2: Credit cards, etc

Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.

Overview of the sector

2.1 A credit card evidences an unsecured borrowing arrangement between an issuing entity and a cardholder, whereby the cardholder obtains goods and services through merchants approved by the Merchant Acquirer (see paragraph 2.9), up to an agreed credit limit on the card. Cards may also be used at ATMs to withdraw cash, which is then added to the balance owing on the card account. Withdrawals (charged to the card account) across a bank counter may be made, upon the presentation of sufficient evidence of identity.

2.2 The cardholder agrees to repay any borrowing, in full or in part, at the end of each statement period. There will be a minimum monthly repayment figure (typically between 2% and 3% of the outstanding balance, depending on the issuer). Interest is charged by the issuing entity, at an agreed rate, on any borrowing not repaid at the end of each period. Any interest or fees charged are added to the card balance.

2.3 Cards are issued by individual Card Issuers, each of whom is a member of one or more Card Schemes (e.g., Visa, MasterCard). Each credit card will be branded with the logo of one of the card schemes, and may be used at any merchant worldwide that displays that particular scheme logo. Cash may also be withdrawn through ATMs which bear the scheme logo.

2.4 Credit cards may be used through a number of channels. They may be used at merchants' premises at the point of sale, or may be used remotely over the telephone, web or mail (referred to as 'card not present' use). In card not present use, additional security numbers shown on the card may or may not be required to be used, depending on the agreement between merchant and its acquiring bank. The Merchant Acquirer (see paragraph 2.9) will undertake its own assessment of the merchant, and decide what type of delivery channel(s) it will allow the merchant to use to accept card transactions.

Different types of credit card

2.5 A Card Issuer may have a direct relationship with the cardholder, in which case the card will clearly indicate the names of the Issuer and of the cardholder. Some Issuers also issue and manage cards branded in the name of other firms (referred to as 'branded cards'), and/or which carry the name of another organisation (referred to as 'affinity cards'). Each card scheme has strict rules about the names that must appear on the face of each card.

2.6 Store cards are similar to credit cards, but are issued in the name of a retail organisation, which is not a member of a card scheme. These cards may be issued

and operated by a regulated entity within the store group, or on their behalf by other firms that issue and operate other cards. Store cards may only be used in branches of the store, or in associated organisations, and not in other outlets. Generally, store cards cannot be used to obtain cash. They are therefore limited to the domestic market, and cannot be used internationally.

2.7 As well as issuing cards to individuals, an Issuer may provide cards to corporate organisations, where a number of separate cards are provided for use by nominated employees of that organisation. The corporate entity generally carries the liability for the borrowings accrued under their employees' use of their cards, although in some cases the company places the primary liability for repayment on the employee (generally to encourage the employee to account for his expenses, and to claim reimbursement from the company, in a timely manner).

2.8 This sectoral guidance applies to all cards that entitle the holder to obtain unsecured borrowing, whether held by individuals or corporate entities, and whether these are straightforward credit cards, branded or affinity cards, or store cards. It is not intended to apply to pre-paid cards (although in terms of processing these would use the same infrastructure as credit and debit cards), which are dealt with in sector 3: *Electronic money*.

Merchant acquisition

2.9 Merchant Acquirers provide a payment card processing service, which facilitates acceptance of payment card transactions between cardholders and merchants. Payment cards that bear card scheme acceptance brands (e.g., MasterCard and Visa) are issued by banks and financial institutions which are members of the relevant card scheme. The Merchant Acquirer processes the card transaction on behalf of its merchant customer, including, in appropriate cases, seeking authorisation for the transaction from the card issuer.

2.10 Payment (settlement) is made by the Card Issuer through the Card Scheme – e.g., Visa. In turn the scheme will pass funds to the Merchant Acquirer through the merchant's bank account. The merchant is therefore a customer of (i) the acquiring bank for the purposes of transaction processing, and (ii) the bank with which it maintains its primary banking relationship, which may or may not be the same as the acquirer. The merchant does not have a relationship with the Card Issuer. For further guidance on transactions through Merchant Acquirers, see Part III, sector 1: *Transparency in electronic payments*, paragraph 1.18.

2.11 At the outset of the relationship with the merchant, the Merchant Acquirer will gather information on such matters as the expected card turnover, and average ticket value. This information is assessed in respect to the type of business the merchant is undertaking and the size of such business.

What are the money laundering and terrorist financing risks in issuance of credit cards?

2.12 Credit cards are a way of obtaining unsecured borrowing. As such, the initial risks are more related to fraud than to 'classic' money laundering; but handling the criminal property arising as a result of fraud is also money laundering. Card Issuers will therefore generally carry out some degree of credit check before accepting applications.

2.13 The money laundering risk relates largely to the source and means by which repayment of the borrowing on the card is made. Payments may also be made by

third parties. Such third party payments, especially if they are in cash or by debit cards from different locations or accounts, represent a higher level of money laundering risk than when they come from the cardholder's bank account by means of cheque or direct debit.

2.14 Balances on cards may move into credit, if cardholders repay too much, or where merchants pass credits/refunds across an account. Customers may ask for a refund of their credit balance. Issuance of a cheque by a Card Issuer can facilitate money laundering, as a credit balance made up of illicit funds could thereby be passed off as legitimate funds coming from a regulated firm.

2.15 Where a cardholder uses his card for gambling purposes (although the use of credit cards is prohibited in casinos), a card balance can easily be in credit, as scheme rules require that winnings are credited to the card used for the bet. It can be difficult in such circumstances to identify an unusual pattern of activity, as a fluctuating balance would be a legitimate profile for such a cardholder.

2.16 Cash may be withdrawn in another jurisdiction; thus a card can enable cash to be moved cross-border in non-physical form. This is in any event the case in respect of an amount up to the credit limit on the card. Where there is a credit balance, the amount that may be moved is correspondingly greater; it is possible for a cardholder to overpay substantially, and then to take the card abroad to be used. However, most card issuers limit the amount of cash that may be withdrawn, either in absolute terms, or to a percentage of the card's credit limit.

2.17 Where several holders are able to use a card account, especially to draw cash, the Card Issuer may open itself to a money laundering or terrorist financing risk in providing a payment token to an individual in respect of whom it holds no information. The issuer would not know to whom it is advancing money (even though the legal liability to repay is clear), unless it has taken some steps in relation to the identity of all those entitled to use the card. Such steps might include ascertaining:

- whether the primary or any secondary cardholder (including corporate cardholders) is resident in a high-risk jurisdiction or, for example, a country identified in relevant corruption or risk indices (such as Transparency International's Corruption Perception Index) as having a high level of corruption

- whether any primary or secondary cardholder is a politically exposed person

Managing the elements of risk

2.18 Measures that a firm might consider for mitigating the risk associated with a credit card customer base include the following:

- deciding whether to disallow persons so identified in the above two categories, or to subject them to enhanced due diligence, including full verification of identity of any secondary cardholder
- requiring the application process to include a statement of the relationship of a secondary cardholder to the primary cardholder based on defined alternatives (eg. Family member, carer, none)
- deciding whether either to disallow as a secondary cardholder on a personal account any relationship deemed unacceptable according to internal policy parameters, or where the address of the secondary cardholder differs to that of the primary cardholder, or to subject the application to additional enquiry, including verification of the secondary cardholder

- becoming a member of closed user groups sharing information to identify fraudulent applications, and checking both primary and secondary cardholder names and/or addresses against such databases
- deciding whether to decline to accept, or to undertake additional or enhanced due diligence on, corporate cardholders associated with an entity which is engaged in a high-risk activity, or is resident in a high-risk jurisdiction, or has been the subject of (responsible) negative publicity
- implementing ongoing transaction monitoring of accounts, periodic review and refinement of the parameters used for the purpose. Effective transaction monitoring is the key fraud and money laundering risk control in the credit card environment
- in the event that monitoring or suspicious reporting identifies that a secondary cardholder has provided significant funds for credit to the account, either regularly or on a one-off basis, giving consideration to verifying the identity of that secondary cardholder where it has not already been undertaken
- deciding whether the cardholder should be able to withdraw cash from his card account
- deciding whether the card may be used abroad (and monitoring whether it is used abroad)

Who is the customer for AML purposes?

2.19 Identification of the parties associated with a card account is not dependent on whether or not they have a contractual relationship with the Card Issuer. A Card Issuer's contractual relationship is solely with the primary cardholder, whether that is a natural or legal person, and it is to the primary cardholder that the Issuer looks for repayment of the debt on the card. The primary cardholder is unquestionably the Issuer's customer. However, a number of secondary persons may have authorised access to the account on the primary cardholder's behalf, whether as additional cardholders on a personal account or as employees holding corporate cards, where the contractual liability lies with the corporate employer.

2.20 The question therefore arises as to the appropriate extent, if any, of due diligence to be undertaken in respect of such secondary cardholders. Hitherto, there have been marked variations in interpretation and practice between Card Issuers with regard to the amount of data collected on secondary cardholders and the extent to which it is verified.

2.21 In substance, an additional cardholder on a personal card account is arguably analogous to either a joint account holder of a bank account, but without joint and several liability attaching, or - perhaps more persuasively – to a third party mandate holder on a bank account. In the case of corporate cards, it is reasonable to take the position that verification of the company in accordance with the guidance in Part I does not routinely require verification of all the individuals associated therewith.

2.22 In both cases, the risk posed to a firm's reputation in having insufficient data to identify a secondary cardholder featuring on a sanctions list or being a corrupt politically exposed person, and the potential liability arising from a breach of sanctions or a major money laundering or terrorist financing case, renders it prudent for the data collected to be full enough to mitigate that risk.

2.23 A merchant is a customer for AML/CTF purposes of the Merchant Acquirer.

Customer due diligence

2.24 In most cases, the Card Issuer would undertake the appropriate customer due diligence checks itself, or through the services of a credit reference agency, but there are some exceptions to this:

- where the Card Issuer is issuing a card on behalf of another regulated financial services firm, being a company or partner (in the case of affinity cards) that has already carried out the required customer due diligence
- introductions from other parts of the same group, or from other firms which are considered acceptable introducers (see Part I, section 5.6)

2.25 Although not an AML/CTF requirement, approval processes should have regard to the Card Issuer's latest information on current sources of fraud in relation to credit card applications.

2.26 Card schemes carry out surveys and reviews of activities related to their members. For example, one scheme carried out a due diligence review of the AML/CTF standards of all its members domiciled in high risk countries. Card Issuers should be aware of such survey/review activity.

2.27 Where corporate cards are issued to employees, the identity of the employer should be verified in accordance with the guidance set out in Part I, paragraph 5.3.121.

2.28 The standard verification requirement set out in Part I, Chapter 5 should be applied, as appropriate, to credit card and store card holders, although ascertaining the purpose of the account, and the expected flow of funds, would not be appropriate for such cards.

2.29 A risk-based approach to verifying the identity of secondary cardholders should be carried out as follows:

- The standard information set out in Part I, paragraph 5.3.70 should be collected for all secondary cardholders and recorded in such a way that the data are readily searchable.
- Firms should assess the extent to which they should verify any of the data so obtained, in accordance with the guidance set out in Part I, paragraph 5.3.71, from independent documentary or electronic evidence, in the light of their aggregate controls designed to mitigate fraud and money laundering risks, and bearing in mind the extent to which the firm applies the risk controls set out in paragraph 2.18. However, there is a presumption that such verification will be carried out, other than in the following circumstances.
  - In the case of store cards, because of the restrictions on their use, see paragraph 2.6.
  - In the case of commercial cards, because of the restrictions on their issue, see paragraph 2.7, although a firm's risk-based approach may deem it prudent to verify employee cardholders of their smaller commercial card customers.

Where a firm employs a low risk strategy of issuing additional cards only to close family members who reside at the same address as the primary cardholder, and the additional cardholder is a close family member whose employment, or continuing education, dictates that they are not permanently resident at the address, then for purposes of verification the primary cardholder's address shall be the main residential

address. This will be acceptable as long as the mailing address for the additional cardholder remains the same as the primary cardholder's address.

In all these situations, firms will still need to consider other types of due diligence check on additional cardholders, e.g., against sanctions lists.

2.30 In relation to branded and affinity cards, where another regulated firm has the primary relationship with the cardholder, the partner organisation would need to undertake that it holds information on the applicant, and that this information would be supplied to the card issuer if requested.

2.31 In respect of a merchant, the Merchant Acquirer should apply the standard verification requirement in Part I, Chapter 5, adjusted as necessary to take account of the activities in which the merchant is engaged, turnover levels, the sophistication of available monitoring tools to identify any fraudulent background history as well as transaction activity, and the location of the bank account over which transactions are settled.

2.32 Where functions in relation to card issuing, especially initial customer due diligence, is outsourced, the firm should have regard to the FSA's guidance on outsourcing (www.fsahandbook.info/FSA/html/handbook/SYSC/8). In particular, Card Issuers should have criteria in place for assessing, initially and on an ongoing basis, the extent and robustness of the systems and procedures (of the firm to which the function is outsourced) for carrying out customer identification.

2.33 It would be unusual for a Card Issuer to revisit the information held in respect of a cardholder. Credit cards are primarily a distance transaction process. An account is opened (after due diligence checks are completed), a balance is acquired, a bill sent and payment received. This cycle is repeated until card closure and the majority of cardholders rarely, if ever, contact the Card Issuer.

Enhanced due diligence

2.34 An issuer should have criteria and procedures in place for identifying higher risk customers. Such customers must be subject to enhanced due diligence. This applies in the case of customers identified as being PEPs, or who are resident in, or nationals of, high-risk and/or non FATF jurisdictions.

2.35 Firms' procedures should include how customers should be dealt with, depending on the risk identified. Where necessary and appropriate, reference to a senior member of staff should be made in unusual circumstances. This will include getting senior manager approval for relationships with PEPs, although the level of seniority will depend on the level of risk represented by the PEP concerned.

Monitoring

2.36 It is a requirement of the ML Regulations that firms monitor accounts for unusual transactions patterns. Controls should be put in place for accepting changes of name or address for processing.