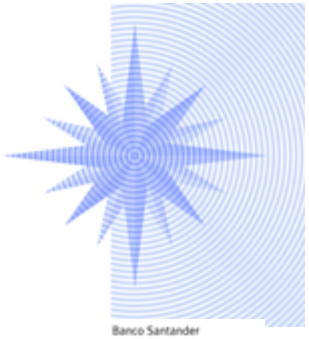
the Wolfsberg Group



Banco Santander
Bank of Tokyo-Mitsubishi UFJ
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
J.P. Morgan Chase
Société Générale
UBS

Wolfsberg Guidance on Prepaid and Stored Value Cards[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 physical Prepaid and Stored Value Card Issuing and Merchant Acquiring Activities and supplements the Wolfsberg Group Statement on Credit/Charge Card Issuing and Merchant Acquiring Activities.

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 in its Reports dated October 2006 and October 2010, it is recognised that there is a growing demand in the marketplace and in financial institutions for migration to electronic payments from paper based processes. It is also recognised that New Payment Methods 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 Prepaid Card is currently the most widely used of the available New Payment Methods

The broadening of payment methods has resulted in greater complexity for regulators and for banks, in relation to assessing the risks attached to them and the application of, and responsibility for, AML controls, particularly if the transactions flow through one or more jurisdictions.

An important aspect when considering NPMs 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 paper based payment methods and the

[1] This paper was written with the collaboration of American Express, The Electronic Money Association, PayLife and Standard Bank South Africa.

more traditional credit/charge cards. The segmentation of services between numerous and varied parties involved in NPMs adds additional complexity.

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.

The regulation of NBSPs may vary:

- they may not be regulated
- they may be regulated to a lower standard than banks
- they may be regulated to the same standard as banks for one specific product/line of business
- they may be only regulated for business in a specific country/countries

3. Scope

3.1 This paper considers the money laundering vulnerabilities of physical Prepaid and Stored Value Cards and provides guidance on managing the risks as part of a comprehensive AML programme. It considers the distinct operations involved in Prepaid and Stored Value Card arrangements.

3.2 This paper does not consider other NPMs referred to by the FATF in their Report, such as Mobile Payments, Internet payment services and Digital Precious Metals.

3.3 Although this paper does not specifically consider terrorist financing and compliance with economic/political sanctions, the application of appropriate AML customer identification procedures or appropriate AML mitigants upon customer acceptance and ongoing (including checking against applicable terrorist and sanctions lists issued by competent authorities) may assist in preventing listed individuals and entities from accessing financial services, including Prepaid and Stored Value Cards.

3.4 Although this paper does not specifically consider the traditional fraud-related threats associated with Prepaid and Stored Value Cards, many risk indicators associated with actual or potential fraud are relevant to the prevention of money laundering.

4. Definition of Prepaid and Stored Value Cards

The terms Prepaid Card and Stored Value Card are used interchangeably in the cards industry.

The physical card is either the token to access value recorded remotely and linked to the card, or the value is stored on and accessible from the physical card's chip (*i.e*. stored value cards, also known as an electronic purse). This means that while all Stored Value Cards are Prepaid Cards, not all Prepaid Cards are Stored Value Cards.

5. The usage of Prepaid and Stored Value Cards

These cards have numerous uses, as indicated below. The common theme is that they are convenient, easy to use and perform a particular function. They also appeal to the sector of the community without access to traditional bank accounts.

The following are typical uses:

- money transmission and payment of bills
- tourism and business travel (replacing use of Travellers Cheques)
- gifts
- pay rewards and incentive programmes
- distribution of government benefits
- payroll disbursement
- storecards
- multi-vendor shopping mall gift cards
- micropayments (*e.g.*) mass transit

6. Roles in Prepaid and Stored Value Card operations

The development and operation of Prepaid and Stored Value card programmes can involve numerous parties. The end to end process can involve up to nine distinct roles for card distribution and use. Several or all roles may be performed by the same party, depending on the setup of the specific Card Programme.

i. **The Programme Manager** is the party that contracts with the Issuer to establish, market and operate a card programme and is responsible for contracting other elements of programme operation as needed. They typically do not themselves issue electronic money. The type of programme manager will vary and may include for example a government body, university or corporate (*e.g*. a payroll manager acting as programme manager and contracting with a bank to offer payroll cards to employees).

ii. **The Issuer** issues cards to cardholders. It is worth noting that some issuing institutions also manage their card programmes themselves, instead of cooperating with Programme Managers.

iii. **The Processor** facilitates payment transactions and may perform a number of different functions: card account set-up, card activation, card production, card mailing, payment authorisations, processing of value load, processing of value reloads, cardholder customer service, chargeback processing, cardholder error and dispute resolution and provision of settlement services with payment networks.

iv. **The Payments Network** (frequently referred to as the Card Brand or Scheme Operator) provides connectivity between retailers/ATMs and the processor for authorisation, clearing and settling payment transactions (*e.g.* branded cards can be used wherever their brand is accepted).

v. **The Distributor** (frequently referred to as the Seller) markets and distributes the card product to customers (*e.g*. a retailer offering gift cards to customers).

vi. **The Cardholder** is the owner or user of a card.

vii. **The Acceptor**, whether a merchant, ATM owner, or a bank, accesses the applicable payments network to debit the appropriate value from the bank account holding funds associated with the card and applies it as a payment.

viii. **The Merchant Acquirer** (usually a bank) offers a number of services to merchants/retailers by providing an interface between merchants and underlying card schemes.

ix. **The Loading/Reloading Service Provider** may act as an agent of the Card Issuer in accepting funds for reloading cards.

7. Types of Prepaid and Stored Value Card Arrangements and Features

7.1 Closed Loop

These are typically used only at specific retailers/outlets, and are not usually part of a scheme/international network.

7.2 Open Loop

These are typically network-branded cards issued by international schemes and can be used at multiple retailers/outlets.

7.3 Principal features of both Closed Loop and Open Loop arrangements

- either funded by known (*i.e*. pre-determined/traceable) source(s) or by unknown source(s)
- either reloadable and/or non-reloadable
- either limited to low monetary value or of high monetary value
- either usable in a restricted outlet(s) or in a wide network

8. Programme Risk Factors

8.1 Programme Features

The general characteristics of Prepaid and Stored Value Cards mentioned below can increase money laundering risk:

- ability to transfer funds (domestically/internationally)
- speed of transfer of funds
- ability to move unloaded unactivated cards across borders
- lack of, or difficulty in providing, an audit trail
- lack of, or difficulty in compiling, an aggregated view of multiple transactions

Additionally, some card programmes have the following characteristics, which can increase money laundering risk:

- lack of face to face contact
- identification material either not taken or taken and not verified
- high negotiability through wide acceptance

- ability to reload
- ability to load/reload cards with cash
- ability to withdraw cash

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

The assessment of potential money laundering risks of a pre-paid card programme should be undertaken by considering each programme's features, including limitations on the source and amount of funds placed on the cards, how the cards are used, and the number of cards one person can own.

The analysis of these features and other factors (by reference to their number and materiality) will assist in determining an aggregate view of the potential money laundering risks and drive the degree to which AML risk management processes and controls can be applied to the pre-paid card programme to mitigate risks. Pre-paid card programme features to consider in assessing potential risks, include, but are not limited to:

8.1.1 Intended geographical scope of the pre-paid card programme

The intended use for the pre-paid programme should be analysed. For example, some programmes, such as travel cards, are specifically designed for cross-border use (but may have limitations on use within specific jurisdictions), while others permit cross border use but have strict limitation on use within specific jurisdictions, and others are strictly limited to use in the jurisdiction of issue.

Factors that decrease risk

- Geographical restrictions on the use of a pre-paid card, such as the ability to limit the use of the card to particular jurisdictions.

Factors that increase risk

- Card programmes that have no geographical restrictions or limitations and, therefore, allow for any type of use in any jurisdiction will increase the potential that the cards could be used for money laundering.

- Cards that can be transacted in jurisdictions considered to be a higher risk for money laundering or terrorist financing, or those that have minimal or non-existent anti money laundering laws, may significantly increase risk.

8.1.2 Intended users of the pre-paid cards

Certain card features, such as requiring a PIN or name embossing may, for money laundering purposes, potentially limit the range of possible use of a prepaid card programme by restricting (or at least complicating) the process of transferring value to third party beneficiaries.

Factors that decrease risk

- Pre-paid card programmes that restrict who can use a particular card to extract value, such as PIN, or embossing the cardholder's name, including the cardholder's photograph on the card, or other features that limit the card use to a specific individual.

Factors that increase risk

- Card programmes that have limited or no ability to restrict or control multiple users.

8.1.3 Knowledge about pre-paid card programme cardholders or acquirers

Gathering certain types of information about the users of a pre-paid card may permit a financial institution to manage their money laundering risks; the same is true for the collection of information on pre-paid card programme acquirers.

Factors that decrease risk

- The collection, availability and (in some circumstances) verification of information related to cardholders (*e.g.*, name, address, date of birth, unique government-issued identification number [tax identifier, passport, driver's license] may reduce risk by allowing for due diligence and screening against government lists, among other "know your customer" type controls.

- Similarly, in terms of the relationship between a card programmes issuer and the programme's acquirer or distributor, an established relationship with the counterparty (*e.g.*, a commercial loan relationship with a corporate customer providing payroll or benefits cards to their employees), provides additional comfort as to the purpose, users and use of the cards

Factors that increase risk

- Lack of relevant information about the cardholder (*e.g.*, name, address, date of birth, unique government-issued identification number [tax identifier, passport, driver's license]) or about parties involved with cards.

8.1.4 Intended scope of card use (open/closed loop)

Pre-paid card programmes can be designed such that card use is limited to a specific merchant or shopping establishment (*e.g.*, a shopping mall), which is known as a closed loop card programme, or they can be designed to offer broader access to the full range of merchants capable of accepting that type of branded card, which is known as an open loop card programme. Some open loop card programmes may offer restrictions on use in terms of the industry types of merchants where the cards may be used (*e.g.*, not casinos).

Factors that decrease risk

- Limitations on the use of the card to one or a limited number of merchants, or the inability to use the pre-paid card for higher risk activities (*e.g.*, card use restricted to targeted merchant types), or transaction/velocity limits on card use.

Factors that increase risk

- Card programmes that have no restrictions on nature and/or place of use or transaction/velocity limits on card use.

8.1.5 Source of funding

The means by which a pre-paid card is funded will present a varying degree of potential money laundering risk, due largely to the relative degree of control that a financial institution has in determining and constraining the source of the funds used to load value onto cards. For example, a card programme managed on behalf of a government entity, such as a government issued benefits card, will generally have a single confirmed source of card funding, as will a payroll card issued for a listed corporation, and both programme types will thereby generally pose a lower risk for money laundering than a card programme where there is less inherent control over the source of funding.

Factors that 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 or an employer (for an employee's compensation or for other benefits from the employer).

- Pre-paid cards, for which review and controls on locations at which the funding can be accomplished are in place, as appropriate for the relevant scheme, may also reduce the risk that the cards will be used for money laundering.

Factors that increase risk

- Unknown sources of funding of the pre-paid card, such as with cash (without other controls that may limit the anonymous nature of the 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.

8.1.6 Source of funding - value limits

Potential card value can be controlled by card programme features such as 1) a maximum amount of funds that can be loaded onto a card in any instance, 2) a maximum amount of total value that can be held on the card at any given time, (ceiling/card limit), and 3) the number of times, or total value with which a card can

be reloaded in a given period. These features may be applied singly or in combination.

In general, lower possible load capacity will result in lower potential money laundering risk, due to the necessity of using more cards to launder a given amount of funds.

Factors that decrease risk

- Pre-paid cards with a low maximum value and those that cannot be funded with additional value may decrease the risk of potential money laundering, as would other card programme features that tend to create lower possible card load capacity.

Factors that increase risk

- Pre-paid cards that either have a high maximum load value or unrestricted reloading capabilities, or both combined, will increase the potential risk that the cards will be used for illicit purposes.

8.1.7 Source of funding – cash

The ability to load value onto a pre-paid card using cash necessarily increases the risk that such a card programme will be subjected to criminal abuse; conversely, money laundering risk is lower for pre-paid card programmes where the cards cannot receive funding in exchange for cash.

Factors that decrease risk

- Card programmes in which card value cannot be funded with cash (*e.g*. pre-funded government benefits cards) will generally pose a lower risk of money laundering activity due to the inability to use card funding as a means of transforming physical currency into electronic currency

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

Factors that increase risk

- The ability to add value to a pre-paid card using cash or cash vouchers sold by retailers will increase the money laundering risks associated with that card programme due to difficulties in determining the legitimacy of the source of the cash.

8.1.8 Funding by value transfer

Pre-paid card programmes where the cards can be loaded online by value transfer from another card (pre-paid, debit or credit) carry an increased risk of money laundering due to the relative ease of transferring funds electronically and the lack

of face to face contact; card programmes where no value can be loaded from another card carry decreased money laundering risk.

Factors that decrease risk

- Card programmes that do not allow for value transfers between unrelated card holders.

Factors that increase risk

- Card programmes that allow for value transfers between unrelated card holders, or, involving value transfers with other pre-paid card programmes.

8.1.9 Cash withdrawal via ATM/Cash redemption of monetary value on card

Cash used to fund a pre-paid card, as well as cash access from a pre-paid card can present unique challenges with regard to assessing the risks of money laundering.

Factors that decrease risk

- Cards that cannot be used to withdraw cash from an ATM are generally considered to pose a lower risk of money laundering.

Factors that increase risk

- Cash access from a pre-paid card, such as through withdrawals from automated teller machines (ATM) or other access points, will increase the potential that the card will be used for money laundering purposes, as will the ability to redeem the value associated with a card for cash. It should be noted, however, that for some pre-paid card programmes (*e.g*. a card issued through a government benefits programme or employer payroll programme) withdrawing cash via an ATM could be considered entirely consistent with anticipated card 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 (cash back).

8.1.10 Value Term Limit

Prepaid card programmes offering cards with a pre-determined and limited lifespan (*e.g*. one year after issuance) are potentially less appealing to money launders due to their requirement that they be used relatively quickly, rather than stored for later conversion.

Factors that decrease risk

- Establishing of fixed duration after which the prepaid card will not retain its value may assist in reducing the potential that the card will be used for money laundering purposes

Factors that increase risk

- No expiry date

8.1.11 Number of Pre-Paid Cards offered to one person

Limitations on the number of cards that can be held by one individual, potentially enforced through monitoring against identifiers (*e.g.* tax identification numbers or other government identifiers) will tend to reduce the possibility that a card programme will be used for money laundering purposes, due to the difficulty of using one individual to handle large numbers of cards, and thereby process large amounts of value. Conversely, programmes that permit an individual to carry multiple cards simultaneously, whether by design or through lack of sufficient identifying information to make such a determination, are more liable to money laundering abuse.

Factors that decrease risk

- Programmes that limit the number of cards that a person can purchase/hold may reduce the potential money laundering risks.

Factors that increase risk

- For some pre-paid card programmes, money laundering risks may increase when a person can purchase/hold multiple cards.

8.2 Segmentation of services

NPMs can be more exposed to risks where several parties are involved in performing the payment service jointly, such as card issuers, 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.

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

9. AML Framework

9.1 Product Design

During design, overall specification and functionality of individual card products are determined. Business Development, Marketing (including sales channel and mode of distribution), Credit Risk, Fraud and Compliance are all stakeholders in this process.

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.

It is also essential that some party in the value chain takes responsibility for compliance.

9.2 AML Controls

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

9.2.1 Due Diligence

- Identification and Verification (ID&V)

  Low risk propositions

  - No ID&V required for cardholder.
  - Any scheme partner not already known to the issuing institution should undergo standard due diligence in accordance with industry/government guidelines (to confirm legitimacy of funding).

  Standard risk propositions

  - Identification of the cardholder is required (capture name, address, date of birth).
  - Verification of the name and address is required. Reliance could be placed on a third party to achieve this, eg if a government agency held list of cardholders who are benefit claimers.

  Higher risk propositions

  - Identification of the cardholder is required (capture name, address, date of birth and nationality).
  - Verification of the name and address is required. This should be in line with government or industry guidelines.
  - Any scheme partner not already known to the issuing institution should undergo standard, or, where they are deemed a high risk institution, enhanced due diligence (to confirm legitimacy of funding).

- Screening

  Low risk propositions

  - No sanctions screening of cardholder.
  - Screening scheme partner is recommended to ensure they or the beneficial owners are not on relevant sanctions lists.

Standard risk propositions

- Sanctions screening of the cardholder should take place, both before the account is opened and during the lifetime of the account.
- Screening scheme partner is recommended to ensure they or the beneficial owners are not on the relevant sanctions lists.

Higher risk propositions

- Sanctions screening of the cardholder should take place, both before the account is opened and during the lifetime of the account.
- Screening scheme partner is recommended to ensure they or the beneficial owners are not on relevant sanctions lists.

9.2.2 Transaction Monitoring

Card activity monitoring frameworks should be developed following an analysis of the particular card programme features and card attributes, including range of use and maximum load value. Monitoring could possibly include unusual card use against such standards as high-value use, high-volume use or loading frequency or unexpected geographical use.

- Card Funding

  For reloadable card programmes 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 unauthorised sources is a key control element, as it gives the issuer confidence that the funds being loaded onto these lower risk cards remain known.

  The employment of duplicate enrolment controls may also be relevant to card programmes with a known source of funding, to eliminate the possibility that a cardholder could obtain an excessive number of cards for a lower-risk card programme. Although such controls may be particularly applicable for the prevention of fraud, they may serve to help mitigate AML risk.

  Card programmes funded through the Issuing Institution only, rather than through multiple financial and non-financial institutions also represent a significant mitigating factor. This is most relevant in instances where cards can only be issued to existing customers of the Issuing Institution.

- Card usage:

  - unusual level and frequency of ATM usage
  - unusually high value/volume card activity
  - unusually high velocity card activity
  - card 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 card features and any other risk factors.

- Card issuance

  Card programmes that limit the number of cards per Unique Identifier (e.g., SSN, TIN or address) may constrain money launderers. Appropriate monitoring should be implemented to ensure that programme limits are not breached.

  It should be noted that there is no central register or view of what each Issuer has issued.

9.2.3 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.

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.

9.2.4 Suspicion Reporting

Generally, if a financial institution 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 financial intelligence unit. Financial Institutions must ensure that suspicious activity related to its involvement in pre-paid and stored value card programmes 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 to the customer, with the opportunity to see suspicious customer behaviour. It is therefore important that agents without reporting obligations are obliged to report suspicions to the principal.

9.2.5 Training

Staff responsible for developing and administering card programmes should be appropriately trained on the relevant ML risks and compensating controls.

10 Typologies/Case Studies and Red Flags

Analysing internally and externally developed typologies, case studies and red flags can supplement further the various elements of a financial institution's AML framework for its pre-paid and stored value card programmes. For example, one source of reference is Chapter 4 of the FATF Report Money Laundering Using New Payment Methods dated October 2010.

Summary

There is a widely held perception that all Prepaid and Stored Value Card arrangements represent a high risk of money laundering.

This paper seeks to counter that perception by underlining that there is a broad spectrum of risk for Card Arrangements, and that a generalised view of risk cannot be taken. Instead, the specific purpose, features, operation and geographical reach of each Card Arrangement 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.