EUROPEAN FINANCIAL COALITION

against Commercial Sexual Exploitation of Children Online

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

This project has been funded with the support of the European Commission. This publication reflects the views only of the author. The European Commission cannot be held responsible for any use which may be made of the information contained therein.

Contents

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

This publication reflects the views only of the European Financial Coalition, and not of any member of the Payments Industry Working Group or the European Commission, none of whom can be held responsible for any use which may be made of the information contained therein.

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 to fight the online distribution of child abuse material for financial gain in the European Union. The initial 16–month project was funded by the European Commission and led by the UK's Child Exploitation and Online Protection (CEOP) Centre. The stakeholders involved included 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 "first phase" of the EFC was concluded in 2010, showing a significant decrease in the number of traditional pay-per-view websites on which child abuse material may be found. Despite its positive outcomes, new challenges were identified, including the migration of illegal material from traditional commercial websites to other new or existing internet environments and platforms.

In response to these new criminal trends, representatives of law enforcement, civil society and private industry jointly launched, with the financial support of the European Commission, the "second phase" of the EFC in November 2012. The current 36-month project is characterised by an enhanced European dimension with Europol-EC3 chairing the Steering group and a stronger public-private partnership with Missing Children Europe coordinating the EFC's secretariat. The "new" EFC is led by a Steering Committee composed of representatives of Europol's European Cybercrime Centre (Europol-EC3), Missing Children Europe (MCE), INHOPE, EUROJUST, Visa Europe, MasterCard, PayPal, Microsoft, Google, CEPOL and the International Center for Missing and Exploited Children (ICMEC).

The EFC's activities are divided into 5 work-streams ("Work Packages" or "WP"), led by one or more Steering Group Members. Each Work Package is responsible for one of the five strategic

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

objectives indicated below:

1. WP1 Operations: support international law enforcement investigations; wherever possible through cooperation with private stakeholders
2. WP2 Analysis and Reporting: assess and study the commercial child sexual exploitation on the Internet through all kinds of Internet environments: hosting services, newsgroups, etc.
3. WP3 Private Sector Support and Cooperation: protect legitimate private business interests from possible misuse of their services perpetrated by criminals with the aim of distributing child sexual abuse content through different information and communication technologies
4. WP4 Training: empower law enforcement authorities and private companies in counteracting the problem through the delivery of training and sharing of resources
5. WP5 Awareness and External Relations: inform decision makers and raise awareness among the public about the EFC's activities

The WPs are composed of both public and private partners who meet regularly to implement their respective deliverables in accordance with the overall timetable of the project.

The EFC works closely with other Financial Coalitions around the world, in particular with the US Financial Coalition against Child Pornography, the Asia-Pacific Financial Coalition against Child Pornography and the Swedish Financial Coalition against Child Pornography. Additionally, the EFC meets on a regular basis with other European networks and initiatives engaged in online protection of children.

The EFC's long term ambition is to become Europe's permanent operational platform and resource centre for public and private entities engaged in the fight against the commercial sexual exploitation of children online.

**This document has been published in the framework of the EFC project 2009-2010 by the Payments Industry Working Group (PIWG) chaired by Visa Europe and consisted 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.*

Under the current EFC structure, the WP3 Private Sector Support and Cooperation is led by PayPal and includes representatives from Elavon, G2 Web Services, GSMA Mobile Alliance against Child Sexual Abuse Content, Mastercard, Visa Europe and Western Union. Following

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

a thorough review of the best practises collected in the present document, WP3 lead and members deem this Best Practice Guidance for the Financial Industry ("BPG") an up-to-date product indicating practices which are still fit for guidance and commonly used in the financial sector. A contribution from the current members covering recently identified trends and possible threats have been included in this updated version of the guide.

This BPG aims to improve the prevention and detection of financial 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

Should you be interested in receiving more information on the EFC's activities, or contributing to the work of WP3 Private Sector Support and Cooperation, please visit the EFC website www.europeanfinancialcoalition.eu and register for our newsletter or contact the EFC secretariat by e-mail at secretariat@europeanfinancialcoalition.eu.

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 imagery. 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 EFC's financial industry members and are not intended to be comprehensive.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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 this BPG contains 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 recommendations 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 imagery 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 members of the Payment Industry Working Group of the EFC in 2010 and has been updated by the EFC Working Group 3 – Private Sector Support and Cooperation, sub-group payment industry in 2014.

The GSMA Mobile Alliance Against Child Sexual Abuse Content has produced guidelines for mobile payments providers to prevent the misuse of their services to monetise online child sexual abuse content. The GSMA Mobile Alliance guidelines complement the recommendations contained in this document and include considerations that are specific to the various players from across the mobile payments value chain. 'Preventing mobile payments services from being misused to monetise child sexual abuse content' can be found on the EFC website, under publications (http://www.europeanfinancialcoalition.eu/document.php).

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

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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
- 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 its 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.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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.

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 clearly and be easy to find on the merchant's website:

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

- Customer service number (toll free preferably), presented consistently wherever a service number appears throughout the site
- E-mail address to contact the company, presented consistently wherever a service contact address appears throughout the site
- Statement on security controls
- Delivery methods and timing
- Age verification methodology (for age restricted goods and services)
- Return and/or refund policy should provide a reasonable time-frame for returns (e.g. no less than 30 days).Privacy statements (permissible uses of customer information)
- Depending on the type of merchant, terms of service and/or acceptable use policy
- The website should prompt users to check a box indicating that they understand the terms of service/AUP before purchasing the product.

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

- Nature of goods/services
- Design of the home-page and location of billing page/s
- Transaction patterns
- Merchant location (physical and legal)
- Business model (one-off transaction, or regular billing.
  - o If regular billing, the conditions and cancellation policy should be very clear to the customer)
  - o If the merchant provides a membership service (even if billing is not recurring), it should provide a clear cancellation policy
- Average (or projected) turnover
- Average (or projected) refund volume
- Average (or projected) chargeback and fraud rates

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

- Average (or projected) refund rates and refund policy
- Disclosure of all payment mechanisms offered
- 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. The Merchant name and website URL should be checked against available Industry Negative Watch Lists; the reputation of the merchant can/should also be checked among consumer complaint websites.

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.

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. Also ensure a correct business classification code (e.g. MCC) is assigned.

It is also recommended that Acquirers review every new Merchant against a robust malcontent database[1] 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 a systematic review of the WhoIs merchant name, Merchant URL, Merchant or principal contact information and principal history for prior violations, as such prior violations can be a predictor of future illegal or high risk activity. Examples of important Merchant history data includes checking for previous IP address/subnets violations, knowing where the address is registered, association with high risk MCC codes and confirming if the domain is listed as private, among other factors that can indicate higher risk.

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

[1] 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 are not limited to);

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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.

Note

Recent boarding trends include a rise in online applications and accelerated and cost-effective pre-boarding diligence, especially for very small merchants. Organizations adopting more automated boarding approaches need to ensure they have a comprehensive approach to manage risk and ongoing monitoring.

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.
- Employ a third-party company to search the internet for Merchants offering

- URL
- doing business as name
- trading name
- principal (business owner/s)
- WhoIs data, including confirming that the WhoIs data is the Merchant's legitimate contact information and not fabricated or privacy-protected
- IP address

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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 Payment Facilitators (PF'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 PF 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. Of course, this can change over time as brick and mortar merchants add e-commerce capabilities. 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

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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 organisations to demonstrate that they understand not only the business model and activities of the aggregator/referral merchant, but also all of the entities that these organisations bring into the payment chain.

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)
- Payment Facilitators (PF)
- E-wallets, or other quasi-cash providers
- Shopping Carts or other payment aggregators
- Membership 'clubs'

Step 4: Persistent Analysis

The main underlying principle of the EFC Best Practice guidance is Know Your Customer

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

(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, PFPFs , 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.

Data Risk: Identify sites that could not be reviewed because they are Inactive, Parked, or Redirected to another site. These sites present risk since the merchants may be conducting business from a site unknown to the Acquirer and not under monitoring. The Acquirer should look for a card not present activity at the unreviewed site and determine if it emanated from a different active website. It may be necessary to monitor multiple sites and/or update the registered URLs for the merchant.

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.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

The Acquirer should have the violating content removed urgently and consider terminating the merchant.

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.

Note

The growing challenge of transaction laundering.

Transaction laundering, also known as unauthorized aggregation, is an extremely difficult problem that occurs when legitimate merchant accounts are used to process unknown transactions (illegal or otherwise) for another line of business. Using an approved merchant's payment credentials, the unknown merchant processes payments for products and services not under monitoring, which can include child abuse material. The best offense against transaction laundering is a good defense, which includes training sales staff to look for signals of malfeasance and strong due diligence before the merchant is boarded. After boarding, specialized and multi-faceted monitoring solutions are required to detect laundering "pairs" in a current portfolio. Other best practice includes training customer service to review dispute spikes, monitoring transaction anomalies and general investigation of suspicious activity. Affiliate programs can also attract launderers, so merchants should be advised to avoid high affiliate payouts.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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 is 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.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

4. E- money providers

The guidelines in this section relate to e-money providers. They 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.

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.

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 images.

All relevant staff should be made aware of the risk that their payment products could be used

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

for illegal purposes including the distribution of child abuse material. 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 material (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.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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, on-line or by postal application. The cards can be used for cash withdrawal at ATM's, purchases on-line, 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.

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

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

card issuers and Program Managers. JMLSG Guidance Notes[2] 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 authorised 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
- Establish if the system can send warnings/alerts to Issuers and/or Program Managers

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

[2] 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.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

- Assess the type of schemes that the PM intends to provide
- Assess the mediums that the PM intends to use and analyse associated risks
- 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 the 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
- Assess to 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

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

- Assess if the programme can be provided under SDD or if full verification is required
- Assess the distribution 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 programme proposal
- Record approval by senior managers of the scheme to enable it to go 'live'

5.3 Types of prepaid cards & mitigation

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 anonymous or SDD version of a prepaid card. Consequently, for the purpose of this best practice guidance, a SDD and anonymous products have been focused upon.

Gift Cards (open loop)

Risks

- Can be used in retailers face to face or for online internet purchases
- Type of merchant may not be restricted
- Cardholder details may not be recorded
- Cards could be passed person-to-person and the end user not known
- Cards are activated at point of sale or are ready activated
- Can be purchased with cash (another anonymous method)

Mitigation and Best Practice

- Maximum prepaid account restrictions
- Unable to re-load (add additional) funds
- Restrict merchant or / and goods availability
- Require purchaser details to be recorded
- Require cardholder details to be recorded

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

Instant Issue Cards (anonymous)

Risks

- Can be purchased from a variety of outlets and merchants
- Purchaser details may not be recorded
- Cards are activated at point of sale or online at the issuers or programme manager's website
- Can be used in merchants face-to-face or for merchant internet purchases
- Cards can be passed from person to person and the end-user cannot be identified
- No postal communication with customer
- Cash loading permitted but within restrictive levels

Mitigation and Best Practice

- Maximum prepaid account value restrictions in accordance with SDD parameters or lower
- Restrict merchant or / and goods availability
- Require purchaser details to be recorded
- Send 'Welcome Pack' to provided address

Simplified Due Diligence Cards (personalised and posted)

Risks

- Provided address may not be the true residential address of the applicant (address is captured for SDD but not verified as limited load and maximum annualized balance of €2,500)
- Can be reloaded by cash or electronic transfer
- Can be used in-store and internet

Mitigation and Best Practice

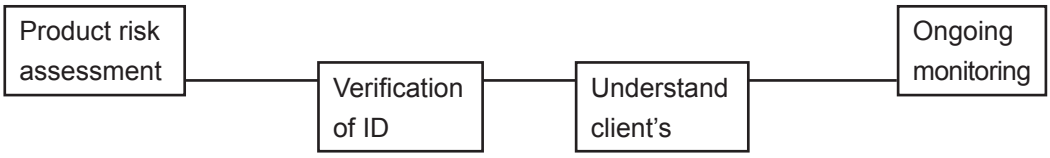
- Maximum purse value restrictions in accordance with SDD parameters

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

- Personal data of the applicant is recorded verified and validated
- Postal communication to address provided creates an audit trail
- Require cardholder to register for activation of card

Cards issued after full verification of customers: Cards provided to applicants who have satisfied the KYC (verification of ID and address) can greatly reduce and mitigate 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 the issuer or programme managers' processes.

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.



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 on-line transactions of small to medium values to suspect merchant codes
- Low value load followed by on-line purchase from suspect merchant code

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

- Transactions involving services the cardholder has not previously used and particularly if the service seems inappropriate for that cardholder
- 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
- 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/on-line/point of sale), merchant type and balance of account.

The recording of such data, even for anonymous and 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, they need to 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.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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-avert culture is adhered to by all stakeholders, prepaid cards are a valuable commodity for the provision of a compliant financial service.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

6. File sharing and cyberlocket merchants

Based upon their business model, file sharing and cyberlocker merchants face significant challenges with regard to child sexual exploitation content. Consequently acquirers should adopt a robust policy focusing on pre-vetting/approval and continuous monitoring of new and existing merchants within their portfolio. The EFC strongly recommends the best practices set forth in Appendix 3 should be followed for each merchant operating within the file sharing and cyberlocker vertical.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

7. Conclusion

The European Financial Coalition believes that the best practice guidelines detailed above should help all Issuers, programme managers and 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 is 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.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

Appendix 1 - 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 voucher 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.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

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.

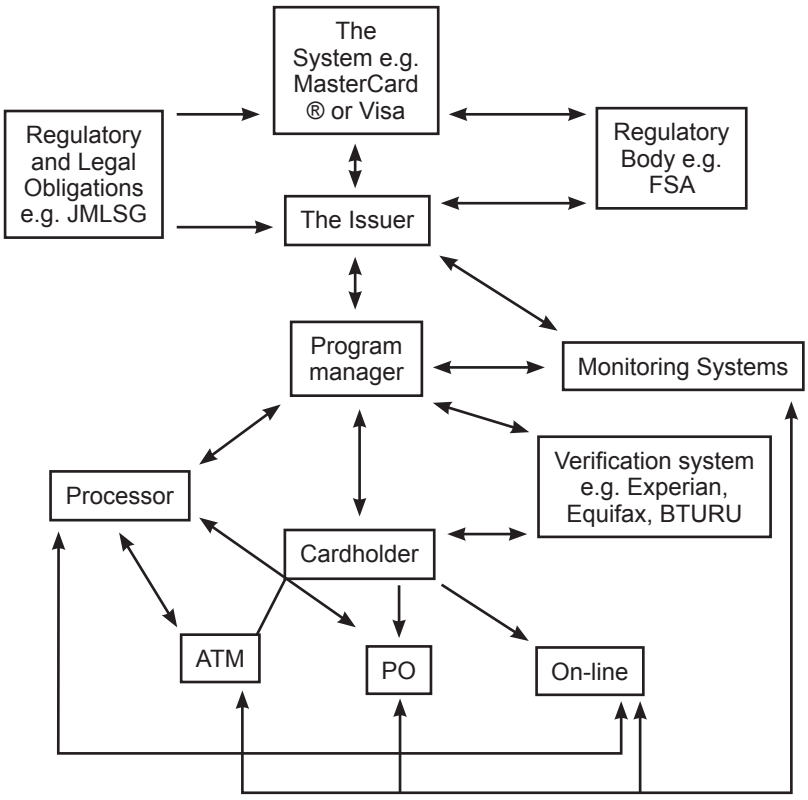
Simplified due diligence (SDD) – Verification of identity is not a regulatory requirement providing that either the card cannot be reloaded and the maximum amount stored on the card is limited to a maximum amount of €150, or if the card can be recharged, a limit of £2,200 is imposed on the total amount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

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

Appendix 2 - 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.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

Appendix 3 – File sharing and cyberlocker merchants

1. General Provision

A. Any acquiring entity (which in this document includes both the acquiring bank and its value chain partners working with the file sharing and cyberlocker merchants) should require merchants providing file sharing services including cyberlockers to receive pre-approval from and undergo ongoing monitoring by its risk team. Such pre-approval and monitoring should be conducted in accordance with a File Sharing Best Practices and Requirements Policy created by the acquiring entity with reference to the best practices set forth in this document.

B. Merchants providing file sharing services should be considered high risk and receive heightened scrutiny at boarding and on an ongoing basis.

C. Merchants providing file sharing services should at all times have the burden of proving compliance with an acquiring entity's File Sharing Best Practices and Requirements Policy.

D. Merchants providing file sharing services should maintain records to prove compliance with an acquiring entity's File Sharing Best Practices and Requirements Policy at all times.

E. Merchants providing file sharing services should fully cooperate with any inquiry concerning the merchant's compliance with an acquiring entity's File Sharing Best Practices and Requirements Policy.

F. Failure to maintain appropriate records or fully cooperate with any inquiry pursuant to an acquiring entity's File Sharing Best Practices and Requirements Policy should result in the merchant account restriction or termination.

2. Merchant review

An acquiring entity should review all merchants providing file sharing services including cyber-lockers for compliance with the following best practices.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

A. The site should have a legitimate business model

1) Archival File Storage sites emphasize the storage and archiving of files for remote access consistent with a legitimate purpose.

I. Storage of specific file types like video and music is not emphasized or promoted.

II. Stored files generally do not have expiration or purge dates.

III. Pricing is based on the size of the storage account as opposed to file size.

IV. Distribution or "sharing" is not an emphasis of archival file storage lockers and is generally limited.

V. Facilities for distributing stored files are not provided to users including "forum codes" or "html codes" to facilitate distribution of stored content on third party websites.

VI. Uploaders are not compensated when a file is distributed or stored.

VII. Links to archived files are generally not found on third-party websites.

2) File Transfer sites emphasize the transfer not storage of large files consistent with a legitimate purpose.

I. Transfer of specific file types like video and music is not emphasized or promoted.

II. File size may be highlighted, but with regard to transfer rather than storage.

III. An email address is generally required to transfer and receive the file.

IV. Email distribution is generally limited to a small number of addresses.

V. Links to stored files generally expire or purge after a short time period or number of downloads.

VI. Files are generally tracked for send and receipt confirmation.

VII. Revenue is not earned when a file is transferred.

VIII. Facilities for distributing stored files are not provided to users including "forum codes" or "html codes" to facilitate distribution of stored content on third party websites.

IX. Links to files are generally not found on third-party websites.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

3) File sharing sites emphasize the distribution of files via download or “streaming” video playback.

I. Storage and distribution of video and music files is often emphasized and promoted.

II. Files are generally stored for long periods of time provided they are regularly accessed.

III. File size is an emphasis of the service including the capacity to store and distribute large files.

IV. Pricing is based on monthly access and file size.

V. “Streaming” video playback may feature display advertisements.

VI. File owners are generally anonymous and do not know the true identity of the recipients.

B. File sharing sites may be legitimate; however, the following characteristics are commonly associated with illegitimate business models.

I. “Rewards,” cash payments or other incentives are paid to uploaders based on the number of times their files are downloaded or streamed.

II. The “reward” program emphasizes distribution of files in excess of 200 MB consistent with long form content like movies and TV shows.

III. Links to prohibited content are indexed or distributed on third party websites.

IV. High volumes of links to prohibited content are identified either by review of linking or indexing websites, search engine queries, reports by rights holders or other methods of identification.

V. Distribution of large files is emphasized consistent with the distribution of prohibited, long form copyrighted content whether in compressed (.rar, .zip) or uncompressed file formats (.avi, .wmv, .mpg, .mkv, .mp4, .divx, .xvid, .flv, .mov, .mpeg).

VI. Free access to stored files may be limited by increased wait times, bandwidth throttling, download limits, captchas, online advertising or other techniques to encourage the purchase of “premium” memberships.

VII. Files are deleted unless the uploader purchases a “premium” membership or a file is regularly accessed.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

VIII. The site provides a “link checker” which allows uploaders to check if a link has been disabled to facilitate re-upload of content removed by rights holders.

IX. The site provides uploaders with “forum codes” and “URL codes” to facilitate incorporation of the links on third party indexing or “linking” websites.

X. Access to the site is sold through third-party resellers.

3. High-risk characteristics

Should any of the following characteristics be present when dealing with a file sharing service, serious consideration should be given to the prospect of terminating the business relationship.

A. Incentives to Distribute Prohibited Content.

I. A merchant should not provide or offer to provide “rewards,” cash payments or any other incentives to users based on the number of times files containing prohibited content are downloaded, streamed or otherwise accessed.

B. Payments to Users Distributing Prohibited Content.

I. A merchant should not transfer any funds to users of file sharing websites in exchange for uploading, distributing, publicly performing, promoting, making available or advertising prohibited content or offering or attempting to engage in any of these activities relating to prohibited content pursuant to an “affiliate,” “reward” or any other similar program. The burden should be on the merchant to demonstrate that any payment made to the user of a file sharing website does not violate this principle.

C. Affiliate programs.

I. The merchant should not pay or offer to pay for referral web traffic from third-party websites purporting to offer links to prohibited content on a file sharing website. The merchant should not pay or offer to pay a commission to affiliates for new or renewal file sharing subscriptions if the affiliate is operating a third-party website that purports to offer links to prohibited content. The burden should be on the merchant to demonstrate that any payment made pursuant to an affiliate referral program does not violate these principles.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

4. Merchant best practices

Merchants offering file sharing services should implement controls to ensure that prohibited content is not stored or distributed using their service and should comply with all applicable laws based on the jurisdictions in which any user is based. An acquiring entity should evaluate a merchant's policies and procedures as well as responses to reports of prohibited content and reserve the right to close, suspend or otherwise limit access to merchant's account(s) for failure to comply with any best practice listed below.

I. Content Monitoring:

The merchant should have a formal program (including both policy and procedural components) for monitoring all files stored on their website to ensure files do not contain prohibited content. This content monitoring program should be effective in preventing the storage and distribution of prohibited content before files are made available for public access. The merchant should have the burden of demonstrating to the acquiring entity that its program is effective in preventing the storage and distribution of prohibited content at all times.

Effective content monitoring may be achieved through a combination of automated methods and manual review. (A program of manual review applied to all uploaded files is a conceivable alternative, but unlikely to be practicable at scale). Automated methods should be designed to address the technical attributes of file sharing services and to reliably identify suspect content for automated takedown or manual review. The following methods, or others having equivalent efficacy, should be used:

a. Unknown Universe Crawling:

i. The merchant should implement a third party service to crawl the internet generally and identify websites that advertise or otherwise connect to files accessible via the merchant's service that contain prohibited content.

ii. For the purpose of content recognition, any file that contains prohibited content or any file that is advertised using a description that identifies prohibited content (regardless of whether that file contains such prohibited content) should be considered a violation.

b. Referral URL Analysis:

i. The merchant should implement a third party service to identify all referral URLs from which a user accesses the file sharing website. This service

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

should include the placement of code identifying such referrals on every page of the file sharing website. If a file sharing website is found to have a page that has not deployed the third party code that violation could result in immediate restriction or termination of the merchant account.

ii. Once the list of referral URLs has been identified, the third party service should be required to crawl each of those URLs to identify any advertised prohibited content.

c. Velocity Monitoring:

i. The merchant should implement a third party service to implement a velocity monitoring program that serves to identify the most frequently requested files and evaluate them for prohibited content.

II. Takedown Policy:

a. The merchant should enforce a written, publicly available notice and takedown policy. The merchant should delete files identified in a valid notice no later than 8 hours after receiving a valid notice. Any notice and take down procedure, whether manual or automated, should result in the deletion of the source file and all identical files from the site's database and should not be limited only to deactivation of the reported link or URL. Once a file is deleted pursuant to a valid notice, the merchant should also prevent subsequent re-uploads of the same file.

III. Repeat Infringer Policy:

a. The merchant should enforce a written and publicly available repeat infringer policy that identifies and terminates users who attempt to upload prohibited content on more than one occasion. The merchant should have the burden of demonstrating to the acquiring entity at any time that the site is enforcing its repeat infringer policy through documentation or other proof as required by the acquiring entity.

IV. Reporting:

a. No less than monthly, the file sharing website should forward to the acquiring entity a report that identifies and summarizes all efforts taken in support of the acquiring entity's File Sharing Best Practices and Requirements Policy. That report should include, but not be limited to:

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

- Prohibited Content Identifications: The number of files identified for prohibited content, including categories for each type of content.
- Gross File Request / Prohibited Content Ratios: Identification of the gross number of file requests and identified prohibited content requests.
- Velocity File Request Analysis: Identification and content review resolution for all files that receive more than 50 requests per day.
- Cybertipline Notifications: A volumetric summary of Cybertipline notifications.

V. Child Sexual Exploitation:

a. The merchant should immediately report files it detects that appear to involve child sexual exploitation to the National Center for Missing & Exploited Children's ("NCMEC") "CyberTipline", the European Financial Coalition against Commercial Sexual Exploitation of Children Online or similar national organization.

VI. Access to System:

a. The merchant should provide the acquiring entity or its designated representatives with access to its system to allow review of the content available through its service.

VII. Point of Contact:

a. The merchant should provide the full name, address, email address and phone number for a point of contact to report violations of this policy. Any notice to this point of contact should be deemed notice to the merchant.

VIII. Law Enforcement Cooperation:

a. The merchant should cooperate with all law enforcement requests and any court order including subpoenas, search warrants, discovery orders and any other valid court order. The merchant should provide its acquiring entity with its written policy concerning response to contact from law enforcement agencies regarding prohibited content stored or distributed through its service.

IX. Card Association Registration:

a. The merchant should cooperate with the acquiring entity to facilitate satisfaction

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs

of all applicable card association registration requirements, including providing required information, paying applicable fees and making any requested demo strations of legal compliance.

5. Potential detection practices

Leaders in the fight against child exploitation material employ a variety of methods to proactively detect illicit content on their systems. Some organizations use **"keyword"** lists in multiple languages and build them into detection tools or systems to proactively block, detect or flag for review potential child sexual exploitation content. For maximum effectiveness, keywords and modelling techniques should be updated at least weekly or, if a company has the resources and technology for real-time scanning, that option should be used. Companies also employ tools that crawl and/or spider systems internally and externally on the web looking for policy violations. One tool to consider is **PhotoDNA**, an image-matching technology developed by Microsoft Research in collaboration with Dartmouth College. It creates a unique signature for a digital image, something like a fingerprint, which can be compared with the signatures of other images to find copies of that image. NCMEC and online service providers such as Microsoft and Facebook currently use PhotoDNA to block known PhotoDNA images upon upload and help detect, report and ultimately eliminate some of the worst known images of child pornography online, helping identify thousands of these images that would previously have gone undetected. Another way to crawl internal systems is to review connections between known child abuse material accounts. The accounts of users who are connected to known abuse through downloads, shared access or uploads can be flagged for manual review. Companies can also use INTERPOL's "Worst of" Child Abuse URL list to proactively block links and uploads. The list is maintained and updated weekly by INTERPOL and sent to all interested parties free of charge.

With the financial support of the Prevention of and Fight against
Crime Programme European Commission –Directorate-General Home Affairs