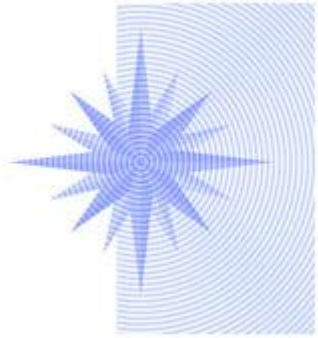
the Wolfsberg Group



Banco Santander
Bank of Tokyo Mitsubishi-UFJ
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
JP Morgan Chase
Societe Generale
UBS

Wolfsberg Guidance on Mobile and Internet Payment Services (MIPS)[1]

1. Preamble

The Wolfsberg Group of International Financial Institutions (the "Wolfsberg Group") has published global anti-money laundering (AML) guidance, statements and principles on a number of topics, including Private Banking, Correspondent Banking, the Suppression of Terrorist Financing, and the Risk Based Approach.

This paper considers the money laundering risks and mitigants of Mobile and Internet Payment Services (MIPS), and supplements the Wolfsberg Group Statements on Credit/Charge Card Issuing and Merchant Acquiring Activities, and on Prepaid and Stored Value Cards.

The Wolfsberg Group believes that adherence to these publications promotes effective AML risk management and furthers the goal of the Wolfsberg Group members to endeavour to prevent the use of their institutions for criminal purposes.

2. Background

As part of the continuing development and use of what the Financial Action Task Force (FATF) referred to as New Payment Methods (NPMs) in its Reports dated October 2006, October 2010 and February 2013, it is recognised that there is a growing demand in the marketplace, and in financial institutions, for migration from paper based payments to MIPS. It is recognised that MIPS are powerful tools in support of financial inclusion, which will result in further and more dynamic expansion of the market for products of this nature.

The broadening of non-traditional payment methods of this nature has resulted in greater complexity for regulators, and for financial institutions, in relation to assessing the

[1] This paper was written with the collaboration of American Express and PayPal

corresponding risks and the application of, and responsibility for, AML controls, particularly if the transactions flow through one or more jurisdictions and involve multiple service providers.

An important aspect when considering MIPS is that these products/applications are distributed by a much wider range of service providers, including non-bank service providers (NBSPs), than the more traditional payment methods via banks or credit/charge cards. The segmentation of services between numerous and varied parties involved in MIPS adds additional complexity and potential risks.

2.1 Non-Bank Service Providers (NBSPs)

NBSPs act in a variety of capacities in relation to both consumers and financial institutions. NBSPs may support financial institutions by way of the provision of outsourced specialist services, act as partners to financial institutions or use the services of financial institutions as part of a NPM business proposition, or indeed, act as competitors to financial institutions.

NBSPs may not be regulated, or:

- they may be regulated to a lower standard than financial institutions
- they may be domiciled in a jurisdiction whose regulatory regime may not meet international standards
- they may be regulated to the same standard as financial institutions for one specific product/line of business
- they may be only regulated for business in a specific country/countries
- they may be regulated in a different country than that where a product is offered

3. Scope

3.1 This paper considers the potential money laundering vulnerabilities of MIPS and provides guidance on managing these risks as part of a comprehensive AML programme.

3.2 Although the prime focus of this paper is AML, the application of appropriate AML customer identification procedures or appropriate AML mitigants to customer acceptance and ongoing due diligence (including checking against applicable terrorist and sanctions lists issued by Competent Authorities) may assist in preventing individuals and entities listed by Competent Authorities from accessing MIPS.

3.3 Although this paper does not specifically consider the traditional fraud-related threats associated with MIPS, many risk indicators associated with actual or potential fraud are relevant to the prevention of money laundering.

It should be noted that a customer's mobile and Internet access to their traditional pre-existing bank account is out of the scope of this Guidance paper, as normal customer due diligence will have been followed by the bank, and the use of mobile phone and/or Internet is merely an access point to that account.

4. Definition of Mobile and Internet Payment Services (MIPS)

For the purposes of this guidance, MIPS are considered to be new and innovative payment products and services which involve different ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as products that do not rely on traditional systems to transfer value between individuals or organisations.

One example of MIPS is using a mobile phone to perform basic payment services without a traditional bank account. This is prevalent in developing countries with low banking penetration and high mobile phone penetration. Examples are SMARTMoney in the Philippines and M-Pesa in Kenya.

Business models vary based on which service provider has the lead role, whether the service is pre-paid or post-paid and which technical platform is used. In terms of technology used, business models may use text messaging and/or mobile Internet access and/or near field communication (NFC) and/or programmed subscriber identity module (SIM) cards to facilitate MIPS.

5. The usage of MIPS

The common theme of these products and services is that they are convenient, easy to use and perform a particular function. While they may be used by those with access to traditional banking services, they also have broad appeal to parts of the community without access to traditional bank accounts.

The following are some of the typical uses:

- money transmission and payment of bills by individuals and small businesses (domestic and/or cross-border)
- micro payments for low value repetitive goods and services (*e.g.* mass transit)
- Person to Person (P2P) transmissions between related and/or unrelated parties (domestic and/or cross-border)
- purchase of goods and services (physical and digital)
- fundraising by charities/non-profit organisations

6. Roles in MIPS operations

- **Network Operator:** providing the technical platform to allow access to funds
- **Distributor**: selling, or arranging for the issuance of, funds
- **Electronic money issuer**: the issuer of the value placed on a payment device, such as mobile phone or computer system, or a non-traditional account with either a banking or non-banking entity
- **Electronic remitter**: initiating the communication of a transfer of value
- **Electronic-money agent**: acting on behalf of electronic or e-money institutions (banks or non-bank entities) in the distribution or redemption of e-money[2]

A single party can perform one, or more, of these roles.

7. Types of MIPS Arrangements and Features

7.1 Closed Loop

- these are typically used only at specific retailers/outlets, or within a defined segment such as a public transport system or a university campus.

7.2 Open Loop

- these are typically issued by schemes/networks and can be used at multiple retailers/outlets within the network.

7.3 Principal features of both Closed Loop and Open Loop arrangements

- funded by known (*i.e.* pre-determined/traceable) source(s) or funded by unknown source(s)
- reloadable or non-reloadable
- limited to low monetary value or of high monetary value

[2] As defined by the European Commission, "Electronic money is a digital equivalent of cash, stored on an electronic device or remotely at a server. One common type of e-money is the 'electronic purse', where users store relatively small amounts of money on their payment card or other smart card, to use for making small payments. E-money can also be stored on (and used via) mobile phones or in a payment account on the internet".

8. MIPS Risk Factors

8.1 Introduction

When the general characteristics of MIPS outlined below are present in a service offering, then they have the potential to increase money laundering risk unless there are appropriate controls in place to mitigate this risk:

- ability to transfer funds (domestically and/or internationally)
- speed of transfer of funds
- lack of, or difficulty in providing, an audit trail
- lack of, or difficulty in compiling, an aggregated view of multiple transactions
- lack of face to face contact
- identification means either not taken, or taken and not verified
- the ability to reload
- ability to load/reload with cash
- ability to withdraw cash
- ability to load/ transfer from alternative funding sources

It is important, however, to note that the above risks can be managed and mitigated by appropriate service features and controls.

The analysis of these features, and other factors (by reference to their number and materiality), in combination will assist in determining an appropriate view of the potential money laundering risks, and drive the degree to which AML risk management processes and controls can be applied to the service in order to mitigate those risks.

The MIPS features to consider in assessing an appropriate view of risk, include, but are not limited to:

8.1.1 **Intended geographical scope of the MIPS**

Factors that may decrease risk

- Geographical restrictions on the use of MIPS, such as limiting the use to one particular jurisdiction or to specified jurisdictions.

- Restricting the value/volume of transactions within specific jurisdictions, based on higher risk for money laundering (it should be noted that restricting the value/volume may not decrease TF or sanctions risk).

Factors that may increase risk

- MIPS that have no geographical restrictions or limitations

- MIPS that can be used to transact in jurisdictions considered to be a higher risk for money laundering or terrorist financing, or those that have minimal or non-existent AML laws

8.1.2 **Intended usages of the MIPS**

Factors that may decrease risk

- Restricting transmission of value to specified third party beneficiaries.

- Restricting the value of transactions (may not decrease TF and Sanctions risk).

- Requiring ID and/or Verification.

Factors that may increase risk

- MIPS that have limited or no ability to restrict or control activity.

- High frequency of usage.

8.1.3 **Knowledge about MIPS users**

Factors that may decrease risk

- The collection, availability and (in some circumstances) verification of information related to MIPS users, (*e.g.* name, address, date of birth, unique government-issued

identification number [tax identifier, passport, driver's licence]) allows identification and also screening against Competent Authority lists.

Factors that may increase risk

- Lack of relevant information about the MIPS user (*e.g.* name, address, date of birth, unique government-issued identification number [tax identifier, passport, driver's licence]).

- Lack of relevant information about parties involved with the service.

8.1.4 **Intended scope of MIPS (open/closed loop)**

Factors that may decrease risk

- Limitations on the use of the MIPS to one or a limited number of merchants, or the inability to use the service for higher risk activities (*e.g.* the use restricted to targeted merchant types).

- Transaction/frequency limits on use or reloadability

- Restricting usage to one off event (*e.g.* major sporting tournament).

Factors that may increase risk

- MIPS which have no restrictions on nature and/or place of use or transaction/frequency limits on use or reloadability.

8.1.5 **Source of funding**

- **General**

Factors that may decrease risk

- A known source of funds, such as a transfer from an existing financial institution account of the purchaser or receiving funds from a known, trusted source, such as a government agency (subject to country risk assessment).

- MIPS for which review and controls on locations where the funding can be undertaken are in place, as appropriate, for the relevant arrangement.

Factors that may increase risk

- Unknown sources of funding of the MIPS, such as cash (without other controls that may limit the anonymous nature of cash) or other monetary instruments that

provide anonymity as to the source or owner of the funds, or by means of a funds transfer from an unknown third party by alternative funding sources.

- **Cash**

Factors that may decrease risk

- MIPS where value cannot be funded with cash, due to the inability to use cash funding as a means of transforming physical currency into electronic currency.

- MIPS in which cash loading is limited to a specific amount, where ID is required at the time of loading, or where other mitigants are employed.

Factors that may increase risk

- The ability to add value, initially and on an ongoing basis to MIPS using cash or cash vouchers sold by retailers, due to difficulties in determining the legitimacy of the source of the cash.

- **Value transfer**

Factors that may decrease risk

- MIPS that do not allow for value transfers between unrelated persons.

- MIPS that cannot be reloaded online by value transfer.

Factors that may increase risk

- MIPS that allow for value transfers between unrelated persons, or involving value transfers with other payment services.

- MIPS that can be reloaded online by value transfer.

8.1.6 **Value limits**

Factors that may decrease risk

Potential MIPS value can be controlled by service features such as:

- a maximum amount of funds that can be loaded in any instance

- a maximum amount of total value that can be held at any given time (ceiling limit) and,

- the number of times, or total value with which a payment service can be reloaded in a given period. These features may be applied singly or in combination.

Factors that may increase risk

- MIPS that either have a high maximum load value or unrestricted reloading capabilities or both combined.

8.1.7 **Cash withdrawal via automated teller machines (ATM)/Cash redemption of monetary value.**

Factors that may decrease risk

- MIPS that cannot be used to withdraw cash from an ATM or other access points.

Factors that may increase risk

- Cash access from a MIPS, such as through withdrawals from ATM or other access points, will increase the potential that the service will be used for money laundering purposes, as will the ability to redeem the value associated with a payment service for cash. It should be noted, however, that for some services, withdrawing cash via an ATM could be considered entirely consistent with anticipated use.

- In several jurisdictions, merchants' points of sale may be used to withdraw cash by overpaying for merchandise and receiving the overpaid amount in cash (known as cashback) or paying for merchandise and receiving the refund in cash or in a monetary instrument (anonymous prepaid card).

- MIPS that permit international value transfers among service providers (system "credits" assigned a value), with subsequent cash payout by one of the providers for a user in national currency.

8.1.8 **Value Term Limit**

Factors that may decrease risk

- Establishing a fixed expiry date (e.g. one year) after which the service will not retain its value.

Factors that may increase risk

- No expiry date, or long expiry date for the service.

8.1.9 **MIPs KYC/CDD requirements for service activation**

Factors that may decrease risk

- Registration of MIPS with a unique customer identifier for service activation as part of KYC/CDD.

- Monitoring against identifiers obtained at registration.

Factors that may increase risk

- Unlimited MIPS may be purchased, used or activated by a single MIPS account holder without provision of sufficient unique KYC identifiers.

9. **AML Framework**

9.1 **Product Design**

It is essential that the Compliance function is a stakeholder during design, overall specification and functionality of individual MIPS, alongside Business Development, Marketing (including sales channel and mode of distribution), Credit Risk and Fraud, as appropriate. It is also important that the Financial Institution's and/or other parties' Compliance functions should remain independent.

It is essential that the evaluation and approval process for new products and services, or for significant changes to existing products and services, considers the relevant money laundering vulnerabilities and risks, plus those of terrorist financing and sanctions and that one or more parties in the process take responsibility for the compliance aspects.

9.2 **AML controls**

The specific MIPS structure and possibilities for usage must be understood in order to identify and mitigate AML risk. The AML controls will reflect an accumulated view of the number and materiality of the various applicable AML risks. Depending on the inherent limitations and risk mitigants of any given MIPS, some require very few specific AML controls, whereas others require a greater number of controls.

9.2.1 **Due Diligence on service users**

- **Identification and Verification (ID&V)**

Low risk propositions

- No ID&V required for MIPS user

- No change in patterns over time

Medium risk propositions

- Identification of the MIPS user is required (such as the capture of name, address, date of birth, unique issued government identification or other as required by jurisdiction/region/type of regulation).

- Verification of the name and address is required. Reliance may be placed on a trusted third party to achieve this. (*e.g.* a government agency held list of service users who are benefit claimers).

Higher risk propositions

- Identification of the MIPS user is required, plus additional data elements (such as mobile phone number and SIM card serial number, or other as required by jurisdiction/region/type of regulation) to reflect increased risk of money laundering, terrorist financing and sanctions activity.

- Verification of the name and address (and other data elements as required by jurisdiction/region) is required. This should be in line with government or industry guidelines.

- **Screening**

Low risk propositions

- No sanctions screening of MIPS users (but may be required depending on the region/jurisdiction requirements, and the geographic limitations/risk of the service proposition).

Medium risk propositions

- Sanctions screening of the MIPS users should take place, before the account/service is opened and during the lifetime of the service.

Higher risk propositions

- Sanctions screening of the MIPS users should take place, before the account/service is opened and during the lifetime of the service.

9.2.2 **Due Diligence on parties involved in a service proposition**

MIPS can be more exposed to risks where several parties are involved in performing the service jointly, such as programme managers, distributors and other types of intermediaries or agents.

The number of these parties generates potential risks of segmentation and loss of information. This may be exacerbated if important services are outsourced to potentially unregulated third parties without clear lines of accountability and oversight, or which are located abroad. Additionally, limitations may be placed on the exportation of MIPS data beyond country borders for processing or data storage.

Providers often use agents, not only for cash acceptance and cash withdrawals, but also to establish new customer relationships.

All partners in the service should be subject to appropriate risk-based due diligence, in accordance with industry/government requirements and screening of MIPS partner(s) is recommended in accordance with industry/government requirements to ensure they, or the beneficial owners, are not on relevant sanctions lists.

9.2.3 **Transaction Monitoring**

MIPS activity monitoring frameworks should be developed and continue to evolve following an analysis of the particular service features and attributes, including range of use and maximum load value. New patterns and trends of activity must be identified based on the particular features and attributes of this product class and client use, adjusting scenarios and thresholds periodically based on analytics of product use in the market. Monitoring could possibly include unusual service use against such aspects as high-value use, high-volume use or loading frequency or unexpected geographical use.

- **Funding**

For reloadable MIPS that are only funded from a specified source of funding (*e.g.* a government entity or listed corporation), monitoring the load channel for reloading from unauthorized sources is a key control element, as it gives the issuer confidence that the funds being loaded onto these lower risk services remain known.

- **Usage**:

  - unusual level and frequency of ATM usage
  - unusually high value/volume payment service activity
  - unusually high velocity payment service activity
  - identifying patterns of high cash activity
  - MIPS usage in unexpected or high risk countries

- identifying patterns related to typologies

The nature and level of monitoring should be designed by reference to the MIPS features and any other risk factors.

- **Issuance**

Appropriate monitoring should be implemented at each stage of the payment chain to ensure that MIPS limits are not breached.

9.2.4 **Record Keeping**

Transaction records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity and support for law enforcement investigations.

Law enforcement agencies have reported investigative cases where providers had not kept records of IP addresses at all, or not sufficiently, or had deleted them before law enforcement agencies could access them, thus impeding criminal prosecution.

As a general guideline based on FATF Recommendation 10, financial institutions should maintain identification data as well as transaction records for at least five years; however financial institutions must assess the specific requirements of the jurisdictions in which they operate to determine if a longer retention period is required.

9.2.5 **Suspicious Transaction Reporting**

Generally, if a financial institution or NBSP suspects, or has reasonable grounds to suspect, that funds are the proceeds of a criminal activity, or are related to terrorist financing, laws or regulations in many jurisdictions require that the suspicion is reported promptly to the relevant Financial Intelligence Unit. Financial Institutions/NBSPs must ensure that suspicious activity related to its involvement in MIPS is routed in a timely manner to its internal investigative units for disposition and suspicious transaction report filing in the appropriate jurisdictions.

Agents are often the only persons having actual face to face contact with the customer, with the opportunity to observe suspicious customer behaviour. It is therefore important that agents who do not have reporting obligations are obliged to report suspicions to the principal, who do have an obligation to report suspicious activity.

9.2.6 **Training**

Staff, including agents, responsible for developing and administering MIPS should be appropriately trained on the relevant money laundering risks and mitigating controls.

10. Typologies/Case Studies and Risk Indicators

Analysing internally and externally developed typologies, case studies and risk indicators can supplement further the various elements of a financial institution's and other parties' AML framework for its MIPS. Some examples are;

- Chapter 4 of the FATF Report Money Laundering Using New Payment Methods, dated October 2010.

- MONEYVAL Criminal Flows on the Internet: methods, trends and multi-stakeholder counteraction, dated March 2012.

- International Bank for Reconstruction and Development Protecting Mobile Money Against Financial Crimes: Global Policy Challenges and Solutions, dated 2011.

11. Conclusion

The Wolfsberg Group believes that:

- NBSPs involved in money transmission should be subject to AML regulation/oversight

- Unregulated NBSPs should be considered as high risk

- Financial Institutions need to consider their regulatory/reputational position of dealing with unregulated NBSPs if money transmission is involved

- Increased harmonisation of mobile, Internet, and prepaid-related terminology is desirable to aid discussion and guidelines

As described in Section 8, MIPS Risk Factors, this paper seeks to counter the widely-held perception that all MIPS arrangements represent an automatic high risk of money laundering by underlining that there is a broad spectrum of risk and mitigants for these arrangements. A generalised view of risk should therefore not be taken.

Instead, the specific purpose, features, operation and geographical reach of each MIPS must be assessed as part of a comprehensive risk-based AML compliance programme. Such programmes will include robust customer due diligence, effective transaction monitoring and appropriate staff training and will also leverage the benefits of existing fraud detection and account management facilities.