oro. The transactions and funds transfers Smart Money users initiate via their mobile phone are authorized against a prepaid account held at Banco de Oro. Smart Money users can also send cross-border remittances by providing relatives with a MasterCard-branded prepaid card linked to the Smart Money account that can be used to withdraw cash from an ATM.

Globe Telecom serves as the intermediary for funds transfers using G-cash and operates without a bank partner. As a result, Globe customers cannot withdraw funds from their prepaid accounts at ATMs but only over the counter at participating businesses. Figure 3 illustrates a G-Cash funds transfer from one Globe Telecom subscriber to another using SMS. Both G-Cash and Smart Money are subject to AML/CFT regulations (including suspicious transaction reporting) and supervision.

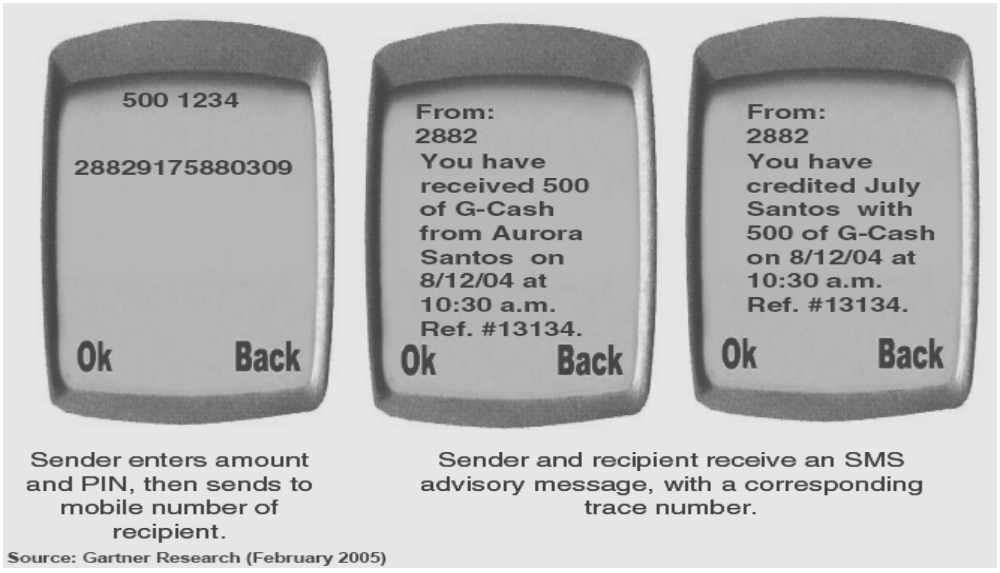



**Figure 3 G**-Cash Phone-to-Phone Remittance

## Internet payment services

The expression "Internet payment services" is generally used to address: (i) payment services that rely on a bank account and use the Internet as a means of moving funds to or from a bank account; and (ii) payment services provided by non-bank institutions operating exclusively on the Internet and that are only indirectly associated with a bank account.

In the former case, Internet payment services refer to traditional payment methods where the Internet is only an innovative channel to exchange the information that is needed to move the funds from one account to another, which allows customers to access their bank accounts from home, 24 hours a day.

Where Internet payment services do not rely directly on a bank account, such as PayPal, individuals can transfer funds, shop online, or participate in online auctions, using a pre-funded account; however, the payment service provider may not be subject to the same AML/CFT measures that apply to banks. The service provider usually

will not have a face-to-face relationship with its customers. Depending upon the accessibility of the Internet payment service, these activities can involve payments or funds transfers across national borders.

Some non-bank Internet payment services allow customers to hold accounts with the payment service provider, while others offer only to send or receive individual payments using the customer's existing bank or credit card account. When non-bank Internet payment services offer customer accounts they may pool those customer funds in a single account at a bank. The account may be held in the name of the service provider. In that case, the bank holding the service provider's account may have no direct relationship with the service provider's individual customers.

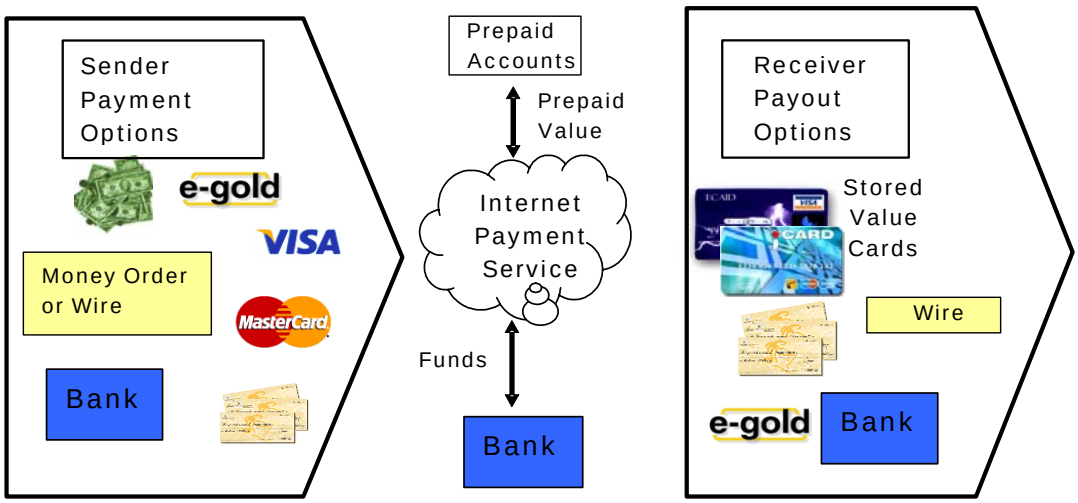



**Figure 4**

While a limited number of similar products exist in certain countries, PayPal appears to be the most widely used non-bank, Internet-based NPM. PayPal primarily functions as a payments intermediary for individuals and organizations that wish to trade with each other or transfer funds via the Internet. PayPal operates by allowing an individual to set up a pre-paid account in his name with PayPal that can be funded from a credit or debit card or a bank account via a credit transfer. Using those pre-paid funds, individuals can buy items or transfer funds to other PayPal account holders. The payment or transfer of funds occurs as a book-entry transaction between the PayPal accounts. When an individual wishes to access the funds in his PayPal account, he directs PayPal to credit his credit or debit card or bank account via a credit transfer or even a paper check.

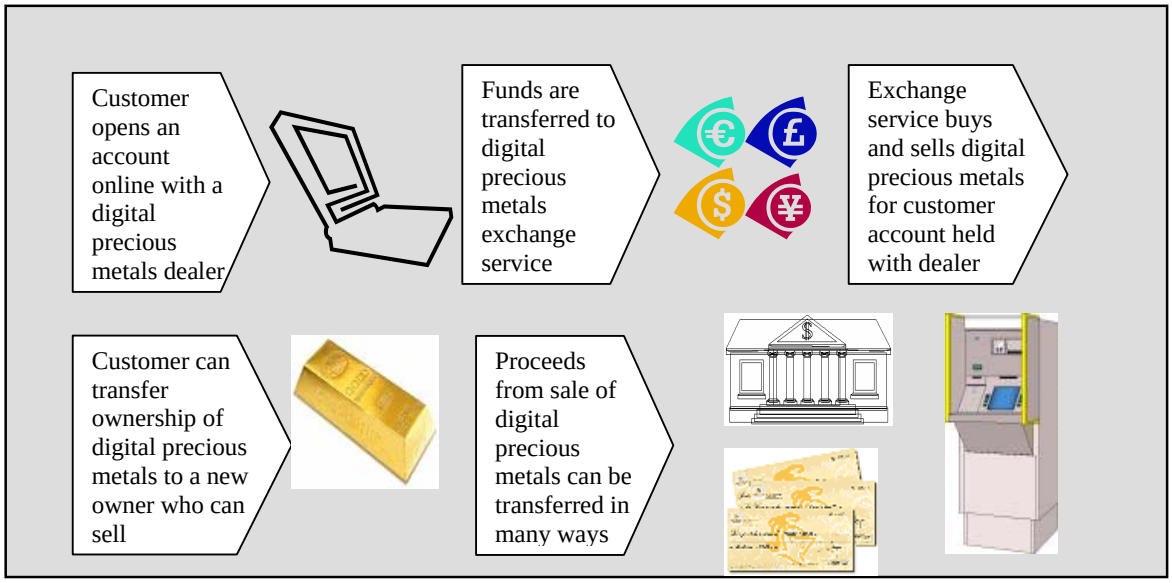
Service providers will differ as to the methods of payment they will accept to initiate a funds transfer, and the methods of payment they will use to distribute funds to the recipient. Figure 4 above illustrates how an individual can use a bank-issued credit card or other traditional payment methods to fund an Internet-based transaction account and subsequently make purchases or transfer all or a portion of the prepaid value to another account holder via book-entry by the service provider. The recipient can then use those funds to conduct additional transactions or withdraw the money via a traditional retail payment method. Online money transfer services set their own terms as what form of payment they will accept from senders and what forms of payment they make available to receivers.

## Digital precious metals[20]

Digital precious metals are a relatively new online MVT 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.

The oldest and best known of the digital precious metals dealers is e-gold Ltd., which claims to have almost 2 million accounts.[21] According to e-gold and other digital precious metals dealers, the rationale for using this store of value is to facilitate online transactions without regard for underlying currencies or access to foreign exchange. Transactions involving digital precious metals have immediate finality, which may appeal to online merchants that must pay high credit card interchange fees due to high fraud rates. Some digital precious metals dealers also allow users to maintain anonymous accounts. These traits are concerning to U.S. federal law enforcement agencies.

The transaction process associated with transferring the virtual holdings of precious metals between account holders can involve two separate service providers: the digital precious metals dealer, which maintains the accounts that contain the virtual holdings of precious metals; and the digital precious metals exchange service, which can act as a broker for the digital precious metals that the dealers buy or sell. Some dealers transact directly with account holders. Upon completion of a transaction, the selling account holder transfers ownership of his virtual precious metal holdings to the purchaser and can receive the proceeds of the sale through a variety of traditional and non-traditional payment methods (See Figure 5).




[20] The issuers of digital precious metals use the term "digital currency" to describe the barter arrangement they facilitate. Because of the potential confusion this common industry term would create with the term "e-purse" and "e-money", we have adopted the term "digital precious metals" for this report.

[21] E-dinar is a spin-off of e-gold and is affiliated with the Islamic Mint, a private organization working to revive the gold and silver currencies described in the Koran, the gold dinar and silver dirham. See: www.e-dinar.com.

**Figure 5 Buying** and selling digital precious metals typically involves working with two separate service provider categories: the digital precious metals exchange service and the digital precious metals dealer.

# 3. NPM Risk Assessment, Typologies, and Case Studies

The potential ML/TF risks posed by an NPM can vary from one service provider to another where there is no applicable AML/CFT law or regulation that establishes a uniform standard. To define high and low ML/TF risk characteristics of NPM operations, the project team developed a risk evaluation matrix (Table 1). The matrix identifies the essential risk criteria, applies those criteria to cash, representing the extreme high risk example, and provides generic NPM high and low risk scenarios.[22] Each NPM then is evaluated individually against the ML/TF risk criteria and wherever possible case studies and typologies are presented. The individual NPM risk assessments are summarized in Table 2.

To assess an NPM's ML/TF risk accurately, all of the risk factors have to be weighed in relation to the needs of the target market and applicable risk mitigating laws, regulations, and industry rules and practices. Taking all these factors into account, a particular NPM can be effective for all legitimate purposes while rendered ineffective or at least inconvenient for illegitimate purposes [23]

Few countries have identified criminal cases or typologies indicating ML or TF directly related to new payment methods. While this appears to indicate that NPMs are little used by criminals or terrorists, it may also indicate a more limited awareness of these NPMs within the AML/CFT community. The following typologies, therefore, should not be considered exclusive to any jurisdiction.

| **Payment Method Risk Factors** | | | |
|---|---|---|---|
| Criteria | Cash | NPM High Risk | NPM Low Risk |
| Identification | Anonymous | Anonymous accounts with no identification or verification requirements | Payment methods that conduct verification of full customer identification |
| Value Limits | No limit | Any anonymous payment method without funding or transfer limits | Specific limits are placed on funding and transaction values[24] |
| Methods of Funding | Anonymous, no intermediary, no transaction record | Using an anonymous funding source (e.g. cash or money orders) to fund or receive funds from an NPM account that also can be used anonymously to | Using funding, pay out and value transfer methods that require verification of customer identification and maintain transaction records for each value transfer. |

[22] Physical cash is often the ideal method of value transfer for criminal activity because it is anonymous, untraceable, requires no intermediary, is widely accepted, and provides for immediate settlement. The money laundering (ML) or terrorist financing (TF) risks posed by the new payment methods discussed in this report can be measured by how closely these alternatives match the attributes of cash. The main problem with cash for money launderers is its bulk, which creates difficulty moving the currency across borders. Criminals turning to cash alternatives, including NPMs, can eliminate the problem of moving large quantities of currency, but may encounter other limitations.

[23] In practice, no single category of the ML/TF risk criteria determines the relative ML/TF risk of a particular NPM. In addition to evaluating the NPMs considered in this report, the risk matrix presented may provide a useful framework for analyzing the level of risk associated with other payment systems or commercial activities.

[24] Account limits may not be necessary when full customer identification is verified and a transaction record is maintained, otherwise limits may be appropriate

| | | | |
|---|---|---|---|
| | | transfer value to an anonymous recipient | |
| Geographical Limits | Some currencies are accepted more widely than others | Payment methods that can be used to send and/or receive funds across national borders | Payment methods that can only be used to send and/or receive funds domestically |
| Usage Limits | No limit | Payment tool can only be used to access cash or can be exchanged for cash | Payment tool can only be used to acquire goods and/or services |

**Table 2**

## Prepaid Cards: Open System

*Identification.* Open-system prepaid cards may be used to support anonymous cross-border funds transfer (See Figure 6). When cards are issued without a bank account and applications are accepted online, via fax, or over the counter at retailers and check cashing outlets, insufficient customer due diligence in the application process may increase the potential ML/TF risk. This risk may be mitigated by account and transaction limits. Some service providers tier the customer identification process to the value held in the account and the frequency or value of account activity. Although prepaid cards have a unique account number and create an electronic transaction record, without adequate cardholder identification the transaction trail alone may be insufficient to help law enforcement trace the cardholder. Depending on the jurisdiction, offshore card issuers may pose additional ML/TF risks.

*Value limits.* Open-system prepaid card programs often target distinct market segments (e.g. children; teenagers away from home; adults without a bank account; and adults unable to qualify for a credit card). Each market segment may have distinct needs, which may be reflected in the funding and value limits which are set by the card-issuing bank. These limits include how much value can be held in a card account, how much can be prepaid at one time, and how often value can be added or withdrawn. The more money that can be moved through a card account, either at one time or through a series of ATM transfers, the greater the risk, relative to the other risk criteria.

*Method of funding.* Prepaid cards draw on a prepaid account that can be funded in a variety of ways. The card-issuing bank and its partners determine how card accounts can be funded. Some methods, such as credit transfers from a bank account or credit card, involve payment sources that: (i) independently verify the identity of the prepaid cardholder; (ii) will maintain a record of the funds transfer to the prepaid card; and, (iii) will usually have AML policies and procedures that include monitoring transactions for suspicious activity. Other methods of account funding, such as cash and money orders, are anonymous and leave no paper trail, increasing the potential ML/TF risk independent of the other risk criteria.

*Geographic limits.* Open-system prepaid cards that have the capability to provide access to cash at automated teller machines (ATMs) increase the potential ML/TF risk independent of the other risk criteria and risk mitigation. Access to cash through the ATM networks, however, usually requires the use of a personal identification number (PIN) that must be pre-set with the issuing institution. The requirement of the PIN may not, however, provide sufficient information within the transaction record to identify with full certainty the recipient.

*Usage limits.* Open-system prepaid cards can have usage limits. Physical cards may be limited to point-of-sale (POS) networks, allowing only the purchase of goods and services and barring access to cash via ATMs. Virtual cards provide the cardholder only an account number to be used for online and telephone transactions; there is no physical card to access cash via ATMs. However, most open-system prepaid cards are physical cards and facilitate access to POS and ATM networks. In some countries, physical cards may also be used to withdraw cash at retailers whereby an amount higher than the price of goods purchased is paid to the retailer and the difference between the price of the goods and the amount paid is given in cash to the cardholder. For the reasons

discussed previously, cards that can provide access to cash via ATMs on a global basis may increase the potential ML/TF risk independent of other risk criteria and risk mitigation.

*Typology.* The transfer of illicit proceeds from one country to another using debit cards associated with personal bank accounts and the ATM networks is an established method of ML. Instances of ML have been identified as having occurred even when a customer identification program is in place at the time the bank account is opened. This can occur when a customer uses false identification documents. Some open-system prepaid cards offer similar ATM access without requiring the cardholder to open a bank account or verify identification, creating the potential for greater use of this typology.

*Case Studies.*

A. In 2001, a suspicious activity report (SAR) filed in the United States detailed the acquisition of more than 300 prepaid cards by a single individual who used them to transfer almost $2 million to Colombia. No further information is available to the public.

B. In 2001, the El Dorado Task Force[25] in New York, identified a significant trend in the number of individuals who appeared to be using ATMs as a means of laundering money through cash withdrawals in foreign countries. Analysis identified more than fifty SARs involving the structured deposit of cash into New York area accounts with subsequent ATM withdrawals in Colombia, Mexico, Peru, Ecuador, and Panama. A similar study conducted by the Financial Crimes Enforcement Network (FinCEN, the U.S. financial intelligence unit) over a four-year period found the most common withdrawal locations were Colombia, Venezuela, Mexico, Argentina, and Brazil. In almost all of the SARs, the banks described the suspected violation as ML-related.

C. In 2004, German tax investigators discovered a case of ML through prepaid cards. Two participants of a criminal fraud/embezzlement scheme had transferred parts of their shares of the criminal proceeds onto several prepaid cards. They used the funds on the cards for cash withdrawals (domestic only, not in foreign countries) and payments for goods. The card accounts were kept only for short periods (6 – 24 months) after which they were closed again and new ones were opened. In this case more than 350.000 EURO were hidden and laundered this way.

[25] Created in 1992 to target money laundering in New York, the El Dorado Task Force became one of the nation's most successful money laundering task forces. It is led by the Immigration and Customs Enforcement federal law enforcement agency and includes representatives from 29 federal, state, and local law enforcement agencies.

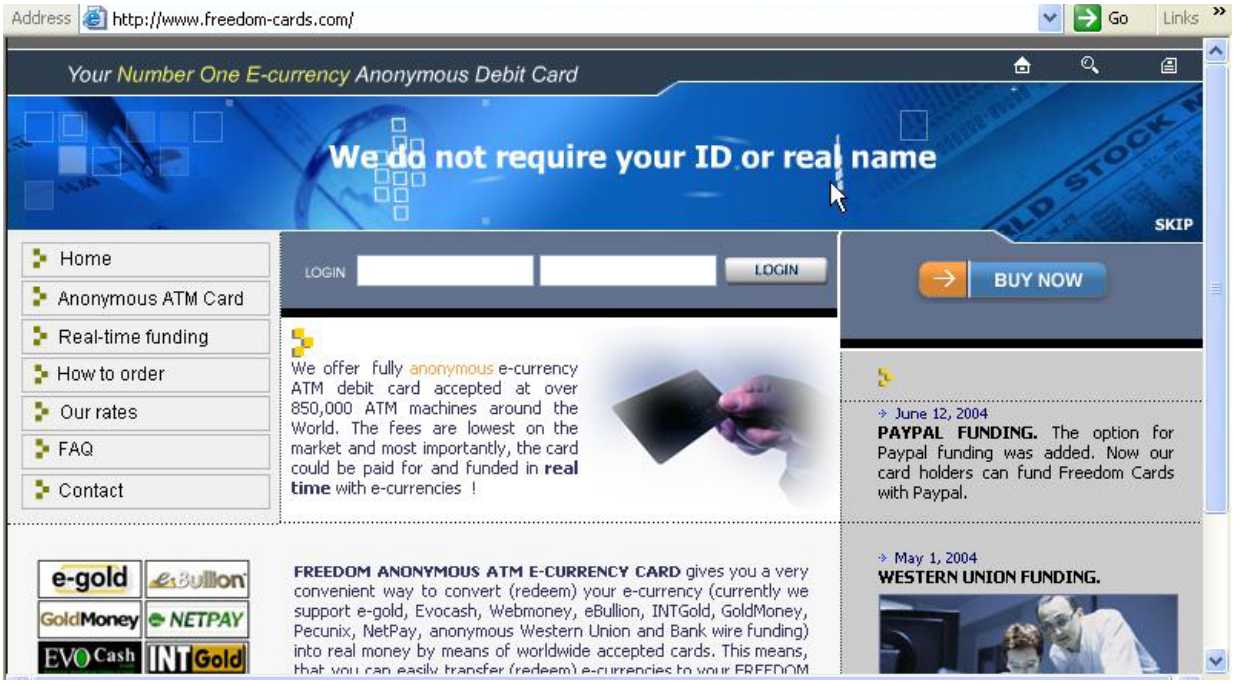



**Figure 6**

## Prepaid Cards: Closed System

*Identification.* Anonymous, closed-system prepaid cards may be resold for cash, which could facilitate ML and TF. This risk, however, is mitigated by the demand for the goods and services that can be purchased with the card as well as the geographic scope of a card's acceptance.

*Value limits*. A high-value, closed system prepaid card that can be resold may be a convenient substitute for cash when moving value across borders. The higher the value limit on a closed system prepaid card the greater the potential ML/TF risk, independent of other risk criteria and risk mitigation.

*Method of funding.* As with open-system prepaid cards, closed-system cards draw on a prepaid account that can be funded in a variety of ways determined by the merchant selling the card.

*Geographic limits.* The resale potential of a closed-system prepaid card depends upon the availability of resale markets and the level of demand for the card. The greater the geographic scope in which the card is accepted, the greater the potential ability to resell it, which may increase its potential use as an ML/TF tool.

*Usage limits.* Closed-system stored value cards are by definition limited in their potential usage. Generally, these cards can only be used to buy goods and services sold by the card issuer. As noted above, the greater the availability of resale markets and the level of demand for the card, its potential ML/TF use may be increased. Unlike open-system prepaid cards, closed-system cards cannot be used to access cash via ATMs, although they can potentially be resold for cash and can be purchased for cash.

*Typology.* The wholesale distribution of prepaid long distance calling cards is, according to the U.S. Federal Bureau of Investigation, a $4 billion a year cash-intensive industry that can provide cover for ML. At the retail level, closed-system prepaid cards can potentially be purchased anonymously in large quantities for cash,

transported across borders, and resold. Unlike currency, the value held on prepaid cards is not apparent to customs and border officials, although the quantity of cards may be.

*Case Studies.*

A. In 2001, FinCEN reported that more than 160 Suspicious Activity Reports were filed on telephone card businesses with dollar amounts that ranged between $300,000 and $50 million.[26] The FBI reported in 2005 that a review of the Suspicious Activity Report database revealed that financial institutions are increasingly reporting suspicious activity related to the prepaid calling card industry.

B. In 2005, U.S. Immigration and Custom Enforcement initiated an investigation into an employee of a state agency in Ohio selling fraudulent drivers' licenses and identification cards in exchange for prepaid telephone cards.[27]

## Electronic Purse

*Identification.* A cardholder with an electronic purse linked to a bank account is identified through the account-opening process. There are other chip card programs, however, not linked to a bank account, which may not require customer identification and provide no transaction record. Independent of other risk factors and risk mitigation methods, insufficient customer identification may increase the potential ML and TF risk.

*Value limits*. Although chip card technology does not prohibit electronic purses from holding unlimited value, current card programs are generally used for small value transactions and therefore tend to have low value limits. Germany's *GeldKarte*, for example, has a value limit of €200.

*Method of funding and receipt of funds.* Electronic purses linked to a bank account can only have funds added through the account. Some e-purse programs also allow for card-to-card value transfers. An e-purse that is not linked to a bank account may have the ability to add value via cash. Independent of any risk mitigation methods, a card with a high value limit, anonymous card-to-card transfers, and cash as an option for loading and withdrawing value could pose a significant ML and TF risk.

*Geographic limits.* The lack of significant cross-border capability associated with any electronic purse program significantly reduces the ML/TF risk posed by these payment tools.

*Usage limits and receipt of funds.* Electronic purses generally are limited to small value retail transactions, although some programs do allow for card-to-card and card-to-cash functionality.

*Typology.* There are no observed ML/TF typologies associated with the current use of electronic purses.

*Case Studies.* There are no observed ML/TF cases associated with current use of electronic purses.

## Mobile Payments

*Identification.* Most mobile payment systems use the mobile phone as a device to access a bank account or credit card. These systems establish customer identification when the underlying bank or credit card account is opened. A similar customer identification process takes place when a telecommunications service provider,

---

[26] Department of the Treasury, FinCEN, SAR Bulletin, June 2001.

[27] U.S. Immigration and Customs Enforcement, News Release, Ice Arrests 9 in Ohio Fraud Driver's License Scheme, available at: http://ice.gov/graphics/new/newsreleases/articles/drivers022405.htm.

rather than a financial institution, holds the mobile payment account and extends credit to the account holder. If mobile phone service is prepaid and the funds used to facilitate mobile payments are also prepaid, the service provider may not be motivated to fully identify customers because of the absence of credit risk.

*Value limits*. Where mobile phones are access devices to underlying bank and credit card accounts, limits may not be necessary. In the Philippines, Globe Telecommunication requires prepayment for transactions through its G-Cash mobile payment program and imposes a maximum per transaction of 10,000 pesos ($182, €145), a maximum per day of 40,000 pesos ($728, €580), and a maximum transfer per month of 100,000 pesos ($1,825, €1455).

*Method of funding.* Mobile payment programs that draw on a prepaid account can be funded in a variety of ways. Payment sources that have independently verified the identity the phone owner and that maintain a record of the funds transfer to the mobile payment account present a low risk. The use of cash to fund a mobile payment account, independent of other risk factors or risk mitigation strategies, may present some limited ML/TF risk.

*Geographic limits.* Mobile payment systems currently do not facilitate cross-border transactions due to incompatible systems. An attempted joint venture (SIMPAY) of several European telecommunications service providers failed in 2006.

*Usage limits.* Payments can only be received by a participating merchant or fellow service subscriber.

*Typology.* There are no observed ML/TF typologies associated with the current use of mobile payment systems.

*Case Studies.* There are no observed ML/TF case studies associated with the current use of mobile payments systems.

## Internet Payment Systems

*Identification.* Internet payment systems may permit anonymous accounts.

*Value limits.* Individual service providers usually determine the limits on account or transaction value, which affects the relative ML/TF risk.

*Method of funding.* Internet payment systems set their own terms regarding what methods of payment they will accept to fund accounts and how funds transfers are paid out to recipients. Service providers accepting cash and money orders or transfers from anonymous prepaid cards may present a greater ML/TF risk than service providers that limit funding sources to a bank account or credit card.

*Geographic limits.* Offshore Internet payment systems may facilitate transactions that are illegal in the payer's home jurisdiction. The online payment service acts as an intermediary, receiving funds that are passed on to a final recipient. In some cases, where direct funds transfers to the final recipient would be blocked under a jurisdiction's domestic laws, the payer can transfer the funds through an offshore online payment system operating under a different regulatory regime

*Usage limits.* Individual service providers determine the usage limits for the service.

*Typology.* Internet payment systems offer the potential for anonymous cross-border funds transfers. The risk is greatest when the service provider operates offshore in a jurisdiction with a weak anti-money laundering and counter TF regime. Even when customer due diligence is undertaken, where the customer relationship exists entirely online, the extent to which service providers attempt to verify customer identification determines the ML/TF risk relative to the other risk criteria and risk mitigation efforts.

*Case Studies.* There are no observed ML/TF cases associated with current use of Internet payment systems.

## Digital Precious Metals

*Identification.* Digital precious metals dealers may permit anonymous accounts.

*Value limits*. There may be no value limits on digital precious metals accounts other than the amount of funds that can be placed into the online account through the use of traditional or non-traditional payments systems.

*Method of funding.* Each service provider sets its own terms as to what methods of payment it will accept. The serve provider's ability to accept any specific method of payment will also be limited by the willingness of the providers of these other payment services to offer digital precious metals brokers or dealers access to their services.

*Geographic limits.* Service providers may operate globally with no geographic limitations, although natural limits do exist based upon access to the Internet. Some governments, such as China and others, and may also place limits on the types of services to which they permit their citizens access. Web hosting and other Internet service providers may also place limits on the types of web sites and businesses they are willing to support.

*Usage limits.* Digital precious metals accounts may have no usage limits. Each service provider sets its own terms as to how it will disburse the funds, but its ability to do so also depends on the willingness of the providers of other payment services to offer precious metal brokers or dealers access to their services.

*Typology.* Digital precious metals offer the potential for anonymous cross-border funds transfers. The risk is greatest when the service provider operates offshore in a jurisdiction with a weak anti-money laundering and counter terrorist financing regime. Even when CDD is envisaged, where the customer relationship exists entirely online, the extent to which service providers attempt to verify customer identification determines the ML/TF risk relative to the other risk criteria and risk mitigation efforts.

*Case Studies.*

A. In March 2004, an Oklahoma man admitted to a financial fraud scheme involving an online investment fund. Thousands of people lost almost $9 million. According to the U.S. Federal Bureau of Investigation, the online investment scheme, E-Biz Ventures, laundered investor money through e-gold Ltd. The Oklahoma man who created this criminal enterprise may have been targeting tax evaders and other criminals because he "allegedly highlighted his reliance on e-gold to appeal to his victims' fear of the federal government and their desire for anonymity."[28]

B. In October 2004, the United States Secret Service shut down ShadowCrew.com, one of the largest illegal online centres for trafficking in stolen identities and payment cards. There were 21 arrests, and to date 12 of the defendants have pleaded guilty. ShadowCrew.com had approximately 4,000 members from all over the world dedicated to malicious computer hacking and the sale of stolen and counterfeit identification and credit and debit card numbers.[29] Those who pleaded guilty "acknowledged that ShadowCrew members sent and received payment for illicit merchandise and services via Western Union money transfers and digital currencies such as e-gold and Web Money."[30] One, "who used the nickname Voleur -- French for thief -- boasted in a chat room that he moved between $40,000 and $100,000 a week," was receiving Western Union money orders from accomplices, which, for a fee, he laundered through e-gold accounts.[31]

---

[28] Grow, Brian, Gold Rush, Business Week, January 9, 2006, accessed at: http://www.businessweek.com/magazine/content/06_02/b3966094.htm.

[29] http://www.usdoj.gov/opa/pr/2004/October/04_crm_726.htm

[30] http://www.usdoj.gov/criminal/cybercrime/mantovaniPlea.htm

[31] Grow, Op. Cit.

C. Estonia reports a case involving the laundering of illicit proceeds from unauthorized bank account withdrawals through the use of digital precious metals. Account information was gathered through the use of fraudulent e-mails that claimed to be sent on behalf of the recipient's bank which sought to confirm the information. If the recipient responded with the account information, the criminals initiated unauthorized withdrawals. The money was laundered through a series of steps involving cross-border transactions via Western Union and Money Gram, and ultimately Web Money, a digital precious metals service.

## Off-shore provision of NPMs

A potential risk factor that may be common across many types of NPMs is that of jurisdiction. In some cases, NPM issuers or service providers may be located in an offshore financial centre and therefore subject to a less robust system of laws and regulation. Additionally, processes related to NPMs often flow through multiple jurisdictions, which has the effect of making the product more complex. The involvement of multiple jurisdictions and resulting segmentation of various parts of the chain of transactions increases the difficulties of designing effective supervisory strategies for NPMs. When NPMs are provided over the Internet, the jurisdiction risk is increased due to the potential difficulties in identifying to which jurisdictions the service providers belong, where they are incorporated, which authorities are responsible for their supervision and what AML/CFT regime is applicable. In this case it becomes extremely complicated for any of the jurisdictions where the NPM is accessible to national customers to intervene and stop illegal activities that are taking place. International cooperation among authorities may be an essential tool to face these situations, especially where efficient and effective exchange of information systems are in place. In this regard, the Early Warning System proposed by Germany at the ASEM symposium which took place in Berlin at the end of 2003 and described in the box below, could represent a good example.

### Germany's Proposal for an Early Warning System

Offshore card issuers and payment services, whether acting through an agent or via the Internet, do not always follow the law in the countries where they seek to do business. Germany introduced the „Early Warning and Information Sharing System" at the ASEM Symposium in Berlin in October 2003 to promote coordination and information sharing between jurisdictions in the context of Alternative Remittance Systems and Underground Banking. The ASEM[32] experts „agreed to nominate a point of contact from the competent law enforcement or supervising body or FIU in each ASEM country in order to promote coordination including exchange of information and, when possible, joint action between relevant domestic and foreign authorities to deter illegal activities or abuse. Experts from ASEM countries agreed that this kind of early warning system would help to disrupt illegal international transactions simultaneously in all affected countries and would enable law enforcement and supervisory authorities to take the necessary co-ordinated action within their own jurisdictions. The experts welcomed the involvement of other countries in this process."[33]

The Early Warning and Information Sharing System was later approved and joined by several FATF members to whom it was introduced during the FATF Seminar on TF in Paris in February 2004.

Although originally intended for fighting Underground Banking, the Early Warning System could also be a very effective tool for the fight against the abuse of new payment systems. These NPM, especially those making use of the Internet, have an international structure very much like Underground Banking Networks. New payment methods can be used to transfer funds worldwide. The Early Warning System therefore is a very useful and effective tool to not only take co-ordinated actions against the abuse of such NPM but also to raise awareness of such abuse not only in singular jurisdictions, but worldwide.

---

[32] The acronym ASEM stands for Asia-Europe Meeting, an informal forum for dialogue between European and Asian jurisdictions. For more information on ASEM and its members see www.aseminfoboard.org

[33] Final conclusions of the Berlin Symposium on Alternative Remittance Services and Underground Banking 30-31 October 2003, sec. IV.

## NPM Money Laundering and Terrorist Financing Risks

| Payment Method | Potential Risk Factors | Current and Potential Risk Mitigants |
|---|---|---|
| Prepaid cards: open-system | • Anonymous card holder<br>• Anonymous funding (inflow) and anonymous access to funds (outflow)<br>• High card value limit and/or no limit on the number of cards an individual can acquire<br>• Access to cash globally through ATMs<br>• Offshore issuers may not observe laws in all jurisdictions | • Verify cardholder identification<br>• Limit funding options<br>• Limit card value and/or the number of cards that an individual can acquire and/or value per transaction<br>• Limit cross-border access to cash<br>• Monitor transactions and report suspicious activity<br>• Implement a card/account block<br>• Limit access to network by undesirable merchants and ATM providers/networks |
| Prepaid cards: closed system | • Anonymous card holder<br>• Anonymous funding<br>• High card value limit<br>• Substitute for bulk cash smuggling<br>• No limit on the number of cards an individual may purchase | • Verify cardholder identification<br>• Limit card value and/or the number of cards any one purchaser may acquire<br>• Limit funding options<br>• Monitor transactions and report suspicious activity<br>• No direct cash access via ATM<br>• Implement a card/account block |
| Electronic Purse | • Anonymous card holder<br>• Anonymous funding and receipt of funds<br>• High card value limit<br>• No transaction record | • Verify cardholder identification<br>• No card-to-card transfer capability<br>• Limits on the amounts that can be spent/stored<br>• Limited cross-border functionality<br>• Limit funding options<br>• Monitor transactions and report suspicious activity<br>• Implement a card/account block |
| Mobile payments | • Anonymous accounts<br>• Anonymous funding and receipt of funds<br>• High or nonexistent account funding limit | • Account holders are identified when phones are used as an access device to a bank or credit card account or when the telecom verifies phone owner identification<br>• Limited cross-border functionality<br>• Limited account and transaction value<br>• Limit funding options<br>• Monitor transactions and report suspicious activity<br>• Implement a card/account block<br>• Limit access to network |
| Digital precious metals | • Anonymous accounts<br>• Anonymous funding and receipt of funds<br>• High or nonexistent account funding limit<br>• Offshore service providers may not observe laws in other jurisdictions | • Identify account holder<br>• Maintain transaction record with payer and recipient<br>• Monitor transactions and report suspicious activity<br>• Limit funding options<br>• Implement account block<br>• Limit access to service |
| Internet payment systems | • Anonymous accounts<br>• Anonymous funding and receipt of funds (ATM)<br>• High or nonexistent account funding limit<br>• Offshore service providers may not observe laws in other jurisdictions | • Identify account holder<br>• Maintain transaction record identifying payer and recipient<br>• Monitor transactions and report suspicious activity<br>• Limit funding options<br>• Implement account block<br>• Limit access to the service |

**Table 3**

# 5. Application of FATF Recommendations and Special Recommendations; and Selected Regulatory Approaches[34]

The FATF 40 Recommendations and nine Special Recommendations highlight potential ML and TF risks associated with new payment methods and provide guidance for regulating domestic service providers.

Recommendation Five addresses anonymous accounts, which is the principal ML/TF vulnerability identified in the new payment methods analyzed in this report. Recommendation five states: "Financial institutions[35] should not keep anonymous accounts or accounts in obviously fictitious names."

Recommendation Eight specifically addresses the ML/TF risks that may be associated with new payment methods: "Financial institutions should pay special attention to any ML threats that may arise from developing technologies that may favour anonymity, and take measures, if needed, to prevent their use in ML schemes."

Recommendation 23 underscores the need for all providers of financial services to be subject to adequate regulation and supervision. With regard to the broad category of money or value transfer services, Recommendation 23 states: "At a minimum, businesses providing a service of money or value transfer, or money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat ML and TF."

Special Recommendation VI amplifies Recommendation 23, stating in part: "Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions."

Special Recommendation VII specifies the information that should accompany domestic and cross-border wire transfers, but allows wide latitude in how financial institutions and jurisdictions may interpret and react to the completeness of the wire transfer information received.

Recommendation 21 signals the potential need to close off "business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations."

The FATF Glossary includes among the activities that are performed by financial institutions as a business for or on behalf of their customers "issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)".

## Regulatory Approaches

Determining either the volume or nature of transactions that use the new payment methods described in this report is difficult because few countries appear to be either aware of these payment tools or to be monitoring their use. The Bank for International Settlements (BIS) notes: "With technology facilitating the breakdown of traditional banking services into multiple components and the addition of analytical tools and other capabilities into traditional banking services, more unlicensed non-bank entities are likely to provide bank-like services via the

[34] The regulatory approaches mentioned in this section have been verified with the jurisdictions concerned. Some measures were not adopted specifically for anti-money laundering purposes but rather by financial supervisors or monetary authorities to protect other financial interests.

[35] The term "financial institutions" refers to service providers that transfer money or value in both the formal and informal sectors.

Internet, including those that are extended cross-border. Differences in definitions as to what constitute a "bank" among jurisdictions would likely be magnified and will increasingly challenge how bank supervisors deal with financial entities with no home supervision."[36] The BIS notes: "Over time some technology companies offering "e-banking-like" services might relocate into jurisdictions where their specific mix of products and services does not require a banking license just as offshore centres developed previously."[37]

"The trend toward a broader range of service providers and to greater networking in end-user markets has raised some regulatory questions. The regulatory approaches taken by different countries to the overall efficiency, risk and consumer concerns associated with new payment instruments, providers and market arrangements have differed somewhat. In some European countries a response to the challenge has been to limit the provision of some payments services to financial institutions. In other countries the provision of payment instruments and services has not been restricted."[38]

## Germany's Regulatory Provisions With Regard to Prepaid Cards

In a prepaid card scheme, German financial supervisory authorities focus on the card issuer (mainly banks) and the card broker (the intermediary service provider between the bank and the cardholder). By acting as an agent to arrange customer relationships between the card issuer and a customer/cardholder, a card broker is considered to be conducting deposit brokering. This is because, in Germany, taking in funds to issue a prepaid card is considered to be the same as taking in deposits. As a consequence, a full banking license is required to issue prepaid cards. The card issuer is considered as a credit institution and therefore subject to full AML compliance including customer identification.

As regards those prepaid card schemes where the card issuer is located abroad, the card issuer may rely on an intermediary service provider (so-called "card-broker) to promote the card in the targeted market. By acting as an agent to arrange customer relationships between the card issuer and a customer/cardholder, a card broker is considered to be conducting "deposit brokering". This business type of deposit brokering does not require a license if the deposit taker (in this case the card issuer) is domiciled within the European Economic Area.

If however a card broker is acting as an agent for a card issuer domiciled outside the European Economic Area, the card broker is considered a financial services institution and is required to be licensed. As a financial services institution, a card broker is subject to full AML compliance including customer identification.

## The EU Regime for e-money

In the EU, there are currently two pieces of legislation which regulate e-money: Directives 2000/46/EC[39] (the e-money institutions Directive)[40] and 2005/60/EC (third money laundering Directive); the latter shall be transposed by Member States into national legislation by December 2007.

Whilst it is widely accepted that the definition of e-money covers prepaid cards, e-purses and internet payments such as PayPal, there is some controversy as to whether pre-paid mobile payments are covered. In the whole EU, there are only 6 "purebred" e-money issuers, as the majority of entities issuing e-money are banks conducting other banking business as well.

---

[36] Management and Supervision of Cross-Border Electronic Banking Activities, Bank For International Settlements, July 2003. Accessed at: http://www.bis.org/publ/bcbs99.pdf

[37] Ibid.

[38] CPSS #33

[39] Official Journal L275, 27/10/2000

[40] Official Journal L 309, 26/10/2005

Following the flexibility provided for by the Directive on e-money institutions as regards the application of AML/CFT provisions, EU Member States (MS) currently apply different regimes to e-money: a majority of MS applies the same AML/CFT provisions as for banks, some apply a lighter regime but the situation is expected to change after the third Money Laundering Directive is transposed by MS in their national legislation.

In particular, the third AML Directive gives the possibility to EU MS to allow e-money issuers not to apply customer due diligence in respect of e-money, where, if the device cannot be re-charged, 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 2500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1000 or more is redeemed in that same calendar year by the bearer.

Simplified CDD applies to other products or transactions carrying a low risk of ML or TF, in accordance with technical criteria identified to help assess whether situations represent a high or a low risk of ML or TF.

Notwithstanding the technical criteria identified, simplified CDD shall not apply in the case where there is information available that suggests a product is subject to a high risk of being misused for ML or TF purposes.

## Regulating Internet Payments, and Other New Payment Systems, in the United States

The comprehensive AML/CFT regime in the United States requires "financial institutions" (as defined in the Bank Secrecy Act and in implementing regulations) to, among other things, establish and maintain anti-money laundering programs, file cash transaction, suspicious activity and other reports, perform CDD, and obtain and retain records regarding customer identification and verification. Within this framework, non-depository financial institutions that provide payment services tend to belong to some category of "money services businesses" (MSBs). MSBs are defined to include five distinct types of financial services providers: currency dealers or exchangers; check cashers; issuers of traveller's checks, money orders, or stored value; sellers or redeemers of traveller's checks, money orders, or stored value; and money transmitters. The five types of financial services are complementary and are often provided together at a common location. Money services businesses have grown to provide a set of financial products that one would traditionally look to banks to provide.

As noted above, money transmitters and issuers, sellers or redeemers of "stored value" are MSBs subject to the US AML/CFT regime, which requires certain MSBs to register with FinCEN (the FIU), as well as to establish an AML programs and to comply with various reporting and recordkeeping requirements. Many types of MSBs also are required to be licensed on the state level. Whether a particular online payment service, stored value provider, digital precious metals service or other value-service provider or payment system or digital currency service meets the definition of an MSB under the regulations is a fact-specific determination. That determination is dependent upon such factors as the structure, location, operations and services of the particular business. If the service or business is found to be an MSB under these regulations, then it would be subject to all of the programmatic, reporting and record-keeping requirements described here. Many payment systems, particularly online payment system providers, are based outside the United States and are not subject to U.S. jurisdiction. U.S. federal banking agencies, FinCEN, and others also routinely provide guidance to depository institutions regarding potential risks associated with non-bank payment service providers and available means to mitigate those risks.[41]

[41] For example, sections of the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual relating to electronic cash, prepaid products and third-party payment processors were updated in July 2006 to outline risk factors in these products and to recommend steps that depository institutions should take to mitigate those risks.

### *Use of "Special Measures" in the United States*

The United States can take action against an NPM based outside the country that poses a ML threat to the U.S.[42] In the United States, the Secretary of the Treasury is authorized – in consultation with the Department of Justice, the State Department, and the appropriate Federal financial regulators – to designate a foreign jurisdiction, institution, class of transactions, or type of account as being of primary ML concern.

There are a range of options available to target the specific ML concern most effectively. Through the imposition of various "special measures," the Treasury Secretary can gain more information about the jurisdictions, institutions, transactions, and accounts that are of concern, and take appropriate action to safeguard U.S. financial institutions.

The special measures available to the Secretary include requiring of domestic financial institutions: (1) Recordkeeping and reporting of certain financial transactions; (2) collection of information relating to beneficial ownership; (3) collection of information relating to certain payable-through accounts; (4) collection of information relating to certain correspondent accounts; and (5) prohibition or conditions on the opening or maintaining of correspondent or payable-through accounts.

## India Forbids Use of Digital Precious Metals

In October 2002, India's central bank, the Reserve Bank of India, forbid the use of "e-gold" as violating national rules requiring only sovereign currencies be used in domestic transactions. The central bank stated in a news release: "An impression is sought to be created among the members of public by some agencies/persons that transactions involving e-gold, purportedly an electronic currency, are freely permitted in India and that e-gold has the status of a foreign currency… The Reserve Bank clarifies for the information of [the] public that 'e-gold' is not a currency of any sovereign state."[43]

## Australia: Unlicensed Digital Precious Metals Sites

In 2004 the Australian Securities and Investments Commission (ASIC) identified several online digital precious metals dealers including some based outside the country as conducting business without a proper license: "Following an examination of electronic currency trading websites, ASIC became aware of three Australian-based businesses that were operating such sites or were acting as agents for similar businesses based overseas. These businesses exchanged conventional currencies to electronic currencies and vice-versa, and charged a commission for their services… ASIC believes that such products can be defined as non-cash payment systems and that people who deal in such products with Australian consumers must hold an Australian financial services licence (AFSL)." The identified businesses "all withdrew their websites and closed down their businesses voluntarily."[44]

# 6. NPM Questionnaire Results and Analysis

## Objectives and methodology

This section gives an overview of the responses to the questionnaire issued by the project team to which there were 37 responses. Most respondents identified NPMs in their jurisdiction. In some countries, respondents have either not identified NPMs (e.g. Argentina, Cambodia and Slovenia) or have only provided information about

---

[42] Some online payment systems may be licensed in one country and maintain operations (including staff, computer systems, and customers) in various other countries without a physical retail presence anywhere.

[43] http://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx

[44] http://www.asic.gov.au/asic/asic_pub.nsf/byheadline/04-366+ASIC+acts+to+shut+down+electronic+currency+trading+websites?openDocument

traditional means of payment (e.g. Qatar, Latvia, Macao and Slovakia), or even traditional means of payment which can be accessed in new ways such as Internet banking (Azerbaijan). Some respondents privately indicated to the project team there were unsettled cases and investigations underway regarding NPMs, but that these cases could not be disclosed.

Summary findings from the questionnaires are presented below for each payment method with more detailed information presented in Appendix B in the following fields of information: NPM category, market size, regulation of access to activity, AML/CFT provisions and AML/CFT cases as well as the existence of illegal operators. Conclusions are provided at the end of this section as well as for each category of NPM.

## Prepaid cards

Fourteen countries, approximately one-third of respondents, report the presence of prepaid cards, both closed-system and open-system cards are reported. With regard to open-system cards, ATM functionality is often present and sometimes allows transferring funds worldwide.

Little information was reported regarding market size, but where such information is available it often indicates a small or emerging market.

Most of the reported types of prepaid cards are submitted either to registration or licensing requirements or under supervision (exceptions are Palau and New-Zealand). The picture is mixed concerning AML/CFT provisions, as for less than half[45] of the countries, no AML/CFT provisions have to be applied (ex. USA and Czech Republic). It is interesting to note that all the payment methods which are not under CFT/AML regulation have a limit to the transferred amount.

Except for the USA and New-Zealand, no AML/CFT cases are reported. The same goes for illegal operators, but with no exceptions.

## Payments initiated by means of a mobile phone (and linked to a bank-account)

Four countries reported mobile phones are used to access bank accounts (Korea, Finland, New-Zealand and China). As the payment method is based on bank accounts, registration/licensing apply, as well as supervision and AML/CFT provisions.

No AML/CFT cases or illegal operators are reported.

## E-purse

Four countries (Belgium, Switzerland, Germany and the Netherlands) reported e-purses are issued in their jurisdiction. In all cases, e-purse issuers are required to be licensed and supervised and AML/CFT provisions apply. In all cases, there are limits to transferred amounts. There is no evidence of ML or examples of law enforcement actions in any of those countries.

## Internet payments

This is the largest group of new payment methods, as they are reported by 15 out of 37 countries (40%). Systems differ per country; some of them (e.g. Paypal, Neteller) operate in several jurisdictions.

Most countries apply registration/licensing requirements and supervision or are working towards putting in place such regulations. Most countries also apply AML/ CFT provisions (sometimes even when registration/licensing/supervision are not applied).

Amongst countries where no AML/CFT provisions apply (NL, ES, CN), only CN has found evidence of ML/TF. Examples of law enforcement cases can be found in the USA, ET, and CA.

---

[45] "Half" is only correct when taking into account that Palau and New Zealand both indicate that even though they apply AML/CFT requirements, they have no registration or licensing requirements nor supervision.

One of the problems reported regarding this NPM is the possibility for payment service providers to offer their services offshore and therefore circumvent the destination country's registration/licensing rules as well as supervision and AML/CFT requirements.

## Mobile Payments

Only five countries (about 10% of the countries responding to the questionnaire) reported this NPM. In those countries, this NPM seems to be used for micro-payments. The picture is mixed as regards regulatory framework and application of AML/CFT requirements.

None of the countries reported evidence of ML/TF or law enforcement cases.

## Digital precious metals

This NPM does not seem to be widespread, as only 2 countries (Estonia and the USA) report its presence in their jurisdiction. Not much information is provided by Estonia,. In the USA case, a significant number of operators are active, but are not necessarily based, in the jurisdiction of the USA and numerous accounts are held. The applicable regulatory framework and AML/CFT provisions depends upon which state the payment method is located. However, most of the digital currency services are based outside the USA and are not subject to US law although they can be used by US-citizens. Law enforcement cases have been reported.

# 7. Conclusions and Issues for Further Consideration

The answers provided by countries to the questionnaire that was sent at the beginning of this study, reflected a legitimate market demand served by each of the payment methods analyzed, yet some actual and potential ML and TF vulnerabilities do exist. The FATF 40+9 Recommendations seem to allow for the pursuit of payment system innovation and AML/CFT, since they provide for the needed degree of flexibility in the application of AML/CFT standards to new emerging technology-based payment methods.

Among the main risk factors identified, specifically, this study notes that providers of new payment methods that are located outside the jurisdiction of a given country may pose additional risks compared with domestic service providers, especially when: (i) the distribution channel used is the Internet; (ii) no face-to-face contact with the customer takes place; and (iii) the NPM operates through an open network that can be accessed in a high number of jurisdictions.

The extent to which the new payment methods identified in this study are used for illegitimate purposes is difficult to determine at this time. The responses to the questionnaire issued by the project team provide only a limited number of typologies and show that the level of development and/or awareness of new payment methods is not uniform across the world. In this regard it should be noted that new payment methods are developing quickly and considerably; law enforcement cases may consequently increase as well in the near future.

As previously noted, it is believed that the FATF Forty Recommendations and Nine Special Recommendations provide an appropriate framework to address the vulnerabilities associated with these new methods of payment that have been identified by the project team. However, given the different characteristics and development that new payment methods may have in each jurisdiction, the study does highlight an opportunity for further examination of specific measures that could be adopted by countries to limit identified risks. In the case of new payment methods, technology plays a twofold role: on the one hand, it may increase typical ML/TF risks (i.e. anonymity, global use, speed of transfers, legal arbitrages, offshore provision of services) and on the other hand, help prevent or limit such risks (e.g. usage and spending limits, electronic record of transactions, etc.). Such additional measures could be applied in addition to or instead of traditional AML provisions (for example, CDD could be replaced by spending and loading limits on a payment instrument, which would represent thresholds, or by usage limits – such as non-reloadability or geographic limitations in the use of a payment instrument).

In light of the findings of this project, it is recommended that the WGTM considers the following possible future actions on this topic:

a) Providing guidance to jurisdictions as to what preventive measures may be taken to limit the risk of NPMs being used to launder money and/or finance terrorism (this could occur under FATF Recommendation 8);

b) Updating this study on the development of new payment methods as well as the relative typologies and risks analyses after a period of two years;

c) Proposing the inclusion of new payment methods as a specific issue to be monitored – during the two years period mentioned under letter b) above - under the project on ML and TF trends and indicators.

# Appendix A: Description of Traditional Credit and Debit Card Networks

## Network description

There are at least six global credit card networks: Visa (market leader), MasterCard, American Express, Diners Club, JCB, and Discover. Proprietary credit card networks, which may also be global in scope, also exist for the limited purpose of purchases at associated merchants. In addition, there are a variety of networks that support debit card and ATM transactions: Plus (Visa), Cirrus (MasterCard), Electron (Visa), and Maestro (MasterCard) operate internationally; Interact (Canada), STAR (U.S.), and others operate within one or more countries or regionally within a country. Historically, the card and EFT/POS network services have been somewhat distinct, not only in terms of the differences in credit and debit as products but also in terms of the authorization approach for those products. Credit cards grew from a point-of-sale (POS), charge card model and initially used "off-line" or signature-based authorization approaches. EFT/POS networks grew from an "on-line" or Personal Identification Number (PIN)-based card and dedicated automated teller machine (ATM) model. More recently, particularly in Europe and other regions outside the United States, the use of PINs and chip-based card infrastructures have become common for both credit and debit cards.

## Infrastructure

The supporting infrastructure of the major credit card and EFT/POS networks has been migrating from proprietary networks and platforms to open systems. As these networks annually process billions of electronic payment transactions, the standards and security adopted by these organizations affect the future technology available to the payments industry. The traditional electronic connection between the merchant and the association, and the connection between the banks in the association for the card networks is typically a proprietary one.

The card associations/companies have proprietary, centralized backbone payment networks that connect retail merchants and associations, and banks within the association using special software and hardware. Regional or national EFT/POS networks provide similar access to other financial institutions and the ability to perform ATM and POS transactions. These networks can offer financial institutions a full range of switching (routing), authorization, clearing, and settlement services, including related back-office operations. Others only maintain a switch, relying on third-party processors to handle much of the data processing related to these services. Financial institutions affiliated with these networks may choose among the menu of options offered by these networks.

## Clearing and Settlement

There are three phases within a credit card transaction: authorization of the underlying payment and purchase request, clearing of the accounting entries among the parties, and settlement among the parties in actual funds along with the payment of various interchange and other transaction-related fees.[46] Authorization and clearing of credit and signature-based debit transactions occurs through a "double message" process that involves two separate electronic transmissions; PIN-based debit transactions, by contrast, are "single message" processes in which authorization and clearing occurs during a single transmission. Credit and debit transactions involving PINs and chip-based card infrastructure may follow either of these authorization and clearance routes.

## Credit cards

The first transmission within a credit card or signature debit transaction is the near real-time authorization request at the time of purchase. Payment information from the card and the merchant is sent from the merchant terminal to the acquiring bank and switched to the credit card processing network, which routes it to the issuing bank. The

[46] The exact processes involved in all three phases can vary significantly depending upon the individually negotiated arrangements between member banks and the card networks or the specific characteristics of the transaction and the parties involved. The remainder of this discussion is meant only to provide a general overview of these processes.

issuing bank responds with an "OK," indicating that the customer's credit card account is valid and that the customer has not surpassed his credit limit. The issuing bank then reduces the cardholder's "open-to-buy" credit line balance by the purchase amount. A stand-in processor may also provide the authorization as an alternative to the issuing bank. Certain PIN and chip-based credit cards may operate similarly.

Later in the day (though this may vary as well), either at multiple pre-determined times or once at the end-of-the-day, the merchant initiates a second batch-file clearing message of all the transaction data processed to his acquiring bank since the last such transmission. The acquiring bank reconciles the data against the authorization information. Once reconciled, the acquiring bank posts a credit to the merchant's account for the amount of the transactions, minus a merchant discount fee. The bank transmits a separate file of all merchant transaction data to the credit card association.

Final settlement generally begins with the credit card association using the member banks' aggregated transaction information to compile each member's net settlement position. The credit card association provides this information to members through proprietary settlement software or an "advisement" message that produces an audit trail and converts the data to a format interpretable by the bank. To settle these net positions, each issuing bank in a net debit position (or its correspondent bank) initiates a credit transfer to the credit card association's settlement bank and its special settlement account. The card association retains some of this payment to cover interchange, foreign exchange, or other association fees. The settlement bank then initiates a credit transfer from the settlement account to the acquirer's account with the remaining amount, minus its association fees. Member banks must maintain collateral with the credit card associations' settlement banks in the case of default. Banks can also settle both credit and debit card transactions directly with each other, through regional settlement bank, or by other net settlement arrangements. There can be significant variation in the settlement process depending upon the member involved.

## Signature debit

A signature-based debit transaction is authorized similar to a credit card transaction, except that the issuing bank validates against the cardholder's demand deposit account or a stand-in authorizing system run by the card network. The clearing process is the same as a credit card transaction. Credit and signature-based debit transmissions may be sent separately. Settlement largely occurs in the same fashion as a credit card transaction. Some EFT/POS networks also process signature-based debit transactions with final settlement involving either credit transfers or direct debits. Overall, the card networks view signature-based debit and credit card transactions as almost identical for processing, clearing, and settlement. Certain PIN and chip-based credit cards may operate similarly.

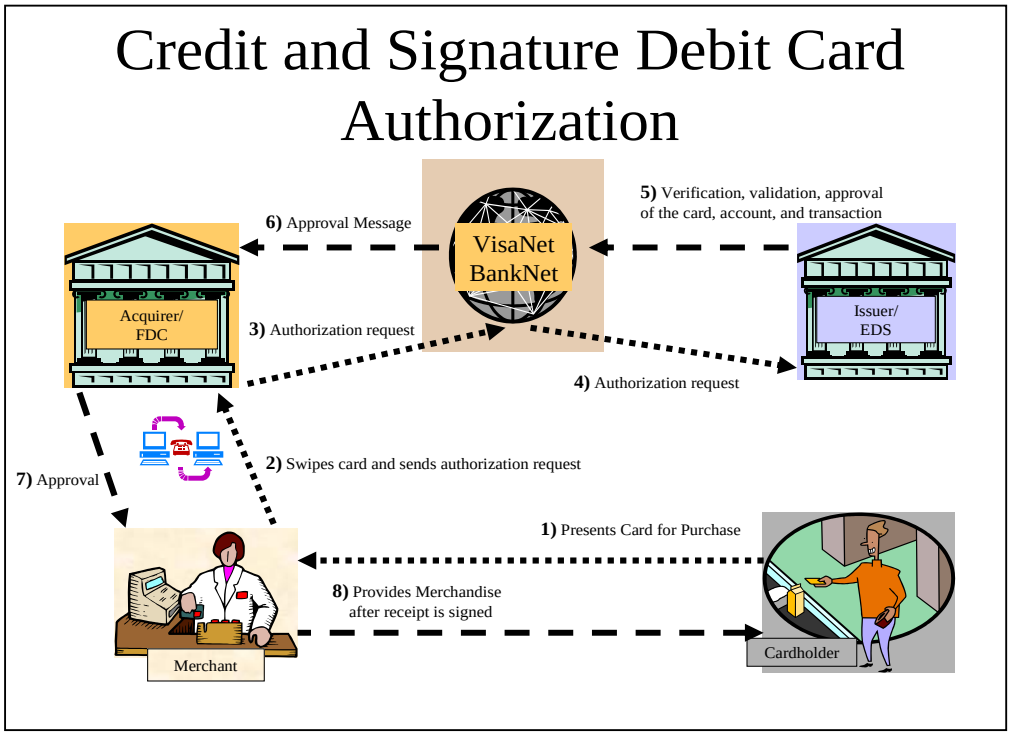



**Figure 7**

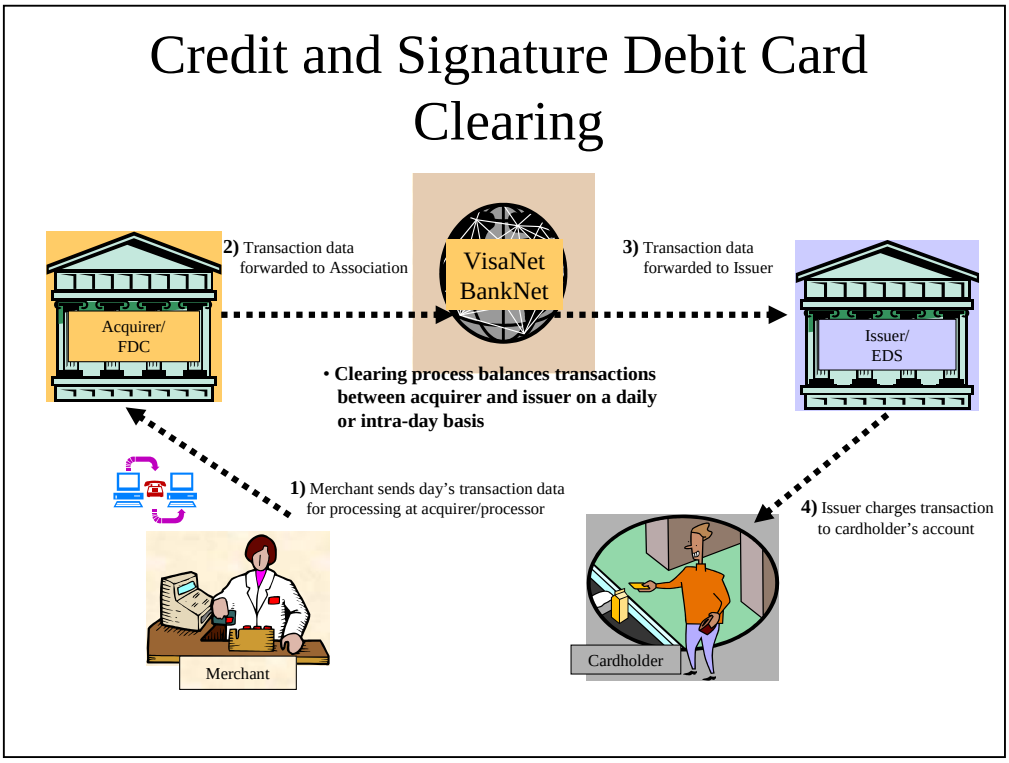



**Figure 8**

## PIN-based debit

In the U.S., the card networks consider PIN-based debit fundamentally different and separate from signature-based debit and credit card transactions. This is not the case in other countries where PINs and chip-based cards are common. For PIN-based debit, the authorization and clearing of the transaction occurs within a single transmission. It can be routed through either an regional EFT/POS network, such as STAR, or a national or international PIN-based debit networks, such as Interact (POS or ATM) or Maestro and Interlink if it is a POS transaction and Cirrus and PLUS if it is an ATM transaction.[47] A stand-in processor may also be used. The authorization process at the issuing bank is the same as the authorization for signature-based debit, save that the consumer must enter a PIN at the merchant terminal or at the ATM. The issuing bank typically debits the cardholder's account immediately as the final amount of the transaction is confirmed at the time of purchase. The acquiring bank or its processor also obtains a full transaction record as a result of the transmission, clearing the transaction between the banks. The acquiring bank typically credits the merchant for the amount of the transaction at that time.

Final settlement among EFT/POS members can occur in a number of different ways, just as it can with the card networks. One way involves book-entry net settlement at the EFT/POS network's chosen settlement bank. Each member bank funds a settlement account at the EFT/POS network's settlement bank. The EFT/POS network and its settlement bank debits and credits the issuing and acquiring members' accounts to finalize the transfer of funds. This includes both the actual transaction amount and any network-related fees. A second option is for members to have their processing agent set up a settlement account at a settlement bank other than the EFT/POS network's or for the member to hold the account. In this case, the EFT/POS network originates a direct debit of the issuing member's settlement account (authorization for this is given as part of the requirements of network membership) to credit the acquiring member's account (or the EFT/POS network's settlement account at

[47] Where transactions can flow over either regional, national, or international EFT/POS networks, the regional network normally take precedence according to their regional routing rules. However, the merchant and acquiring bank may be able to prioritize that routing order to some extent.

its settlement bank in the case of network fees). Depending upon the EFT/POS network, the daily settlement process may include just the individual transaction amounts or there may be separate settlements of the day's transactions and their associated network fees. Some EFT/POS networks will delay the settlement of the network fees until the end of the month.

Alternatively, if the transaction flows through a card network, the clearing among the banks and the national network occurs later, through a similar net settlement process as that used with signature-based debit and credit card transactions. Settlement may use traditional national direct debit or credit transfer systems. Settlement is based on the issuing bank's positive response to the authorization request. The issuer rather than the acquirer pays the network interchange fees for PIN-based ATM transactions.

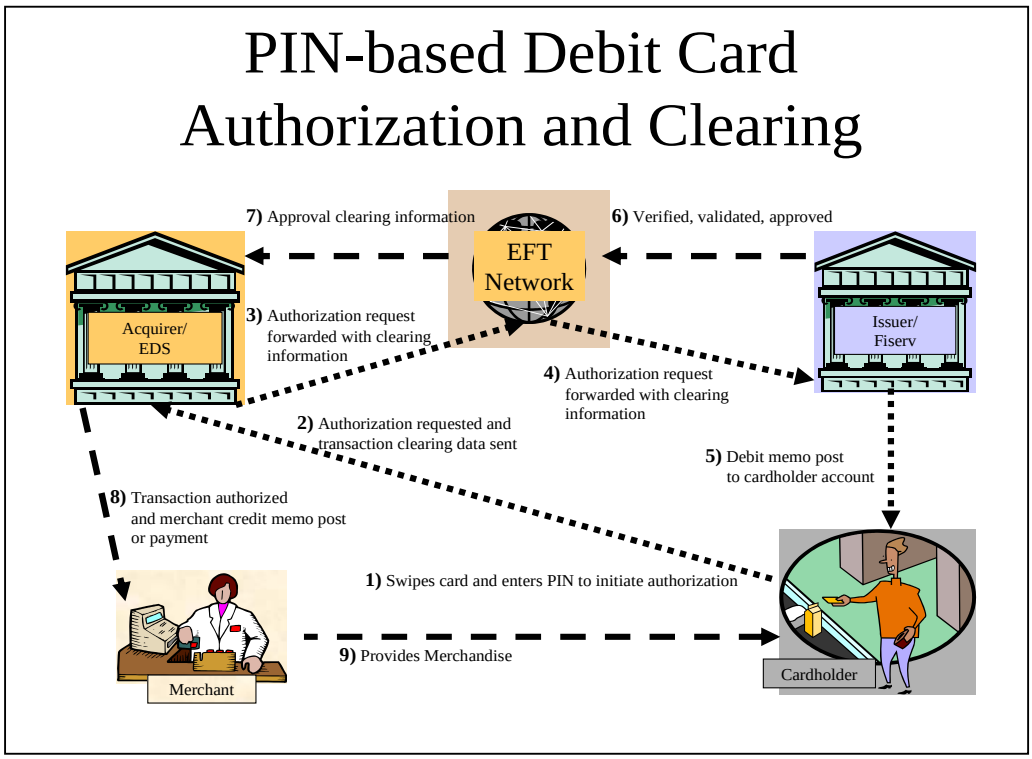



**Figure 9**

# Appendix B: Supplemental NPM Questionnaire Results and Analysis

Table A: Short description of the NPM.

Table B: The two main indicators for market size are the estimated number of domestic service providers and the estimated number of accounts held or cards issued.

Table C: Information on regulatory provisions. The distinction between registration (R) and licensing (L) is noted. The main difference between these two categories is that licensing pre-supposes authorization to provide payment services (subject to conditions such as prudential rules, etc), whereas registration is not subject to conditions. As regards supervision, different approaches are also possible, and whenever detailed information is provided, it is reported under "additional information".

Table D: AML/CFT provisions can derive from regulations in place or from business practice (a typical example of business practice being limits to transferred amounts).

Table E: Reports of AML/CFT cases or if any illegal operators have been found (illegal operator means those which are not registered or licensed).

## Prepaid or prepaid payment cards

A. Description of the NPM

| Countries | Short description of the NPM |
|---|---|
| Ireland (IE) | "Virtual visa voucher" – offered by permanent TSB bank in association with Visa and 3V transaction services – available since September 2005 – customer registers online, voucher is printed upon request at a participating retailer, and a "disposable" pre-paid card is issued; this card can be used to purchase goods on the internet or by mail/telephone order. |
| Turkey (TR) | "Pre-paid debit cards" are mentioned, but no detailed information is provided. |
| Lebanon (LB) | Prepaid cards are mentioned but insufficient information is provided (e.g. in relation to Visa/ Mastercard branded networks)- "Liters plus" referred as limited-purpose pre-paid card) |
| Palau (PA) | Reference to pre-paid debit cards that can be used in ATM networks, no additional information is provided. |
| Lithuania (LT) | Reference to pre-paid debit cards issued by banks or shops, but no detailed information is provided. |
| New Zealand (NZ) | "Visa Cash passport" (available for purchase in NZ and for ATM cash withdrawal in NZ and overseas); other store-value cards used in NZ for purchases in closed systems (transport operators, educational institutions, etc.) |
| Cyprus (CY) | Pre-paid card issued by a bank; it can be used at venues where Visa electron is accepted and for internet payments; the information is limited |
| Czech Republic (CZ) | E-tickets for the payment of public transport; this service is not cross-border. |

| | |
|---|---|
| Italy (IT) | Rechargeable prepaid cards require full CDD, and AML provisions fully apply. Prepaid cards that may not be recharged may not exceed the amount of 500 EUR and do not require CDD to be applied, they may thus be anonymous. Such cards are issued by financial institutions (i.e. banks and e-money institutions). In some cases the customer originally holds a credit with a telephone company (the card is at this stage a telephone card) and then converts such credit into a credit with a financial institutions which is legally the prepaid card issuer (at this stage the card is a payment instrument). |
| Austria (AT) | Pre-paid debit cards (2 systems) which do not require a bank account and which can be used for cash withdrawals at an ATM or for purchases at a point of sale; funding methods include cash and credit transfers. No information on market size. |
| USA | Different types of prepaid cards are identified, covering a variety of uses and technologies, both operating within either an "open" or "closed" system. |
| Spain (ES) | Hal-Cash; it is based on a pre-paid account which allows ATM cash withdrawal cross-border; mobile phone is issued as an access device and as a messaging system; this product is mainly offered to un-banked, immigrant populations. |
| Switzerland (CH) | A pre-paid multi-purpose debit card. Micro-payments can be made through the internet and/or mobile phone by online merchants. Users scratch off a panel on the card to access a code which corresponds to their pre-paid credit amount. When executing the payment of products or services ordered over the internet or by means of a mobile phone, users have to indicate the card's code, which gives access to the pre-paid account held in the issuer's server. The amount is then deducted from the actual card balance. |

B. Market size

| Estimated number of Domestic Service Providers | | Estimated number of Accounts Held Cards Issued | |
|---|---|---|---|
| ≤ 3 | > 3 | ≤ 1000 | > 1000 |
| IT,IE, PA, NZ, CH | CZ, USA, ES | NZ (per anum) | CZ, IT, USA |

C. Access to activity

| Registration/Licensing | | Supervision | | Additional information |
|---|---|---|---|---|
| Yes | No | Yes | No | |
| AT, CZ, IT, IE(L), LB (L), CH | PA, NZ, HK, ES (?), USA | IE, LB, AT, CZ, IT, CH | PA, NZ, HK, ES (?) | IE, LB: providers are banks. |

D. AML/CFT Provisions

| Customer Due Diligence | | Record-keeping | | Suspicious Transaction Reporting | | Other AML Policies & Procedures | | Limit to transferred amount if any | |
|---|---|---|---|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No | Yes | No | ≤ 500 | > 500 |
| AT, IT IE, LB, PA, NZ, CH | DE, IT, USA, HK, ES | IE, LB, PA, NZ, IT, AT, USA, CH | IT , HK, ES | IE, LB, PA, NZ, AT, IT, CH | USA, HK, ES | IE, LB, PA, AT, IT, USA, CH | NZ, HK, ES | AT, CZ, IT, IE(350), LB, NZ (25.000 NZ$); NZ yes but depends on ATM network | USA, ES, PA no limit |

E. AML/CFT Cases - illegal operators

| Evidence of Money Laundering | | Examples of Law Enforcement | | Illegal Operators | |
|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No |
| NZ | AT, CZ, IT, USA, IE, LB, ES, CH | USA, NZ | AT, CZ, IT, IE, LB, ES, CH | | AT, CZ, IT, USA, IE, LB, NZ, ES, CH |

## Payments initiated by means of a mobile phone (and linked to a bank-account)

A. Description of the NPM

| Countries | Short description of the NPM |
|---|---|
| Finland (FI) | "Mobiiliraha" – linked to a bank account; no detailed information is provided. |
| New Zealand (NZ) | Mobile phone banking, meaning access to a bank account by means of a mobile phone device. |
| China (CN) | Mobile phone banking, meaning access to a bank account by means of a mobile phone device. |
| Korea (KO) | The use of mobile phones or PDA's for cross-border payments from a bank-account to a (foreign) bank-account. |

B. Market size

| Estimated number of Domestic Service Providers | | Estimated number of Accounts Held Cards Issued | |
|---|---|---|---|
| ≤ 3 | > 3 | ≤ 1000 | > 1000 |
| | KO, FR | | KO |

C. Access to activity

| Registration/Licensing | | Supervision | | Additional information |
|---|---|---|---|---|
| Yes | No | Yes | No | |
| KO, FI, NZ, CN, FR | | KO , FI, NZ, CN, FR | | |

D. AML/CFT Provisions

| Customer Due Diligence | | Recordkeeping | | Suspicious Transaction Reporting | | Other AML Policies & Procedures | | Limit to transferred amount if any | |
|---|---|---|---|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No | Yes | No | ≤ 500 | > 500 |
| KO, FI, NZ, CN | | KO, FI, NZ, CN | | KO, FI, NZ, CN | | KO, FI, NZ, CN | | | KO |

E. AML/CFT Cases - illegal operators

| Evidence of Money Laundering | | Examples of Law Enforcement | | Illegal Operators | |
|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No |
| | KO, FI, FR | | KO, FI, FR | | KO, FI, FR |

## E-purse

A. Description of the NPM

| Countries | Short description of the NPM |
|---|---|
| Germany (DE) | Geldkarte: The funds of the card are on the card itself; in general, the funds are loaded from a bank account and no online connection and no cardholder identification are needed to make a payment; this card has almost no cross-border |

| | |
|---|---|
| | operability. Geldkarte is actually a common technological standard for chipcards; many banks issue their own Geldkarte cards. However, as all these cards are fully inter-operable, for the purpose of this report Geldkarte can be considered as a singular payment instrument. |
| Netherlands (NL) | Chipknip: The money is loaded from a bank-account and can be used as an independent electronic purse. |
| Switzerland (CH) | CASH system: The money is loaded form a bank-account and can be used as an independent electronic purse. |

B. Market size

| Estimated number of Domestic Service Providers | | Estimated number of Accounts Held Cards Issued | |
|---|---|---|---|
| ≤ 3 | > 3 | ≤ 1000 | > 1000 |
| DE, NL | CH | | DE, NL, CH |

C. Access to activity

| Registration/Licensing | | Supervision | | Additional information |
|---|---|---|---|---|
| Yes | No | Yes | No | |
| DE, NL, CH | | DE, NL, CH | | |

D. AML/CFT Provisions

| Customer Due Diligence | | Recordkeeping | | Suspicious Transaction Reporting | | Other AML Policies & Procedures | | Limit to transferred amount if any | |
|---|---|---|---|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No | Yes | No | ≤ 500 | > 500 |
| CH, NL, | DE[48], | CH, DE, NL | | CH, DE, NL | | CH, DE, NL | | DE, NL, CH | |

E. AML/CFT Cases / illegal operators

| Evidence of Money Laundering | | Examples of Law Enforcement | | Illegal Operators | |
|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No |

[48] In Germany, e-purses can be legally issued only by credit institutions which are subject to full AML policies and procedures with only one exception: due to the low loading limit, customer identification/CDD is not deemed necessary.

| | | | | | |
|---|---|---|---|---|---|
| | DE, NL, CH | | DE, NL, CH | | DE, NL, CH |

## Internet payments

A. Description of the NPM

| Countries | Short description of the NPM |
|---|---|
| Canada (CA) | Many providers, including offshore. |
| Belgium (BE) | Paypal (which is regulated by the FSA in the UK, and provides its services in Belgium under the license of e-money institutions granted by the UK's FSA, which provides for the possibility to operate all across the EU). It is therefore not under Belgian, but UK's supervision. |
| Finland (FI) | "Digiraha" described as “digital purse for internet payments”. No detailed information. |
| Estonia (ET) | Fogott, Paypal, Netteller- no detailed information is provided. |
| New Zealand (NZ) | Paypal |
| Austria (AT) | Emerging server-based system for purchases on the Internet. |
| China (CN) | Different emerging e-business enterprises and third party intermediaries are providing their own business and online payment intermediaries. |
| Czech Republic (CZ) | Internet shopping; the user has a virtual account on the website and the provider debits this account at the moment of purchase; limited information is provided. |
| France (FR) | Neosurf: customer exchanges funds for a scratch card (of various amounts), which gives a code to pay on the internet. This system is active in France, Belgium and Switzerland. |
| Germany (DE) | Paypal (which is regulated by the FSA in the UK, and provides its services in Germany under the license of e-money institutions granted by the UK's FSA, which provides for the possibility to operate all across the EU). It is therefore not under German, but UK's supervision. |
| Indonesia (ID) | Online payment for on-line merchants and person-to-person money transmission; the services can be used for local and cross-border payments; these payment methods are still under construction and do not operate yet. |
| Italy (IT) | 1) Moneta On Line: This is a scratch card issued by a bank to make low-value purchases over the internet at merchants adhering to the VISA circuit; the users are not identified;<br>2) BankPass Web: This is an electronic wallet to pay on the internet. |
| Netherlands (NL) | Several providers, including Paypal |
| Spain (ES) | 1) Paypal: Spain seems to have imposed stricter AML/CFT provisions on |

| | |
|---|---|
| | Paypal than Germany and the Netherlands.<br>2) Click & Buy: This is an internet billing mechanism for enterprises; it can be used to buy at merchants in different parts of the world. |
| Switzerland (CH) | Click and buy micro-payments through the internet at online merchants other than the issuer of the card. |
| USA | There are several domestic online payment services, including PayPal, and others offshore that access the U.S. market. |

B. Market size

| Estimated number of Domestic Service Providers | | Estimated number of Accounts Held Cards Issued | |
|---|---|---|---|
| ≤ 3 | > 3 | ≤ 1000 | > 1000 |
| CZ, FR, DE, ID, ES(1), ES(2), CH, BE | NL, IT, USA, CA | CZ, ES(1) | NL, FR, DE, USA |

C. Access to activity

| Registration/Licensing | | Supervision | | Additional information |
|---|---|---|---|---|
| Yes | No | Yes | No | |
| AT, GE, ID, IT, NL, ES(1), CH, USA, BE | CN, ES(2), NZ, CA, ET | AT, DE, ID, IT, NL, ES(1), CH, CA (for AML purposes), USA, BE | CN, ES(2), NZ, ET | CN is working on regulation- ET will soon enforce the EU e-money Directive. |

D. AML/CFT Provisions

| Customer Due Diligence | | Recordkeeping | | Suspicious Transaction Reporting | | Other AML Policies & Procedures | | Limit to transferred amount if any | |
|---|---|---|---|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No | Yes | No | ≤ 500 | > 500 |
| AT, ID, IT, ES(1), CH, USA, NZ, CA, ET, DE, BE | CN, NL,ES(2) | AT, ID, USA, IT, ES(1), CH, USA, NZ, CA, ET, DE, BE, NL | CN, ES(2) | AT, ID, IT, ES(1), CH, USA, NZ, CA, ET, DE, | CN, ES(2) | AT, ID, IT, ES(1), CH, USA, CA, DE, BE | CN, NL, ES(2), NZ, ET | AT, FR, CH, CA (has a limit, but amount depends on business practice) | DE, IT, NL, ES(1), ES(2), CN |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | BE, NL | | | | | |

E. AML/CFT Cases - illegal operators

| Evidence of Money Laundering | | Examples of Law Enforcement | | Illegal Operators | |
|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No |
| CN, ET, CA, USA | AT, FR, DE, ID, IT, NL, ES(1), ES(2), CH, NZ, BE | USA, ET, CA | AT, CN, FR, DE, ID, IT, NL, ES(1), ES(2), CH, NZ, BE | CN, ID, USA | AT, FR, DE, IT, NL, ES(1), ES(2), CH, BE |

## Mobile Payments

A. Description of the NPM

| Countries | Short description of the NPM |
|---|---|
| France (FR) | Post-paid and pre-paid payment service are offered by telephone companies. |
| Belgium (BE) | Mobile payments (SIM reload only) are estimated to be available in Belgium on a reduced scale for at least 2 years. |
| Lithuania (LT) | Information provided suggests use of mobile phones to pay for limited purposes (parking, tickets for concerts or other events) from prepaid balance or mobile phone bill; but no detailed information is provided. |
| Germany (DE) | 1) Crandy is a pre-paid mobile payments system, which allows person-to-person transfers and payments at POS; funds can be transferred from a bank account.<br>2) Pre-paid scratch cards for payment by mobile phone |
| Netherlands (NL) | Payment services by telephone company for payments using a mobile phone (for example for purchasing of ring-tones). |

B. Market size

| Estimated number of Domestic Service Providers | | Estimated number of Accounts Held Cards Issued | |
|---|---|---|---|
| ≤ 3 | > 3 | ≤ 1000 | > 1000 |
| | FR, DE, NL | | FR, DE, NL |

C. Access to activity

| Registration/Licensing | | Supervision | | Additional information |
|---|---|---|---|---|
| Yes | No | Yes | No | |
| DE (L) | NL | DE | NL | |

D. AML/CFT Provisions

| Customer Due Diligence | | Recordkeeping | | Suspicious Transaction Reporting | | Other AML Policies & Procedures | | Limit to transferred amount if any | |
|---|---|---|---|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No | Yes | No | ≤ 500 | > 500 |
| | NL, DE, BE | DE, BE (but not required by Law) | NL | DE | NL, BE | DE | NL, BE | DE, NL,BE (fixed by the telecom operator) | |

E. AML/CFT Cases - illegal operators

| Evidence of Money Laundering | | Examples of Law Enforcement | | Illegal Operators | |
|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No |
| | FR, DE, BE | | FR, DE | | FR, DE |

## Digital precious metals

A. Description of the NPM

| Countries | Short description of the NPM |
|---|---|
| Estonia (ET) | "Icegold" No detailed information is provided. |
| USA | A number of digital precious metals dealers are accessible online. Funding accounting and withdrawing funds is accomplished through “an exchange service.” Each exchange service sets its own terms as to how it is willing to receive and remit funds. Some may only accept transfers from bank or credit card accounts, while others will accept cash and money orders. |

B. Market size

| Estimated number of Domestic Service Providers | | Estimated number of Accounts Held Cards Issued | |
|---|---|---|---|
| ≤ 3 | > 3 | ≤ 1000 | > 1000 |
| ET | USA | | USA |

C. Access to activity

| Registration/Licensing | | Supervision | | Additional information |
|---|---|---|---|---|
| Yes | No | Yes | No | |
| USA | | USA | | In the United States, money transmitters are among money services businesses that are required to register with the FIU (FinCEN), they<br>also are subject to AML reporting and recordkeeping requirements and are often required to be licensed on the state level. Whether an online payment system or digital precious metals dealer meets the definition of a money transmitter pursuant to the relevant regulations, though, depends upon its location and the ways in which it participates in or conducts transactions. Many online payment systems are based outside the United States and are not subject to U.S. jurisdiction. |

D. AML/CFT Provisions

| Customer Due Diligence | | Recordkeeping | | Suspicious Transaction Reporting | | Other AML Policies & Procedures | | Limit to transferred amount if any | |
|---|---|---|---|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No | Yes | No | ≤ 500 | > 500 |
| | USA | USA | | | USA | | USA | USA: established by each issuer | USA: established by each issuer |

E. AML/CFT Cases - illegal operators

| Evidence of Money Laundering | | Examples of Law Enforcement | | Illegal Operators | |
|---|---|---|---|---|---|
| Yes | No | Yes | No | Yes | No |
| USA | | USA | | USA: offshore | |