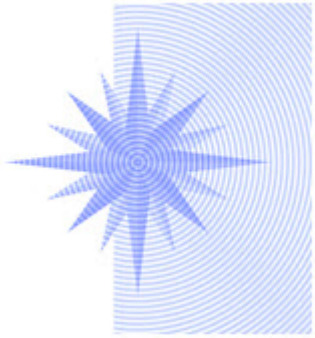
the Wolfsberg Group



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

Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities (2009)

1. Preamble

The Wolfsberg Group of International Financial Institutions (the "Wolfsberg Group"[1]) has published global anti-money laundering ("AML") guidance, statements and principles on a number of related topics including private banking, correspondent banking, the suppression of terrorist financing, transaction monitoring, pooled vehicles and the risk based approach. The Wolfsberg Group believes that adherence to these principles promotes effective risk management and enables financial institutions to exercise sound business judgment with respect to business dealings and furthers the goal of Wolfsberg Group members to endeavor to prevent the use of their institutions for criminal purposes.

2. Scope

2.1 The purpose of this paper is to consider the threats to, and vulnerabilities of, credit/charge card "Issuing" activities in relation to money laundering and provide guidance on managing these risks as part of a comprehensive approach to AML compliance management. The paper also addresses merchant acquiring ("Acquiring") - the underwriting, provision and maintenance of Point of Sale relationships. Acquiring activities, and their attendant AML controls, may be closely aligned to the risks and controls associated with cards, and many large financial institutions extend services to both card and merchant customers.

This guidance therefore should be considered in conjunction with other Wolfsberg Group papers as appropriate - in particular its principles on the Risk Based Approach[2].

2.2 This paper does not consider Debit Cards, including "Automated Teller Machine" only products which are solely linked to deposit accounts or Stored-value / Pre-paid cards.

---

[1] The Wolfsberg Group consists of the following leading international financial institutions: Banco Santander, Bank of Tokyo-Mitsubishi-UFJ Ltd, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JPMorgan Chase, Société Générale, and UBS.

In addition, the following institutions also participated in the preparation of this paper: American Express Company, Lloyds TSB.

[2] See existing Wolfsberg papers at http://www.wolfsberg-principles.com/standards.html.

2.3 Although this paper does not specifically cover the traditional fraud-related threats associated with these types of products, about which considerable evidence is available, many risk indicators associated with actual or potential fraud, particularly identity theft, are highly relevant to the prevention of money laundering. At the same time, however, it is important to understand certain differences between fraud and money laundering methodologies, described more fully below (refer to section 5.6 "Transaction/Customer Monitoring") and these should be considered when developing and implementing an effective transaction monitoring framework.

2.4 Whilst this guidance does not specifically address terrorist financing, the undertaking of appropriate customer identification (including checking against applicable sanctions lists where provided by competent authorities), acceptance, initial and ongoing due diligence may assist in preventing terrorists or terrorist organizations from accessing all financial services – including those associated with the provision of credit card/charge card issuing and merchant acquiring.

3. Background

The continuing threat of money laundering through financial institutions is most effectively managed as part of an effective overall AML compliance program by understanding and addressing the potential money laundering risks associated with customers, products, services, geography and transactions. This program should also be used to determine the level and type of training to be provided to relevant staff.

The banking industry, banking regulators and law enforcement officials, have historically considered credit card issuing and acquiring as posing a lower risk of money laundering compared with other financial products and services. The sophisticated application screening and fraud monitoring systems employed in relation to credit card products and services combined with restrictions on cash payments, cash access and credit balances, make them less effective as a vehicle for money laundering.

The nature of the card product itself creates certain "structural" controls/restrictions at the Placement and Integration stages of the money laundering lifecycle (e.g. (i) credit line facilities generally limit the amount of currency that can be accessed by card holders; (ii) there are similar limitations on the ability of a card holder to insert cash into the financial system; and (iii) settlement payments by card holders are generally required to be denominated in local currency, and therefore the funds used to pay card bills will already have been placed into the local regulated banking system before reaching the Issuer).

Despite this, credit cards in common with other financial services products can be vulnerable to abuse unless effective controls are employed to minimize the risks. Credit cards, for example, may be used to transfer funds that are the result of criminal activity. Rapid technological advances in the electronic banking environment in general and the introduction of certain new product features in response to consumer demand (refer to section 5.1 "Product Design"), also have the potential to introduce money laundering vulnerabilities. Periodic reviews should be undertaken by the Issuer to identify emerging risks and to determine the extent to which further enhancements to existing AML related controls are needed to address these risks.

Historically, Issuing and Acquiring activities have developed and refined rigorous controls and oversight in relation to fraud threats. The use of a false or stolen identity enhances the chances of success for all financial crimes, including money laundering, and both Issuers and Acquirers place emphasis on maintaining effective customer identification procedures. These controls may also be effective in managing the money laundering risks associated with Issuing and Acquiring activities.

4. Types of Card

Banks and other institutions may issue their branded cards as members of an association/global credit card network. The association, under this business model, is known as a Card Scheme operator of a credit card system. Large global associations such as Visa, MasterCard, American Express and Discover are operators who partner with third-party issuers who, in turn, issue "dual-branded" cards. This Guidance extends to all Issuer relationships established and delivered for and through the following types of credit and charge cards:

- Open Loop Cards. These are typically issued by global associations and can be used at multiple retailers, for example:
    - General Purpose cards;
    - Affinity cards (e.g. Owners Clubs);
    - Partnership cards;
    - Corporate cards (issued to businesses and companies for use by their employees).

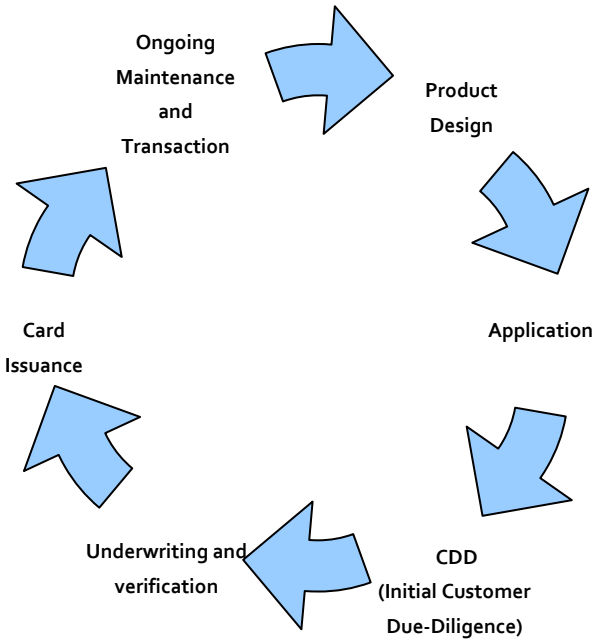
- Closed Loop Cards. These are typically used only at a specific retailer that issued the card and are not usually part of an association/global credit card network.

Financial institution Issuers are responsible for maintaining an AML compliance program, but the operators are also responsible for maintaining their own risk-based AML compliance program *in addition* to the responsibilities of the Issuer. These programs consider certain additional risks associated with card issuance through third parties as well as any local legal/regulatory requirements that may vary from country to country.

5. Card Issuing

Generic Card Lifecycle

In assessing the overall risks associated with card issuing (distinct from the risks associated with Merchant Acquiring, discussed below), the Wolfsberg Group believes it is appropriate to consider the specific threats and vulnerabilities associated with the various stages in the lifecycle of card development, delivery and use. These stages, which include ongoing transaction monitoring, can be represented as follows:



5.1. Product Design

During this phase of the product lifecycle, market area, overall product specification and functionality of individual card products are determined. Financial Crime, Compliance, Business Development, Credit Risk and Marketing groups 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 risk attributes and the appropriate controls required. All aspects of the product offering must be considered from an AML perspective, as well as controls to mitigate and manage these risks. For example, it may be appropriate to set limitations for certain features of the product or service, such as the amount of the credit line that can be used for cash.

Product features which could introduce vulnerabilities to money laundering and consequently may necessitate mitigating controls, include:

- Issue of convenience cheques;
- Ability to access cash, especially offshore, in multiple currencies;
- Multiple authorized users (or supplemental card holders);
- Card account settlement, especially with currency and cash equivalent instruments or by third parties;
- Instant Credit Cards (usually in conjunction with a third party supplier (e.g. a retail store)).

Product features may also reduce vulnerabilities to money laundering. Restrictions on cash access, authorized users and other higher risk features, coupled with appropriate controls for overpayments and credit balance refunds, and supported by rigorous transaction monitoring for

fraudulent and unusual transactions, will lessen or eliminate the need to risk-rate by customer type.

5.2. Application / Identity & Verification

The tools available to card issuers to identify and verify their applicants will necessarily vary depending upon jurisdiction and may be influenced by the timeframe within which such activity has to take place. Some jurisdictions will have well developed credit reference agencies/systems, while others will not. Similarly, some jurisdictions may require an Issuer to obtain a government issued identity number from the card applicant while other jurisdictions may prohibit an Issuer from requiring such a number, citing privacy or other concerns. In all situations however, account opening procedures should be sufficiently robust to ensure that the Issuer can gain a reasonable belief that it knows the true identity of its customers. In those jurisdictions with well developed credit reference agencies/systems, this may be utilized as part of a non face-to-face account opening process, which is typical of the credit card issuance business model. For example, information obtained from the customer's credit report during pre-screening[3] or from other reliable sources may be used to both verify identity and corroborate other information provided in the application

Where the relevant jurisdiction has enacted laws or regulations concerning what a card issuer must do to identify its customers, adhering to those laws or regulations can generally be considered sufficient for purposes of due diligence. However, depending on the risk associated with the product and customer relationship more rigorous measures may be appropriate. For example, more information may be considered appropriate of applicants for credit card products intended for business use (e.g., records of incorporation and business licenses) than of applicants for card products intended for personal and household use.

5.3. Initial Customer Due Diligence

Issuers should apply a risk-based approach when considering the level of due diligence to be carried out. For additional/supplementary or multiple card holders this should be considered both in terms of the appropriate verification required in respect of the individual(s) and the limitations and controls placed on the product features to which additional users have access (e.g., prohibiting contractual changes to the account). This should be ascertained at the Product Design stage.

Different risks are also posed in respect of corporate cards issued to employees of publicly held, regulated or transparent corporations compared with those of small businesses and privately held companies where more limited assurance can potentially be placed on the existence of appropriate controls.

At this stage, processes should also be introduced to identify and manage potentially higher-risk customers. Unless specified under local legislation and/or regulation this should be undertaken

[3] Pre-screening is a process undertaken to identify potential customers for card products, including those that are "pre-approved."

[4] See existing Wolfsberg papers at http://www.wolfsberg-principles.com/standards.html

using an appropriate risk based approach. Further guidance can be obtained by reference to the Wolfsberg principles on the Risk Based Approach[4].

With respect to compliance with global sanctions regimes, local legislation/regulation or scheme rules may require Issuers to screen individuals and entities against applicable sanctions lists. It is recognized that certain sanctions programs targeting specific countries are not (or, for legal reasons, may not be able to be) uniformly applied in all jurisdictions. Suitable controls should be incorporated into an Issuer's account opening process to ensure compliance with local and applicable global sanctions targeting individuals and entities.

In addition to the primary applicant, the screening of additional cardholders against applicable lists should also be considered as part of a risk based approach.

5.4. Channels

Many credit card issuers offer multiple application channels including: in person, over the Internet, by telephone, through direct mail, event marketing and relationships initiated through intermediaries. Each channel should be evaluated independently for the AML risks associated with it. The fact that the application stage is typically a non-face-to-face process does not, by itself, mean that this stage is "high risk". Rather, it means that an Issuer must fully evaluate available controls (most notably the non-documentary identity verification alternatives) to address the risks. It is worth noting that a prescriptive regulatory approach may detract from an Issuer's ability to apply a flexible and dynamic set of controls to the risks identified at this stage of the card lifecycle.

5.4.1 Internet /Telephone; Direct Mail

Issuers must ensure adequate controls are in place to verify customers. Appropriate risk-based non-documentary customer identification processes, such as credit bureaus, public record information, or third party services may be employed. Issuers and third-party service providers processing applications should receive appropriate training to be able to detect obvious "red flags" or other irregularities with the applications (e.g., obvious tampering with the application, multiple applications from the same IP address, etc).

5.4.2 Third Party

Issuers must ensure that applications obtained by third parties on their behalf meet similar customer identity standards as do applications received through direct channels. It is critical that both Issuers and third parties maintain effective AML compliance programs including a risk based schedule of periodic checks and reviews.

5.4.3 Merchant Private Label (e.g. Department store Cards)

The risks involved with merchant private label cards will vary depending on the utility of the card. For instance, "closed-loop" private label cards that can be used only at one merchant, or a defined number of merchants, pose significantly less risk than cards issued by merchants which can be used as a general purpose "open loop" card. Just as with other

third parties, appropriate training and merchant supervision should be in place, and transaction monitoring scenarios may be designed to look for unusual spend patterns at these merchants.

5.4.4 Instant Credit

Additional risk considerations should be given to instant credit card approval processes. In this type of arrangement the Issuer may be undertaking a limited initial review of the applicant in order to provide the customer with an immediate single-use of a credit product at a particular merchant (the customer will typically receive the credit card within a few days). In addition to fraud controls, special attention should be given to the AML considerations posed by such a process.

5.5. Underwriting and Verification

Issuers must ensure that customer information is obtained prior to allowing the customer to access credit, and the Issuer must have a risk-based method for verifying the customer's identity in a timely manner.

5.6. Transaction/Customer Monitoring

5.6.1 Once the card has been issued, Issuers must establish an effective transaction monitoring framework as part of ongoing due diligence. They should seek the opportunity to develop and, where appropriate, integrate their AML monitoring scenarios with other systems, for example, those used for fraud control. As noted above, identity theft or misuse may be a component of financial crime, and of equal relevance to fraud and money laundering prevention. For these reasons a large degree of overlap exists between the components of effective anti-fraud and AML compliance programs. In other respects, however, such as restricting large payments, cash payments, and wire transfers, the objectives of these programs will not coincide and may even appear to be at odds. In short, when designing monitoring tools to identify unusual money laundering activity, it is important to consider both the similarities and the differences between these risks.

5.6.2 Designing effective fraud monitoring scenarios is often commenced by reference to an earlier series of objective events leading up to an identified loss, while a money laundering scenario is designed from an intelligence/typology perspective. In other words, a money launderer will seek to operate their account in a way that appears innocuous (e.g. by paying their bills on time), with the result of fewer "red flags" to monitor with "standard" metrics. These differences must be understood in order to design useful monitoring tools and perform periodic assessments of the tools' effectiveness.

5.6.3 An effective transaction monitoring framework must include, at a minimum, procedures for: (i) internal escalation of potentially suspicious activity, (ii) filing reports of suspicious activity with Government Financial Intelligence Units or other Authorities, (iii) consideration of whether to terminate the relationship with the card holder, and (iv) record keeping and documentation of these processes. The monitoring program should include an

appropriate use of technology solutions, and must ensure that all personnel who are evaluating and investigating the transactions are adequately trained to do so.

5.7. "Red-Flag" Indicators

As noted above, certain product features, functionality or activity may pose the risk of misuse for money laundering. Listed below are several AML-related "red flags", although the list is not all-inclusive and it should be kept in mind that identifying typologies is a dynamic and evolving process. It is further acknowledged that there may be significant limitations (e.g., data availability) which may impede the ability of an Issuer to monitor against all these indicators, but they may be appropriate for consideration when investigating unusual and potentially suspicious transactions.

Monitoring of and training on, unusual and potentially suspicious activity indicators remains an important component of a robust AML program.

5.7.1 Application, Identification and Underwriting:

- Information mismatch from application;
- Application information/address/customer differs from pre-screened applicant;
- Inability to verify card holder identity information;
- Inability to provide government issued identification details;
- Primary/secondary user name appearing on applicable government watch/sanctions lists;
- Change of address to high-fraud area or to problematic jurisdiction, shortly after the card issuance or credit line increase.

5.7.2 Transaction Monitoring:

- Frequent and unusual use of the card for withdrawing cash at ATMs;
- Structuring payments/Overpayments: balances on cards may move into regular credit where card holders pay too much or where merchants give credits to an account. Money laundering may be facilitated via refunds of the credit balance;
- Unusual cash advance activity and large cash payments: the monitoring of incoming cash is critical, as excessive cash payments are often an attribute of money laundering. Credit balance accumulation resulting in refunds (CBRs) should be monitored as they can be used as part of a scheme to launder funds;

- Cross Border: cash withdrawn via cards in another jurisdiction permits easy (and potentially high-value) cross-border movement of funds with a limited audit trail;

- Unusual purchase of goods or services in countries regarded by an institution as posing a heightened risk for money laundering;

- Excessive payments on private label credit cards via gift card from the merchant;

- Purchases at merchant on personal cards which are significantly out of pattern with historical spending behavior;

- Merchant credits without offsetting merchant transactions;

5.7.3 Customer Monitoring

- Excessive customer service calls;

- Abnormal customer contact behavior (e.g., frequent changes of address).

5.7.4 Card Account Settlement:

- Multiple and frequent cash payment or money orders; large, cross-border wire transfer payments;

- Where Issuers have access to this information, Settlements/partial settlements from unrelated third parties;

- Where Issues have access to this information, unrelated checking/current account paying multiple credit card accounts;

- Excessive/ongoing large credit refunds.

5.8. Card Account Closure

Based on the severity or frequency of suspicious activity, it may be appropriate, where legally permissible, to exit a card relationship. As noted above, Issuers should establish criteria for exiting card relationships after suspicious activity is detected and reported, or after negative customer information is identified. These criteria should address whether, and under what circumstances, the Issuer will proactively notify law enforcement, and should include procedures to avoid the risks of "tipping off" the card holder.

6. Merchant Acquiring

The Merchant Acquiring business presents different, and potentially somewhat higher, risks for money laundering than card issuance. This is due to fundamental differences in the financial transactions being effected by the merchants compared to the card holders (including volume and value differences; the merchant's ability to effect refunds, which can raise the risk of collusion; charging for non-existent goods; transferability of charge receipts; etc.).

Acquirers should consider the type of business being undertaken by the merchant as part of their risk based assessment to determine the appropriate level of due diligence that should be undertaken before establishing a merchant acquiring arrangement. Merchants identified as representing a high risk should be the subject of enhanced due diligence (which may include on-site visits where possible and deemed appropriate) and more frequent reviews during the course of the relationship.

6.1. Risk Mitigation

There is an expectation from some regulatory authorities that merchant acquirers be aware of the risks associated with this process and implement appropriate account and transaction monitoring accordingly. Many Operating Regulations, for example those issued by MasterCard and Visa, related to Merchant Acquiring provide fraud-related guidelines in this regard.

Acquirers should mitigate the risk that one or more of their merchants may be involved in money laundering (and be alert to the risk of collusive merchants) by understanding the types of goods their merchant offers and what activities/transactions are indicative of money laundering in the context of that business.

Where Acquirers use third parties (e.g. Independent Sales Organizations (ISOs)) to perform underwriting and/or provide equipment, or other services on behalf of the Acquirer they should ensure that appropriate contracts are in place that set out clear statements of requirements and of the standards of service expected from the third party provider.

6.2. Initial & On-going Due Diligence

Acquirers should obtain sufficient detail from merchant applications to enable them to assess the risks. Relevant information contained therein might be corroborated by either appropriate electronic means or by suitable documentation. This may include, where available and appropriate, commercial credit bureau reports and personal credit reports for the principals. Acquirers should form an understanding of the merchant's typical charge type and amount by analyzing both pre and post-acquisition information and validate activity over time.

Initial due diligence should be supported by the use of transaction monitoring to assist in the identification of activity (volumes, velocity etc.) that may be indicative of money laundering and other illegal activity.

6.3. Risk/Red Flag Indicators

As with card issuing, the merchant acquiring business presents a unique set of threats that can be associated with either fraud or money laundering. Some of these are represented by the following lists of "Red Flags". It is acknowledged that there may be significant limitations (e.g., data availability) which may impede an Acquirers ability to monitor against all these indicators, but they may be appropriate for consideration when investigating unusual and potentially suspicious transactions.

6.3.1 Account Set Up:

- Principals of the merchant appear to be unfamiliar with, or lack a clear understanding of, the business;
- Higher risk merchants/product types;
- Lack of reliable third party and/or governmental verification of business;
- The address indicated (or corroborated) is identified as mail drop or other high-risk address, as opposed to a physical street address;
- Proposed transaction volume/refunds/charge-backs inconsistent with on-site visit or merchant/industry peer group;
- The business is relatively new, with little to no operating history that can be evaluated;
- Where appropriate, no government issued identity document, or bureau verification of principals/owners of business;
- Merchant/principals/owners match entries appearing on applicable watch/sanctions lists.

6.3.2 Transaction and Merchant Monitoring:

- Unusual or changing trends in processing volumes (velocity) and value from account opening estimates (e.g. average transaction amount, sales volumes, chargeback and refund rates, etc);
- Out of pattern or excessive cash advance volume or credit refunds;
- Lack of charge activity (i.e., monitoring inactive accounts for possible fraudulent diversions);

- Enhanced monitoring of transaction activity at merchants assessed by an institution as representing a higher risk

- Mismatch of charge-backs with transaction types/volumes;

- Unusual volume, account address changes or other activity immediately following account opening;

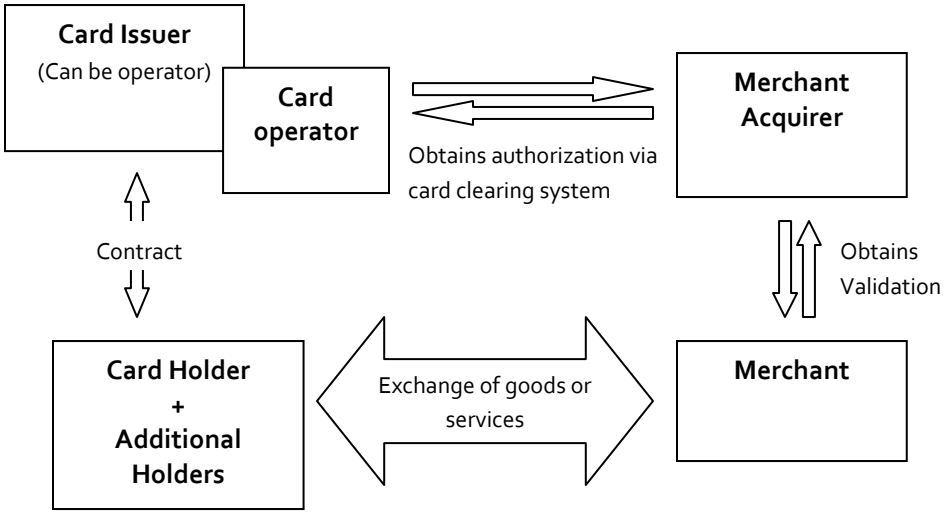
- Indications that a Merchant's facility is used by third parties;

- Merchant/principals/owners potentially appear on government watch/terrorist lists.

7. Summary

The money laundering risks associated with card issuing and acquiring activities have historically been considered lower than for many other financial products and services. These activities are nevertheless susceptible to compromise and abuse unless appropriate control measures are employed to identify and manage these risks. This is best achieved as part of a comprehensive risk-based, AML compliance program that includes robust customer due diligence, effective transaction monitoring and appropriate staff training and which leverages the benefits of existing fraud detection and account management facilities.

Appendix 1
Parties to a Card Transaction



Appendix 2
Glossary of Terms

Acquirer (merchant acquirer)
A bank or other financial institution having a business relationship with merchants, retailers and other service provides to process their card transactions. The acquirer handles/processes debit and credit card transactions received, reimbursing the merchant for the amount of the sale and levying a service charge/commission for the service.

Authorisation
The process whereby a merchant requests permission for the card to be used for a particular transaction amount.

Automated Teller Machine (ATM)
Also known as a cash machine, cash dispenser or hole-in-the-wall machine. A computerised self-service device permitting the holder of an appropriate card and personal identification number (PIN) to withdraw cash from their account and access other banking services.

Card Issuer
A Financial Institution issuing payment cards, ATM cards or cheque guarantee cards to its customers. For payment and ATM-only cards, the card issuer undertakes responsibility to settle transactions made with the card (except in some cases where fraud is present).

Card Holder
The cardholder is the customer or client of the Card Issuer and has the issued card in their name. The cardholder also includes any additional card users that the holder may request on their account and for whom the Issuer agrees to issue further cards.

Card Operator
The Operator handles the production and management of the card including accounting for repayment of any outstanding balance for a credit card or ensures that for a debit card transaction balances cannot exceed the available balance on the underlying account. The operator and Issuer may be the same entity, or the operator may contract to operate the card for the Issuer.

Card scheme(s)
Card schemes set the business rules that govern the issue of the payment cards that carry their logo. Typically, these rules apply throughout the world to ensure interoperability of cards. In many countries, domestic schemes also operate. The schemes operate the clearing and settlement of payment card transactions. In the UK, banks and building societies must be members of the appropriate scheme to issue cards and acquire card transactions. Examples of international card schemes are Visa, MasterCard, American Express, Discover and Diners Club.

Charge card

A payment card, enabling holders to make purchases and to draw cash, usually to a pre-arranged ceiling, the terms of which include the obligation to settle the account in full at the end of a specified period. Cardholders are normally charged an annual fee.

Chargeback
Transactions returned by an issuer to the acquirer because they have been disputed by the cardholder and/or found to be improper by the issuer.

Convenience Cheque
A cheque provided by the credit card issuer to a consumer and drawn on their credit card account. Convenience cheques can be used in the same way as a personal cheque.

Credit card
A payment card enabling the holder to make purchases and to draw cash, usually up to a pre-arranged ceiling. The credit granted can be settled in full by the end of a specified period or can be settled in part, in which case interest is charged. In the case of cash withdrawals, interest is normally charged from the transaction date. Cardholders may be charged an annual fee.

Electronic Point of Sale - EPOS
A terminal or similar device that may be used at the point of sale; e.g. shop, bank etc.

Issuer
A bank or building society issuing payment cards, ATM / cash machine cards or cheque guarantee cards to its customers. For payment cards, the card issuer undertakes responsibility to settle transactions made with the card (except in some cases where fraud is present).

Merchant
Any person, firm or corporation that has contracted with an acquirer to process transactions.

Payment Aggregator
A provider of payment services who specializes in combining multiple small transactions from the same merchant (or credit card account) into an aggregated master account from which larger and fewer payments are made.

Personal Identification Number (PIN)
A set of numeric characters, usually a four-digit sequence, used by a cardholder to verify their identity at a point-of-sale (POS) or by a customer activated device, such as a cash machine. The number is generated by the card issuer when the card is first issued and may be changed by the cardholder thereafter.

Pre-screening
The generation of a customer mailing list and the treatment of the consumer's response as an application, including a review of the consumer's credit report.