



# EUROPEAN FINANCIAL COALITION

against Commercial Sexual Exploitation of Children Online



## European Financial Coalition:

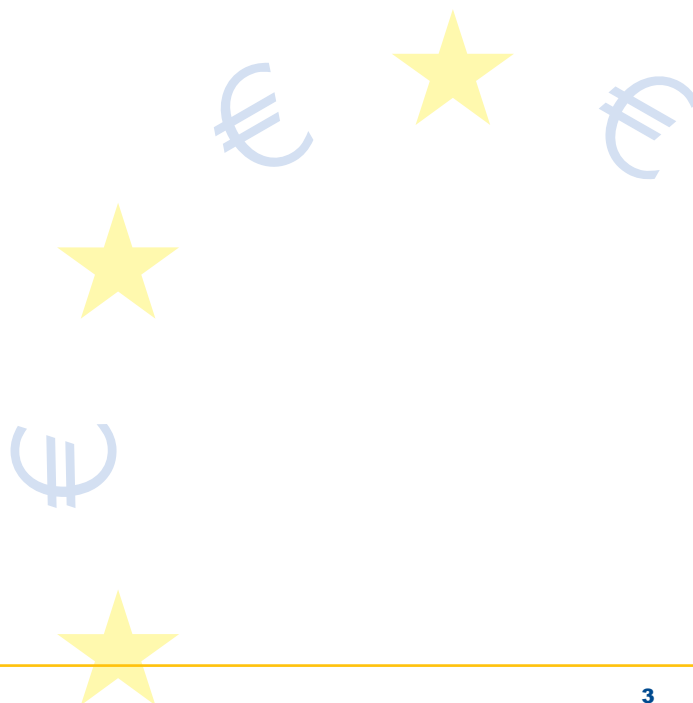
Best practice guidance for the financial industry  
on the prevention and detection of commercial  
child abuse images





## Contents

Executive summary	5
<b>1 The European Financial Coalition</b>	<b>9</b>
1.1 Background to the European Financial Coalition	9
1.2 Introduction	10
<b>2 Internet payment processing acquisition and monitoring</b>	<b>11</b>
2.1 Merchant monitoring	11
<b>3 Online payment processors</b>	<b>17</b>
3.1 Policy	17
3.2 Internal Models and Detection Tools	17
3.3 People	17
3.4 Public – private partnerships	17
<b>4 E-money providers</b>	<b>19</b>
4.1 Guidance	19
<b>5 Prepaid</b>	<b>21</b>
5.1 The prepaid card market	21
5.2 Establish a Risk Management Strategy	21
5.3 Types of prepaid cards and mitigation	23
5.4 Summary	26
<b>6 Conclusion</b>	<b>27</b>
Appendix A Glossary of terms	29
Appendix B Prepaid card system infrastructure	30





## Executive summary

### 1. Objective of the Best Practice Guide

This document contains a compilation of best practices found within the payment industry, offering practical ways to reduce the risk of acquiring illegal or prohibited goods or services, in particular those of commercial child abuse images. They cover the development of policy, the merchant application and verification process, as well as persistent monitoring to ensure that this criminal activity is kept out of the payment system. These best practices are being shared in an attempt to raise awareness of this issue, and to make it more and more difficult for criminals to take advantage of payment systems to facilitate their crimes.

It is important to note that these best practice guidelines are only guidelines and each organisation must establish their own policies, procedures and systems which are appropriate to their transaction environment and business model. The European Financial Coalition (EFC) recognises that each organisation will have different business models and products and not all the guidance contained in this document will be applicable to or effective for all entities. The EFC also recognises that the rapid advance of technology and the growing sophistication of the criminals producing, distributing and purchasing commercial child sexual abuse images means that constant vigilance is required to ensure that each organisation's policies and procedures remain fit for purpose.

### 2. Internet payment processing acquisition and monitoring

The guidance in the first section is written from the perspective of payment card schemes such as Visa, MasterCard and American Express and relates to the way that Merchant Acquirers interact with Merchants, content providers, aggregators and third party payment processors to facilitate the acceptance of their payment products. Due diligence is required in each step –from recruitment, through transaction management, to issue identification, resolution and reporting.

This first step relates to the development and integration of policies that prohibit commercial child abuse images within the wider policy relating to regulatory diligence and brand protection.

The second step relates to the Merchant application process which is an effective tool for verifying the Merchant's identity, its credit qualifications and assessing its potential risk for fraud and other legal exposure. It should also be used to gain a thorough understanding of the Merchant's business model and product/service offering, so that this can be reviewed against the financial institution's own and the payment card scheme rules and policies.

As with any Merchant, online Merchants must be subjected to rigorous screening prior to acquisition. The application and underwriting process provide an excellent opportunity to learn more about the merchant and how it conducts business and to begin to identify tracking data points that will be useful in ongoing risk analysis.

The due diligence involved at this stage will cover all relevant aspects of the merchant's business background.

The third step relates to the monitoring of the existing Merchant portfolio's online presence, including the processing activities performed through Internet Payment Service providers or other forms of third party or intermediary services. It may be advisable, given the volume of work associated with this current Merchant online presence identification to use reasonable risk prioritisation to determine the most effective way to mitigate risk as quickly as possible, e.g. by focusing first on 'high risk' transaction types and merchants who may have high risk profiles.

Specific attention, in this monitoring activity, should be devoted to the activity of aggregators or referral merchants who can be easily used by unwanted merchants as a disguised route into the payment chain.

The fourth step relates to the fact that due diligence during the acquisition process must be complemented by a persistent monitoring of the Merchants for volume, content and relationship changes. Therefore, the EFC Best Practices guidance recommends that any Merchant monitoring programme include a combination of proactive and persistent site monitoring steps, which will include reporting violations to Law Enforcement through the country's domestic hotline.

## Executive summary

### 3. Online payment processors

As with payment card schemes, online payment processors should have a zero tolerance policy for the use of their system for illegal material and services and clearly formulate policy statements in their User Agreement, to the effect that any account offering illegal materials and/or services violates the Acceptable Use Policy or Terms of Service and will be subject to immediate closure.

The implementation of a no tolerance policy will comprise the development of detection models and tools as well as the creation of specialised personnel groups focusing on child protection issues.

### 4. E-money providers

As with payment card schemes and online payment transactions, the best practices for e-money providers are based on a clear proactive policy statement combined with merchant customer and transaction monitoring and identification programmes in order to identify if illegal products or services are being sold.

Appropriate resources must be allocated for the prevention and detection of the illegal activities, including through staff awareness raising and training schemes.

### 5. Prepaid

Here again, it is important, that, whatever the type of prepaid card concerned, the issuer must establish policies, processes and procedures that address all aspects of risk and suitable acquisition of third party associates, while ensuring that the authorisation of such policies, processes and procedures is driven and authorised by Board level management and subject to regular review and updating.

The best practice distinguishes, with regard to the procedures for risk mitigation, between the different types of prepaid cards, according to the level of ID and address verification to which the purchaser is subjected.

Specific mitigation techniques and best practices are proposed for each of the following categories, which are considered as presenting a higher risk due to the absence of full verification of the customers: giftcards, open loop cards; non personalised instant issue cards; Simplified Due Diligence cards (personalised and posted).

Separate requirements and recommendations are formulated for cards issued after full verification of ID and address of customers. Such cards mitigate the risks associated with criminal activities, but do not rule out illegal use of the card. Therefore the verification of the identity which is an important part of Customer Due Diligence (CDD) is only part of the process of understanding the transactions that the cardholder is likely to conduct and the purpose of why the consumer has opted to use a prepaid card. An ongoing monitoring of the transactions focusing on certain types of risk indicators is suggested.

Finally, reference is also made to the benefits of customer's personal data and customer transaction data record keeping requirements.

Each Issuer of prepaid cards and their third party associates should take into account the expected market segment through which the product will be purchased, how the card can be loaded with funds and the channels through which those funds can be spent. The conclusions drawn from the assessment will signify the levels of due diligence that should be applied to acceptance of the applicant and the controls that must be applied throughout the business relationship. Risk assessment cannot stop during the application and transaction process, but must be included in an on-going organisational culture of awareness to the vulnerabilities of the products supported by the company.



3295 1100

LEVIN TRON



## 1. The European Financial Coalition

### 1.1 Background to the European Financial Coalition

The European Financial Coalition against commercial sexual exploitation of children online (EFC) was established in July 2009 and developed to combat internet child exploitation and child sexual abuse imagery in the European Union. Funded by the European Commission and led by the UK's Child Exploitation Online Protection (CEOP) Centre, the EFC involves a unique partnership approach by stakeholders, including law enforcement agencies, financial payment systems providers, banks, internet service providers and non-governmental organisations (NGOs) to create a flexible and dynamic task force. The make up of the EFC consists of a Steering Group and five working groups who represent the key sectors involved in the coalition. These include the Payments Industry Working Group, the Law Enforcement Co-Operation Working Group, the Internet and Technology Working Group, the Legal Working Group and the Awareness Raising and Prevention Working Group.

The EFC aims to eradicate commercial child sexual abuse imagery and exploitation via the internet through traditional means such as personal computers and mobile telephones, as well as looking at devices such as games consoles and digital music players, all of which can be capable of providing connectivity to the internet.

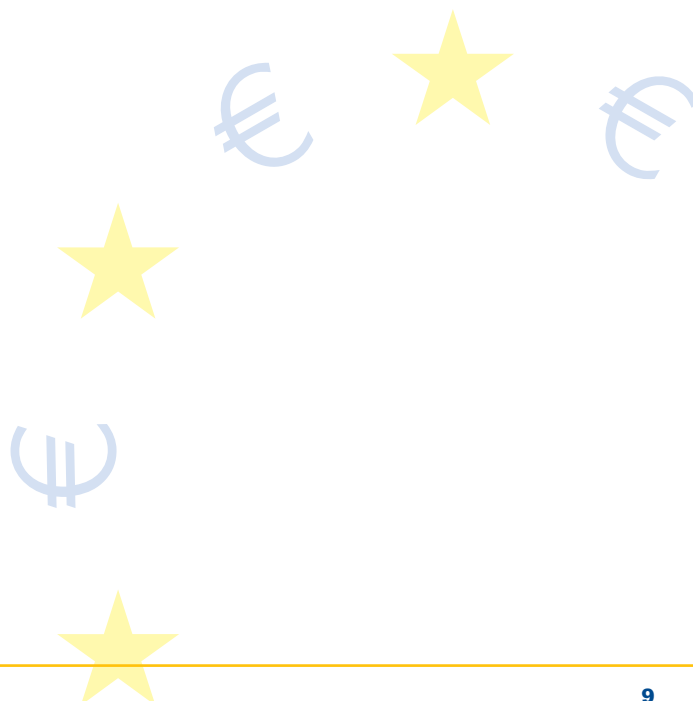
The continued growth of the internet has provided excellent opportunities for legitimate entities to make the most of the new technology and the breadth of audience and content it allows is now truly worldwide. However, along with these opportunities, threats from illegal and disreputable activities have appeared in a small proportion of online content.

The Payments Industry Working Group (PIWG) is currently chaired by Visa Europe and consists of members from MasterCard (co-chair), American Express, PayPal, e-money association, Newcastle Building Society and Western Union. Collectively, these organisations have created this Best Practice guidance for dissemination to financial industries throughout Europe.

This guidance aims to improve the prevention and detection of their systems being utilised by criminals to distribute and/or obtain child sexual abuse imagery and is the culmination of collective best practice from across the financial industry.

#### Contact us

If you would like more information about the EFC, would like to join the PIWG or to comment or contribute to these Best Practices, please contact the EFC Secretariat via the website [www.europeanfinancialcoalition.eu](http://www.europeanfinancialcoalition.eu) or by email [efc@ceop.gsi.gov.uk](mailto:efc@ceop.gsi.gov.uk).



## 1. The European Financial Coalition

### 1.2 Introduction

To reduce a financial institution's risk of reputational and financial damage as well as working to prevent abuse of the system (combating the commercial sale and exploitation of children) associated with these activities, the European Financial Coalition believes it is essential to develop content based Internet Payment Processing Guidelines. These guidelines aim to complement existing payment scheme, industry and legal regulations which prohibit the acceptance of payment vehicles for activities which are either illegal in the jurisdiction of the seller or the purchaser.

This document contains a compilation of Best Practices found within the payment industry. These Best Practices offer practical ways to reduce the risk of sellers or purchasers acquiring illegal or prohibited goods or services, in particular those of commercial child sexual abuse images. They cover the development of policy, the Merchant application and verification process, as well as recommend persistent monitoring to ensure that this criminal activity is reduced or kept out of the payment system entirely.

These Best Practices have been produced in an attempt to raise awareness of the issue amongst the payments industry, making it more difficult for criminals to take advantage of payment systems to facilitate their crimes. It is important to note that these Best Practices do not necessarily represent the individual views of the Payments Industry Working Group members and are not intended to be comprehensive.

All organisations are requested to consider them, along with regulatory obligations of their organisation's own Corporate Social Responsibility (CSR) policies to ensure that they are doing all they can to protect themselves and society from being exploited by criminals.

It is also important to note that these Best Practice guidelines are only guidelines and each organisation must establish their own policies, procedures and systems which are appropriate to their transaction environment and business model. The EFC recognises that each organisation will have different business models and products and not all the guidance contained in this document will be applicable to or effective for all entities. The EFC also recognises that the rapid advance of technology and the growing sophistication of the criminals producing, distributing and purchasing commercial child sexual abuse images means that constant vigilance is required to ensure that each organisation's policies and procedures remain fit for purpose.

This document has been produced by current members of the Payment Industry Working Group and it is expected, with more organisations from the payment industry getting involved in the EFC in the future, these guidelines will grow to increase the depth and value of these best practices.

*Appendix 1 provides a glossary for the technical and Industry terms used in this paper.*

## 2. Internet payment processing acquisition and monitoring

The guidance in this section relates to payment card schemes such as Visa, MasterCard and American Express and relates to the way that Merchant Acquirers interact with Merchants, content providers, aggregators and third party payment processors to facilitate the acceptance of their payment products. Due diligence is required in each step, from recruitment and transaction management, to issue identification, resolution and reporting.

The term 'Merchant' will be used in this document to describe the commercial provider of goods/ services and the term 'Acquirer' will be used to describe a financial institution authorised by the relevant payment scheme to enter into agreements with Merchants for Card Acceptance. All 'Acquirers' should take notice and apply these Best Practices.

### 2.1 Merchant monitoring

#### Step 1: Develop policies that prohibit commercial child sexual abuse imagery

Organisations should look to establish a Merchant acquisition policy to include;

- legal requirements;
- payment card scheme requirements; and
- the Acquirer's own recruitment policy.

It is likely this will in turn form part of a wider policy relating to regulatory diligence and brand protection. Board level endorsement should be obtained, enabling them to sign off of the policy (and it's adoption), which should be regularly reviewed to ensure it remains fit for purpose and is well communicated, understood and complied with by the whole organisation.

#### Step 2: Merchant review at acquisition

The Merchant application process is the foundation of an Acquirer's relationship with a Merchant. It is an effective tool for verifying the Merchant's identity, credit qualifications and assessing its potential risk for fraud and other legal exposure. It should also be used to gain a thorough understanding of the Merchant's business model and product/service offering, so that this can be reviewed against an organisation's own and payment card scheme rules and policies.

As with any Merchant, online Merchants must be subjected to rigorous screening prior to acquisition. The application and underwriting process provide an excellent opportunity to learn more about the Merchant and how it conducts business, as well as how to begin to identify tracking data points that will be useful in ongoing risk analysis.

**Merchant history:** Organisations need to obtain the Merchant's authority to research its background, including credit banking, financial history and history of acceptance of payment instruments (card payments etc). The Merchant should be asked to supply information on any other businesses that it owns, operates or has owned in the past. Organisations also need to ask for information on connected entities (partners, affiliates etc) and if the Merchant and/or its principles have any current or previous relations with other financial institutions.

If they have, further details should be requested including banking statements for previous months. If the Merchant has been terminated in the past by another Acquirer, the reasons should be investigated and a decision made to determine if the Merchant remains an acceptable proposition.

If the Merchant will not provide information requested the application should be declined.

**Doing Business as (DBA) or trade name:** Both the DBA and the legal/trade name should be disclosed on the application. Some Merchants may conduct their business under one name and yet trade under a different identifier. It is important to identify all names used and the reasons for them.

## 2. Internet payment processing acquisition and monitoring

**Legal Structure:** Organisations should enquire about the legal form of the Merchant's business. Is the Merchant a partnership, a sole proprietor or a corporation? Verification of business licenses, corporate charters, articles of association or other similar documents should be obtained. Check for consistency between the documents and compare to all the other application information. Remember that publicly available documents such as articles of incorporation are easy to fabricate, so it may be preferable to verify non-public information such as driving licences, passports and utility bills, etc.

**Financial history:** An independent confirmation should be sought into the Merchant's bank account. Compare the account number to the one noted on the application form to ensure a match. The name on the bank account the Merchant wishes to use for deposits needs to match the legal name of the applicant and if it does not, organisations should seek further information from the applicant.

For Merchants with an online presence, the application process (and the Merchant contract) should stipulate that the following information must appear on the Merchant's website:

- customer service number (toll free preferably);
- email address to contact the company;
- statement on security controls;
- delivery methods and timing;
- age verification methodology (for age restricted goods and services);
- refund and return policies;
- privacy statements (permissible uses of customer information); and
- depending on the type of Merchant, terms of service and/or acceptable use policy.

In addition, due diligence by the Acquirer should include investigation into the:

- nature of goods/services;
- design of the home-page and location of billing page/s;
- transaction patterns;
- Merchant location (physical and legal); and the
- business model (one-off transaction, or regular billing. If regular billing, the conditions and cancellation policy should be very clear to the customer);
- average (or projected) turnover;
- average (or projected) refund volume;
- average (or projected) chargeback and fraud rates;
- average (or projected) refund rates and refund policy;
- disclosure of all payment mechanisms offered; and
- disclosure of all sales channels (including all URLs or referral sites).

The Merchant's telephone number, email address, listed personnel and other contact information should all be checked for validity.

Background and reference checks for Merchant principals, partners or owners should be made, using personal and business credit reports to better assess the risks and make a more informed decision. Additionally, organisations should obtain bank and trade references as appropriate, to validate that the business is legitimate and in good standing with its creditors. Compare contact information (address and phone number) on the application with that which appears on the credit reference.

## 2. Internet payment processing acquisition and monitoring

Check the Merchant's website(s) to ensure that the products or services, the pricing, contact details and refund policies etc all match with the descriptions made on the application. This information should be stored and reviewed regularly to identify changes, which should in turn be reviewed against acceptable norms.

It is also recommended that Acquirers review every new Merchant against a robust malcontent database<sup>1</sup> during the Merchant acquisition or evaluation process. (This database could be administered in-house, or by a reputable third-party provider).

Such investigation should include, but not be limited to:

**Acquisition Investigation:** Acquirers should use a tool that allows them to enter a target URL and receive a risk response based upon their own or their vendor's database and preliminary investigation. Specifically, such a response should:

- Query a mal-content database to confirm that the target URL does not match any IP, URL, address, Who is linking, or other data in the malcontent system
- Provide basic reporting data, including but not limited to: IP address, Whois, key scoring for all targeted mal-content.

### Note

**Some Merchants (generally the kind of Merchants that an Acquirer would try to avoid) attempt and are sometimes successful, in gaining entry to the payment chain through indirect routes. Undesirable Merchants may 'disguise' their real business activities in order to gain payment acceptance through an Acquirer. If this occurs, it is subsequently impossible for an issuing bank to determine a Merchant's 'true' nature and apportion an accurate risk scoring to that Merchant's transactions.**

**It is for this reason that due diligence investigation, both prior to acquisition and on a continual basis, is essential to provide a robust defence against these entities.**

By using these Best Practices, Merchant Acquirers will be able to identify potentially problematic Merchants before they begin processing; they will establish key metrics that can be used to identify changes in Merchants' businesses and they will reduce their financial and reputational risk within the e-commerce environment.

### Step 3: Current Merchant Online Identification

One of the greatest immediate dangers for an Acquirer is that they may be currently unaware of the extent of their existing Merchant portfolio's online 'presence'. If Acquirers do not know that their Merchant is trading online, they are not in a good position to be able to provide adequate guidance for the Merchant and protection for themselves and the payment system. Such Merchants may have legitimate reasons for trading online, however they may (possibly unwittingly) be at a greater risk of data compromise or excessive disputes and the Acquirer may be unwittingly allowing transactions for internet based content which they would not normally allow. Alternatively, as explained above, some Merchants will seek to disguise the true nature of their goods or services and this may be achieved by pretending to have only face-to-face transactions.

There are various ways in which an Acquirer can monitor and identify the 'totality' of their Merchants that are trading through the internet:

- Review the Acquirer's current portfolio for Merchants who have a known 'online' presence (i.e. a website) even if an online payment facility has not been declared.

<sup>1</sup> The Malcontent database should record all 'touch-points' previously identified as referencing entities that do not comply with the payment schemes' or member's rules. These 'touch-points' could include (but not be limited to):

- URL;
- doing business as name;
- trading name;
- principal (business owner/s);
- who's data; and
- IP address.

## 2. Internet payment processing acquisition and monitoring

- Employ a third-party company to search the internet for Merchants offering or purporting to offer a payment relationship between themselves and the Acquirer.
- Finally, Acquirers can scan their list of offline Merchants to determine if they have an online presence.

**Member's known E-Commerce Merchants:** Acquirers should begin by collating and detailing information about their existing 'known' e-commerce Merchant base. Acquirers should check whether their existing Merchant database has an up-to-date and comprehensive list of website URLs associated with the Merchant. As well as reviewing the content of each URL, Acquirers should also take the opportunity to review their Merchant contracts and the Merchants' compliance with internal regulations to ensure the complete safety of the payment environment.

Acquirers must also ensure they understand and are aware of all Merchants processing through Internet Payment Service Providers (IPSP's) or any other form of third party or intermediary. Such third parties aggregate sales volume from 'sponsored Merchants' they provide payment services for and can pose a significant additional risk to the payment system, as they enable disintermediation between the Merchant and the Acquirer. If an Acquirer is not diligent in their monitoring of IPSP and connected entities, they may discover that they are acquiring Merchants offering goods, services or online content that are either illegal or non-compliant with payment scheme regulations.

### Note

#### Client's Existing Merchant Database

As noted above, one of the most important things any payment industry member can do to help identify and reduce their e-commerce risk is to identify which Merchants are online. All Acquirers should develop and execute a plan to identify which of their Merchants are online. This can be accomplished by in-house efforts or through the use of third party investigative firms. The goal should be to use a variety of search and identification procedures to identify sites where the Acquirer's Merchants are accepting payment online.

Reviewing all Merchants can be a daunting task. Therefore, the Acquirer should use reasonable risk prioritisation to determine the most effective way to mitigate risk as quickly as possible. These Best Practices suggest that when this cannot be accomplished in one project, the effort be broken up into areas of relative risk over a period of months. The first group should be 'high risk' transaction types and Merchants who may have high risk profiles. The next grouping should be all Merchants who have had 'Card Not Present' transactions within the past year or who have registered with the Acquirer for e-commerce transactions. The third group should be any Merchants who show an increase in volume beyond their stated targets or show a sudden spike in traffic from geographically diverse consumers. Finally, Acquirers should begin the process of investigating the rest of their database.

**The rest of the Acquirer's Merchant Portfolio:** Identifying and monitoring the 'known' e-commerce Merchants is a very positive first step for Acquirers, but will not guarantee complete protection from unwanted Merchants or unknown Merchant activity. Acquirers may have an incomplete picture of their Merchants' presence on the internet. For example, a Merchant's business may evolve over time and they may set up a web-site for payment without informing their Acquirer. Alternatively, a Merchant may set up a web-site for the sale of goods or services entirely unrelated to the activities that the Acquirer recorded at the time of Merchant acquisition. This can create a significant additional risk to the Acquirer and to the payment system generally.

**Aggregators/Referral Merchants:** Organisations that act as aggregators or referral Merchants can pose a significant risk to an Acquirer. Unless an Acquirer demonstrates constant due diligence with respect to these organisations, they can easily be used by unwanted Merchants as a disguised route into the payment chain. Acquirers must show extreme care when dealing with these types of organisation, to demonstrate that they understand not only the business model and activities of the aggregator/referral Merchant, but also of all the entities that these organisations bring into the payment chain.

## 2. Internet payment processing acquisition and monitoring

The EFC strongly recommends that all Acquirers monitor these organisations to highlight all relationships that exist and all URLs that are associated to them. Examples of such organisations include (but may not be limited to):

- Internet Sales Organisations (ISO);
- Internet Payment Service Providers (IPSP);
- e-wallets, or other quasi-cash providers;
- shopping carts or other payment aggregators; and
- membership 'clubs'.

### Step 4: Persistent Analysis

The main underlying principle of the EFC Best Practice guidance is Know Your Customer (KYC). KYC requires thorough due diligence during the acquisition process and it requires Acquirers to persistently monitor their Merchants for volume, content and relationship changes.

Therefore, the EFC best practice guidelines recommend that any Merchant monitoring programme include a combination of proactive and persistent site analysis. Acquirers should ideally review every page on every site no less than every 30 days. If this is not possible, due to the Acquirer's choice of monitoring tool, then 'sampling' of the Acquirer's Merchant portfolio may be acceptable, provided the Acquirer can demonstrate the adequacy of the sampling.

This activity can be accomplished in house by some Acquirers. Where this is not an option, third party specialist organisations may be able to assist. The EFC best practice guidance recommends the following persistent monitoring steps:

**Identify Target Sites:** Acquirers should identify their e-commerce Merchants as noted above. All reasonable efforts should be made to identify all ISOs, IPSPs, e-wallets and sponsored Merchants.

**Content Targets:** Acquirers should clearly identify the content violations (child abuse imagery as well as other violations) to both the payment schemes' and the Acquirer's own rules and policies. Additional concerns regarding Merchant business model, MCC code and policy violations (billing policies, return policies, etc) should all be identified through regular monitoring.

**Filter and Score Sites:** If a technology solution is used for web crawling, the Acquirer (or technology partner) should dynamically score the reviewed pages based on content, links and other mal-content precursors. This scoring data should be used to determine which pages are forwarded to an analyst for human confirmation and action.

**Review & Confirm:** Each site that meets the stated thresholds of an organisation (as determined by scoring algorithms) should be reviewed by a trained analyst to confirm such content meets your risk threshold criteria.

**Action & Report:** If there is a confirmed violation, the entity wishing to report the violation should make the first report to Law Enforcement through their own domestic in-country hotline. Following this, the Acquirer must also report the violation to the relevant payment schemes.

**Monitor & Review:** After the Acquirer's total e-commerce Merchant portfolio has been established, the Acquirer should examine each Merchant's web pages for changes on a monthly basis, or if this is not possible, then sampling may be acceptable. When changes are detected, the Acquirer should determine if the changes are relevant (for further investigation) and forward them to an analyst for confirmation.



### 3. Online payment processors

The guidance in this section relates to the online payment processors, for example the PayPal model. This section does not replace, but instead builds on, the previous section.

Outside of the traditional Merchant-Acquirer relationship, there are additional business models that have joined the payment space. Online payment processors, whilst they may function under a different set of regulations, should still maintain a high level of due diligence and develop a robust system for detecting illegal activity.

#### 3.1 Policy

As with payment card schemes, online payment processors should have a zero tolerance policy for the use of their system for illegal material and services.

Organisations should clearly state in User Agreements that any account offering illegal materials and/or services violates the Acceptable Use Policy or Terms of Service and will be subject to immediate closure.

#### 3.2 Internal Models and Detection Tools

Closed loop systems provide a unique opportunity to examine user behaviour and develop proprietary models.

Modelling tools should include the use of a keywords list to allow for quick identification of users attempting to abuse the system. The keywords list should be kept fully updated. Organisations should continue to invest and develop learning in this area to keep internal models fresh. Channels should also be developed to allow the public to alert organisations to any violations and route reports to the appropriate team for quick action.

Similar to other brands, organisations should consider the use of external vendors to search the internet for potential violations.

#### 3.3 People

It is suggested that organisations develop a group of specialised personnel who focus on child exploitation. Training should be sought from entities such as law enforcement and non-governmental organisations (NGOs) that are experts in this area, to ensure staff are fully trained to identify high risk behaviour. Training of staff should be continuous to ensure skills are kept up to date, invest in training and mentoring programs for specialised teams, including internal and external training, online libraries and other resources to ensure they have the most up to date reference materials.

In addition to using detection models, a research program should be developed where staff can research industry trends, news, events and explore next generation technology.

#### 3.4 Public – private partnerships

It is important for organisations to be proactive and develop relationships with law enforcement, regulatory and non-governmental organisations specialised in this area. This will allow for the exchange of information and intelligence and ensure that emerging trends are quickly identified and strategies developed to prevent the misuse of systems, particularly in the areas of new technologies or payment methods.





## 4. E-money providers

Electronic money (e-money) is a pre-paid payment product accessible to consumers through an online account, a card or a voucher that can be used to make purchases at physical or e-commerce Merchants. In Europe, e-money can only be issued by authorised and regulated firms.

Payment services can also be offered by payment institutions that are regulated to offer other payment services such as fund transfers, issuing of credit cards and acquiring of payments.

These guidelines are suggestions for good practice and are not binding. It is the responsibility of each payment service provider to establish its own policies and procedures appropriate to its respective business model and perceived risk of abuse.

### 4.1 Guidance

E-money and payments institutions should adopt a proactive approach to ensuring that their products are not used to support illegal activities, including the sale and distribution of illegal images of children. Responsibility for ensuring that e-money and other payment products and services are not used for illegal purposes, including the purpose of supporting the distribution of child sexual abuse images, should be allocated to a suitable senior manager.

Customers should be clearly advised that their e-money or other payment product should never be used for any form of illegal activity. E-money providers should establish an 'acceptable usage' policy which includes policy on content for which the provider will not allow payment using its products.

Initial due diligence of Merchant customers should ascertain the nature of the Merchant's business. This should include reviewing the Merchant's website to confirm the type of products or services being provided and whether the Merchant adheres to acceptable content or services policies. As part of these ongoing due diligence procedures, Merchant customers should be routinely reviewed to identify if illegal products or services are being sold and if the Merchants' business activities are correctly classified.

Transaction monitoring systems and procedures should include parameters and alerts to identify illegal transactions, including those involving the possible sale of illegal child abuse material.

All relevant staff should be made aware of the risk that their payment products could be used for illegal purposes including the distribution of child abuse images. Training should include information that will enable relevant staff to recognise scenarios that may be related to illegal activities, including the sale of child abuse images.

Procedures for dealing with transactions relating to illegal matters, including those identified as being related to the distribution of child abuse images (including escalation routes to law enforcement), should be formally documented and communicated to all relevant staff.

The potential use of e-money and other payment products for illegal purposes including the distribution of child abuse images should be recognised and appropriate resources allocated for the prevention and detection of financial crime. Monitoring for indicators that may suggest that distribution of child abuse images is taking place should be undertaken. The E-Money Association will seek to communicate typologies to its members and provide access to information provided by law enforcement and regulators as well as information from other payment service providers.





## 5. Prepaid

The guidance written in this section focuses on Prepaid Card Issuers based in the UK and relates to the way that Issuers interact with their Programme Managers, cardholders and third parties, which conduct transaction processing on behalf of the Programme Manager. Recommendations within the document have been built upon UK standards which have been implemented to satisfy EU Directives.

This guidance will illustrate a range of different types of prepaid cards available in the market, purchase channels, spend options and the various levels of due diligence conducted upon the cardholder.

The aim is to provide 'Best Practice' guidelines for the issue and use of prepaid cards and how restraints can be applied to mitigate opportunities of illegal and disreputable use of the cards for internet-based child exploitation and sexual abuse.

### 5.1 The prepaid card market

Prepaid cards can be offered in various forms and range from gift cards to corporate loaded 'open-loop' expense cards. These products may be purchased face-to-face, online or by postal application. The cards can be used for cash withdrawal at ATM's, purchases online, purchases at Merchant outlets or electronic money transfers. Prepaid cards can be offered to individuals and markets that may not typically have access to cards and electronic payment facilities, such as young people and the un-banked. Prepaid cards can offer additional security in environments where cash is normally the only alternative.

However, with this new and growing market comes a responsibility to manage these offerings in a way that does not introduce danger or reputational damage into the payments system.

Most prepaid schemes require the identity and address of applicants to be fully verified. Consumer checks include verification of identity and address but, as credit searches are not conducted (because credit is not offered in the case of prepaid), registration of a 'footprint' on reference files is not performed. Consequently, it is not as easy for law enforcement agencies to identify persons who hold prepaid cards as opposed to those individuals who are credit or debit card holders.

However, Simplified Due Diligence (SDD) permits organisations to accept customers without completing the full due diligence process. It can only be used for products that are regarded to be of a lower risk and regulatory guidance has implemented stringent requirements of usage. In such cases, monetary limits and conditions are imposed to mitigate the associated risks to card issuers and Program Managers<sup>2</sup>. JMLSG Guidance Notes state that the identity of the customer must be verified prior to the limits being reached. Should the limits be reached prior to identification being confirmed, the card account must be frozen until requirements are satisfied.

### 5.2 Establish a Risk Management Strategy

The Issuer must establish policies, processes and procedures that address all aspects of risk and suitable acquisition of third party associates. Organisations must ensure that authorisation of policies, processes and procedures is driven and authorized by Board level management and are regularly reviewed and updated. All documents should be readily available for staff and relevant third parties to read and acknowledge as understood. Competency testing and audits should ensure that staff understand and implement the stated controls.

*(Refer to Appendix 2 for diagram of Prepaid Issuer infrastructure).*

#### Appointment of a Processor

- Conduct corporate due diligence against the firm;
- assess to suitability of systems including audit controls and record retention procedures;
- confirm that the system can apply blocks to certain types of attempted Merchant transactions;
- confirm the system can decline transactions that exceed authorised parameters; and
- establish if the system can send warnings/alerts to Issuers and/or Program Managers.

## 5. Prepaid

### Appointment of a Program Manager (PM)

- Conduct corporate due diligence against the firm;
- assess the type of market segment to which the PM's business is focused;
- assess the type of schemes that the PM intends to provide;
- assess the mediums that the PM intends to use and analyse associated risks; and
- assess the systems and controls that the PM intends to use and if gaps are identified, advise upon necessary improvements.

### Selection of Customer Verification System

- Conduct corporate due diligence against the firm;
- confirm the databases searched and acceptance criteria used for proof of customer identity;
- confirm how controls are implemented and managed;
- confirm the restrictions that can be applied for data access;
- assess to overall suitability of systems including audit controls and record retention procedures.

### Selection of a Monitoring System

- Conduct corporate due diligence against the firm;
- assess the controls and rules that apply to adequate monitoring of transactions and customer activities;
- confirm how alerts will be managed;
- establish if a 'hot-list' system is available;
- confirm if monitoring is conducted real-time or post-transaction;
- confirm if a stop and/or alert facility is available; and
- assess the suitability of systems including audit controls and record retention procedures.

### Card scheme application assessment

- Assess the general card requirements and if they fit the risk appetite of the Issuer;
- assess the type of card scheme required and the financial value parameters requested;
- assess if the scheme can be provided under SDD or if full verification is required;
- assess the access channels for purchase and use of the card;
- assess how and where the card will be marketed;
- ensure that marketing material meets all legal and industry advertising standards;
- provide a risk analysis of the scheme proposal; and
- record approval by senior managers of the scheme to enable it to go 'live'.

<sup>2</sup> JMLSG Guidance notes: '(d) electronic money, within the meaning of Article 1(3)(b) of the electronic money directive, where:—

(i) if the device cannot be recharged, the maximum amount stored in the device is no more than €150; or

(ii) if the device can be recharged, a limit of €2,500 is imposed on the total amount transacted in a calendar year, except when an amount of €1,000 or more is redeemed in that same calendar year by the bearer (within the meaning of Article 3 of the electronic money directive).'

Non-reloadable purses: where electronic money purses cannot be recharged, and the total purse limit does not exceed €150, verification of identity does not need to be undertaken. This takes into account the ability of individuals to purchase multiple purses and to therefore accumulate a higher overall total of purchased value.

## 5. Prepaid

### 5.3 Types of prepaid cards and mitigation

The guidance in this section will now cover the risks associated to prepaid cards and recommended mitigation and advise on best practice guidelines, to reduce opportunities of illegal and disreputable use of the cards for internet-based child exploitation and sexual abuse.

When assessing the risk of fully verified cards against those issued where verification is not fully conducted, the analysis indicated that the criminal is more likely to purchase the SDD version of a prepaid card. Consequently, for the purpose of this best practice guidance, SDD and Instant Issue products have been focused upon.

#### Gift Cards – open loop

##### Risks

- Can be used by Merchants face-to-face or for Merchant internet purchases;
- type of Merchant may not be restricted;
- purchaser details may not be recorded;
- cardholder details may not be recorded;
- cards will be passed person-to-person and the end user not known;
- cards are activated at point of sale or are ready activated; and
- can be purchased with cash.

##### Mitigation and Best Practice

- Maximum purse value restrictions;
- unable to re-load (add additional) funds;
- decline online use of open-loop gift cards;
- restrict Merchant or/and goods availability;
- require purchaser details to be recorded;
- require cardholder details to be recorded; and
- require cardholder to register for activation of card.

#### Instant Issue Cards (non-personalised)

##### Risks

- Can be purchased from a variety of outlets and Merchants;
- purchaser details may not be recorded;
- cards are activated at point of sale;
- can be used by Merchants face-to-face or for Merchant internet purchases;
- no postal communication with customer;
- cash loading permitted; and
- potential of no audit trail formed by credit or debit card loads.



## 5. Prepaid

### Mitigation and Best Practice

- Maximum purse value restrictions in accordance with SDD parameters or lower;
- decline online use of instant issue cards;
- restrict Merchant or / and goods availability;
- require purchaser details to be recorded;
- require cardholder to register for activation of card; and
- send 'Welcome Pack' to provided address.

### Simplified Due Diligence Cards (personalised and posted)

#### Risks

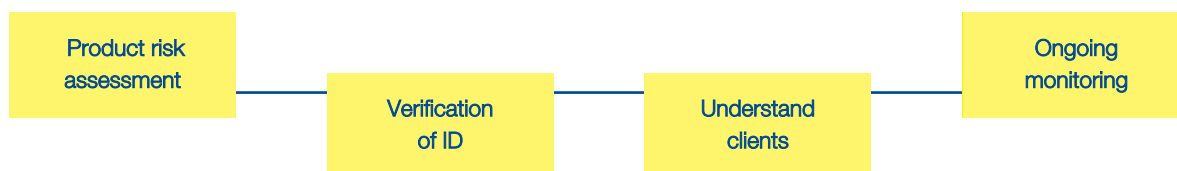
- Personal data provided may not be true;
- provided address may not be the true residential address of the applicant;
- can be reloaded by cash or electronic transfer; and
- can be used in-store and internet.

### Mitigation and Best Practice

- Maximum purse value restrictions in accordance with SDD parameters;
- personal data of the applicant is recorded but not verified;
- postal communication to address provided creates an audit trail;
- require cardholder to register for activation of card; and
- consider restricting/declining online access.

**Cards issued after full verification of customers:** Cards provided to applicants who have satisfied verification of ID and address mitigate the risks associated with criminal activities. However, it must be noted that illegal use of the cards cannot be ruled out simply because the cardholder has satisfied due diligence checks. Continuous assessment of the customer relationship must be part of company processes and procedures.

**Ongoing Monitoring:** Verification of identity is the essential part of the Customer Due Diligence (CDD) process. However, it is important to understand that it is only a part of the continual process of understanding the transactions that the cardholder is likely to conduct and the purpose of why the consumer has opted to use a prepaid card.



## 5. Prepaid

It is a requirement of the Regulations that there is a system implemented which performs monitoring of transaction activity. This process may be performed by manual procedures or by automated systems. Such a process can be applied in two stages:

**Stage 1:** Identification of transactions that represent illegal activities including money laundering, fraud or disreputable usage.

**Stage 2:** Review the transaction, assess the risk and decide on the appropriate action.

For the purpose of this guidance, risk indicators may include:

- multiple card opening from same address or other shared data triggers;
- unexplained batch purchase of gift cards;
- frequent online transactions of small to medium values to suspect Merchant codes;
- low value load followed by online purchase from suspect Merchant code;
- transactions involving services the cardholder has not previously used and particularly if the service seems inappropriate for that cardholder; and
- frequent payments for top-ups to mobile phones.

**Record Keeping:** In the UK, the Money Laundering Regulations require that records of transactions and customer information are retained for a minimum of:

- customer personal data – five years after the cessation of the customer relationship; and
- customer transactions – five years from the date of the transaction.

Regulations across Europe may of course vary from this.

**Customer personal data:** Includes name, address and date of birth and the documents or electronic verification sources that have been used (if applicable). Additional desired data can include nationality, land and or mobile phone numbers, email address, IP address and expected source of funds.

**Customer transaction data:** Includes amount, credit/debit, source of funds, payee, type of spend (i.e. ATM/online/point of sale), Merchant type and balance of account.

The recording of such data, even for SDD products, is imperative to assist in investigations of disreputable or illegal activities. Whilst some of the suggested data may not be recorded in all instances, analysis of available information can identify trends that can locate and apprehend the criminals.

### Training of Personnel

Systems and processes are only as good as the staff that manage and use the data, understand the associated risks and know what the next steps should be.

Staff training should be delivered to all personnel who have access to customer or transaction systems. The training content should be pitched to the level of responsibility and type of work that the employee conducts. However, even where the employee is liable to observe or have access to limited systems, training to detect potential money laundering or suspicious activity is essential.

Staff should be trained at the commencement of their employment. If they move to another role that has different or increased potential risks, annual refresher training should be delivered and at any time that new risks are identified. The training should include competency testing and records should be kept covering retention of the delegates, training content and date of delivery.

## 5. Prepaid

### 5.4 Summary

Best practice can be suggested for the supply and use of prepaid cards and e-money services. Each Issuer and their third party associates should take into account the expected market segment through which the product will be purchased, how the card can be loaded with funds and the channels through which those funds can be spent. The conclusions drawn from the assessment will signify the levels of due diligence that should be applied to acceptance of the applicant and the controls that must be applied throughout the business relationship.

Risk assessment cannot stop during the application and transaction process, but must be included in an on-going organisational culture of awareness to the vulnerabilities of the products supported by the company.

Whilst an argument could be presented that an individual has a right to privacy, equating the right to withhold their personal details under certain financial circumstances, firms should consider the implications of potential misuse of prepaid cards. Providing that the product is managed effectively and a risk-averse culture is adhered to by all stakeholders, prepaid cards are a valuable commodity for the provision of a compliant financial service.

## 6. Conclusion

The European Financial Coalition believes that the Best Practice guidelines detailed within this document should help all Payment Processors understand what types of controls and monitoring they should have in place to combat internet child exploitation and child sexual abuse images from being distributed.

However, organisations must regularly review their own policies and practices to ensure that they remain 'fit for purpose' in protecting themselves and the payment industry from financial and reputational harm.

The consistent common themes running throughout the different sections of this document are the importance of developing relations between the private sector, law enforcement and NGOs to allow for a holistic approach to this issue, developing effective staff training so that employees have the required and necessary skills and ensuring that internal models and controls are constantly reviewed to ensure they are up to date and fit for purpose.

We would encourage the entire financial industry to undertake a review of their current procedures and processes. Whilst this document is intended as a basic and in many ways simplistic guide to preventing the selling and purchasing of child abuse images, organisations are reminded that their existing guidelines should be reviewed on a regular basis to allow for changes in technology and payment methods to be taken into account at an early stage.



# Appendices

## Appendix A Glossary of terms

**Merchant** – refers to any Person that enters into an agreement with an Acquirer [not always a banking entity] for participation in the acceptance of Cards for purposes of originating payment transactions.

**Acquirer** – A bank that contracts with a Merchant for the acceptance of cards and other payment vehicles.

**Issuer** – A bank that provides cards to consumers to facilitate payment.

**Chargeback** – A transaction that an Issuer returns to an Acquirer as a result of a dispute.

**Merchant Category Code (MCC)** – A code designating the principal trade, profession or line of business in which a Merchant is engaged.

**Proceeds of Crime Act 2002 (POCA)** – The Act that consolidated and extended the existing UK legislation regarding money laundering. The legislation covers all crimes and any dealing in criminal property, with no exceptions and no de minimis value.

**The Money Laundering Regulations 2007** – The Money Laundering Regulations 2007 specify arrangements that firms specified within the Regulations must adopt to prevent activities relating to money laundering and terrorist financing.

**Joint Money Laundering Steering Group Guidance Notes** – The Guidance is prepared by a number of professional associations and trade bodies and sets out the obligations of the Regulations and POCA in a standard approach. The FSA also confirms that regard will be considered to whether an organisation has followed the provisions of the Guidance when potential breaches of obligations are highlighted.

**Electronic money** – Electronic money is a retail payment product that is used predominantly for making small value payments (should adapt to the legal definition). As an electronic means of payment, it is susceptible to the same risks of money laundering and terrorist financing as other retail payment products. In the absence of controls over the use of the product, there is a significant risk of money laundering taking place. The implementation of purse limits, usage controls, and systems to detect suspicious activity contributes to mitigating these risks.

**Prepaid card-based products** – These are products that employ a card or other electronic vouchers for authentication, or to store the electronic money or a record of it on the card or voucher. Prepaid cards can be loaded (i.e. credited) with funds by cash, bank transfer or by transfer of funds from other card offerings such as credit or debit cards. They do not offer a credit facility.

**Open/closed loop systems** – A closed scheme or system contains single Merchant or limited to one retail organisation for the redemption of funds. An open scheme or system allows the participation of multiple places and Merchants for the redemption of the funds.

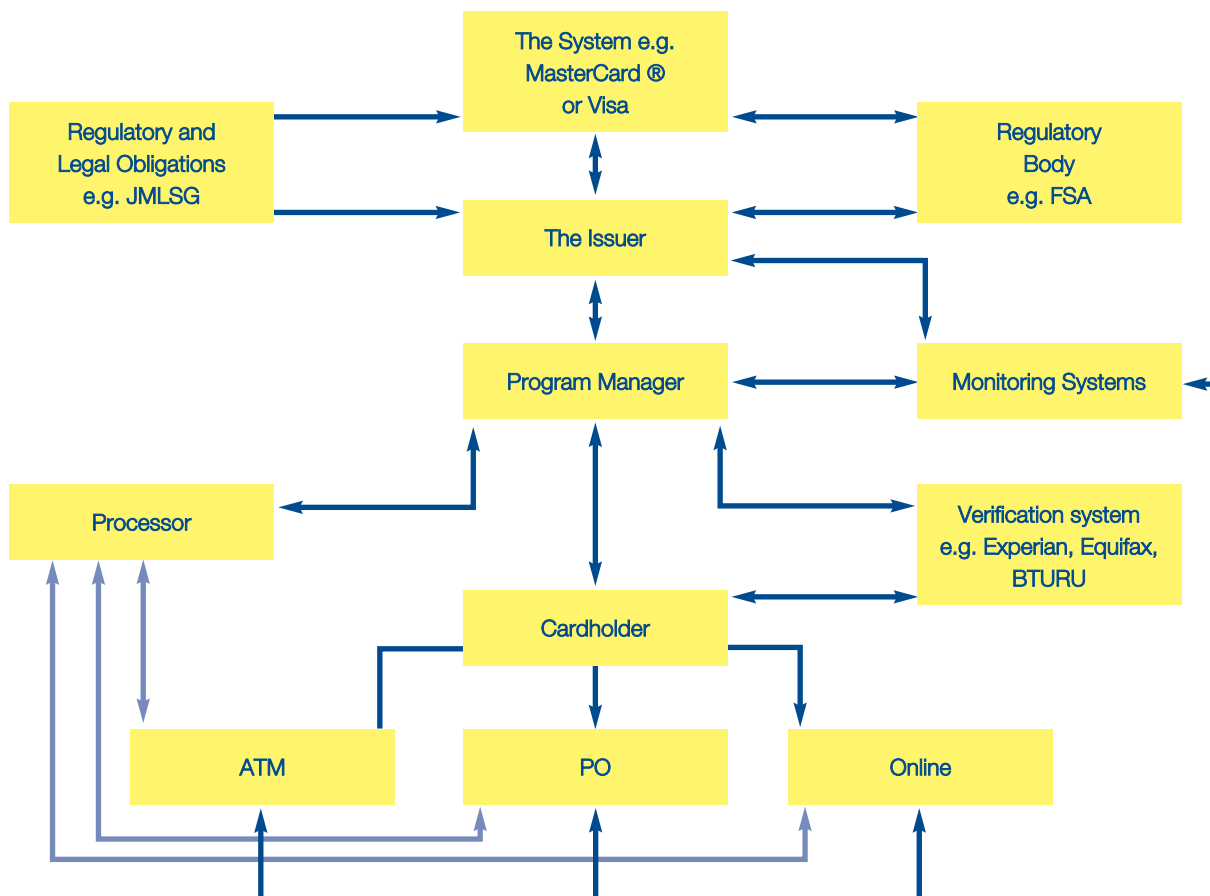
**Customer due diligence (CDD)** – Identification standards that are applied to applicants for the financial product which prove (verify) personal identity and confirmation of address. This may be achieved by provision of documents or by conducting electronic checks using approved systems.

**Simplified due diligence (SDD)** – Verification of identity is not a regulatory requirement providing that either the card cannot be reloaded and the maximum amount stored on the card is limited to a maximum amount of €150, or if the card can be recharged, a limit of £2,200 is imposed on the total amount transacted and cash redemption does not exceed £800 in a twelve month period.

**Financial exclusion** – The FSA Rules adopt a view that where people are unable, and cannot be reasonably expected, to provide standard evidence of identification they are not unreasonably denied access to financial services. Examples can include young adults; migrant workers; persons who are in temporary accommodation such as students. In cases where standard identification evidence is not available, applicants for prepaid cards may be accepted for a SDD product, subject to the risk-based approach of the organisation.

## Appendix B Prepaid card system infrastructure

The chart explains the interconnection between the different parties.



**The Issuer** is granted a licence from the Card Scheme to issue cards and, linked to the Processor, moves money to settle purchases and ATM withdrawals made by the cardholder. The Issuer is also the Bankers Identification Number (BIN) sponsor, is regulated and holds an E-Money Licence. As Program Managers are providing cards under the Issuer’s licence, the Issuer is ultimately responsible for the regulatory conduct of the product.

**The Program Manager** is contracted to the Issuer and acts as a form of intermediary to market and supply cards to cardholders. The Program Manager ensures that suitable due diligence is conducted against cardholders before provision of the facility and must implement the requirements of the Issuer.

**The Verification System** is an electronic system to confirm personal information of the applicant. This will include a minimum of name, address and date of birth.



