
# Mobile Alliance Against Child Sexual Abuse Content

# Preventing mobile payment services from being misused to monetise child sexual abuse content

March 2014

# The Mobile Alliance Against Child Sexual Abuse Content

The GSMA's Mobile Alliance Against Child Sexual Abuse Content (the Mobile Alliance) was founded in 2008 by an international group of mobile operators committed to working collectively on obstructing the use of the mobile environment by individuals or organisations wishing to consume or profit from child sexual abuse content.

The Mobile Alliance's aim is to help stem, and ultimately reverse, the growth of online child sexual abuse content. Through a combination of technical measures, co-operation and information sharing, the Mobile Alliance seeks to create significant barriers to the misuse of mobile networks and services for hosting, accessing, or profiting from child sexual abuse content.

## BACKGROUND AND PURPOSE OF THIS DOCUMENT

In 2013, the Mobile Alliance updated its 2007 research assessing the risk of mobile payments services being misused to monetise child sexual abuse content (CSAC).

The research confirms that it is still rare for mobile payment mechanisms to be offered as an option on commercial CSAC sites. It also highlights that even where premium SMS is advertised as a payment option on a website, it is generally limited to specific countries, is not working cross-border, and is not necessarily a real 'functioning' option in spite of it being offered. The research and findings are outlined in Part 1 of this document.

In order to ensure that mobile networks and services remain hostile to those wishing to profit from the sexual exploitation of children, and in anticipation of the continued evolution of the mobile payments market, members of the Mobile Alliance have worked together to create good practice guidelines on processes for combating misuse. These guidelines can be found in Part 2 of this document.

In addition, the Mobile Alliance, through its relationships with the Financial Coalition Against Child Pornography (FCACP) and the European Financial Coalition (EFC), the Internet Watch Foundation (IWF) and INHOPE, as well as international law enforcement agencies, continues to monitor payments trends closely and be prepared to respond as needed.

## MOBILE PAYMENTS SERVICES

The term 'mobile payments' can be applied to any payment option which enables a payment to be carried out via mobile devices. In some cases, the mobile operators' own billing systems play a core role in the payments process, and in others, the role of the mobile operator can be as simple as securely routing messages and operating the mobile and / or internet network. For example:

- With premium SMS or 'charge to bill' payments, mobile users buy digital content or services by charging it to their monthly mobile phone bills or debiting it from their pre-pay balance. Having collected the fee from the customer, the mobile operator passes on the payment, minus the agreed revenue share, to the content or service provider.

- With 'mobile wallet' type services (including mobile contactless / Near Field Communication card payments, or mobile remote card payments), the customer's payment service provider 'owns' the transaction between customer and merchant. The mobile operator is responsible for securely routing messages and operating the mobile and/ or internet network, and, in some cases, may also provide the secure domain on the SIM for the consumer's payment application.

This document focuses on the types of mobile payments which use mobile operator billing systems - rather than mobile payments which are enabled by other payment service providers but are available via mobile - and refers primarily to premium SMS. However, the vetting and monitoring processes outlined in Part 2 of this document would also apply to 'charge to bill' processes, or any mobile payment where the mobile operators and their aggregator partners 'own' the transaction.

1.

# Risk assessment: Misuse of mobile payments to monetise commercial child sexual abuse content

1.1

## OVERVIEW OF CURRENT STATUS OF MISUSE OF MOBILE PAYMENTS FOR CSAC

### 1.1.1 DIGITAL COMMERCIAL CHILD SEXUAL ABUSE CONTENT – BACKGROUND

In 2012, INHOPE, the international umbrella organisation for national hotlines for reporting illegal content online, reported that 18 per cent of websites confirmed to be hosting CSAC were commercial in nature. The UK's hotline, the Internet Watch Foundation (IWF), reported that 27 per cent (2,587 in total) of the online CSAC URLs processed by IWF analysts in 2012 were assessed as being commercial in nature - although as the same websites often re-appear multiple times on different URLs there are fewer commercial CSAC entities than the number of URLs suggests.

It should be noted that the INHOPE and IWF figures refer specifically to CSAC websites and do not include other platforms such as peer-to-peer (P2P), through which a growing proportion of CSAC is shared, typically on a non-commercial basis. In the recent European Financial Coalition report, *Commercial Sexual Exploitation of Children: A Strategic Assessment*, the European Cybercrime Centre (EC3) division of Europol observed that the vast majority of [child abuse material] is still distributed non-commercially on the open net, using P2P technologies." Citing interviews in 2012 with informed sources from 10 members of the European Union's COSPOL Internet Related Child Abusive Material Project, the report estimates that a figure between 7.5 and 10.1 per cent is probably more representative of the amount of CSAC being shared commercially as a proportion of the whole.

However, CSAC continues to be commercially distributed, and the EFC report, as well as observations shared with the Mobile Alliance by the Financial Coalition Against Child Pornography (FCACP) and US Immigration and Customs Enforcement (ICE) have all noted the rise of new commercial 'formats', for example, Video On Demand or live 'shows'. The EFC report also notes that "...law enforcement has observed that an ever increasing demand has made new material to be a currency in itself. The value is in the novelty of the image, as a result of which images and videos have become bargaining chips."

Although traditional payment mechanisms are still misused to pay for commercial CSAC, EFC reports that "proactive approaches by payment processors, including the engagement of third parties to conduct monitoring and test purchasing exercises, appear to have been effective in reducing the number of sites able to take payments". A range of non-traditional payments are now being implicated, and the IWF, having observed a growing number of non-traditional payment options being offered on commercial CSAC sites over the preceding two to three years, began formally logging this information in 2012.

### 1.1.2 CURRENT LEVELS OF MISUSE OF MOBILE PAYMENTS FOR COMMERCIAL CHILD SEXUAL ABUSE CONTENT

Both the US and the UK hotlines – The National Center for Missing and Exploited Children (NCMEC) CyberTipline and the IWF – collate data on premium SMS being offered as a payment method on commercial CSAC sites.

NCMEC reports that between January 2012 and October 2013, of the 835 reports they received relating to commercial sites containing "Apparent Child Pornography" only nine (1%) offered SMS as a payment option. Although test transactions were not carried out on all of the reported sites, the one attempt that was made by the team from U.S. Immigration and Customs Enforcement, which carries out some of the test transactions on behalf of the FCACP, was unsuccessful.

The IWF data from 2012 also confirms that potential misuse of mobile payments for CSAC is still rare:

- Of the 2,587 reports of commercial CSAC websites handled, 78 (i.e. 9%) offered Premium SMS. In all but one case, these were offered in conjunction with other payment mechanisms.

- Details on the countries affected are not available, but the IWF has confirmed that this is generally only seen in the Eastern European region with different SMS short codes being shown for each country listed (i.e., this is not working cross-border) and only occasionally is it seen elsewhere.

At present, no test transactions are being performed in this region and it is therefore unclear whether sometimes SMS payment options are not genuinely operational but are part of the 'sales pitch' leading to other options: the IWF states that, according to feedback they have in the past received from law enforcement, it is not uncommon for multiple payment options to be offered upfront to encourage a decision to purchase, but then for users to be told that 'systems are currently down' and re-directed to a different payment option.

The IWF has also noted that 'cell phone balance' has occasionally been listed as a payment option on some sites. Again, there have been no test transactions, and in practical terms this type of payment would, at present, only usually work between customers on the same network in the same country, preventing any significant take up.

The Mobile Alliance continues to liaise closely with informed sources from hotlines and law enforcement, as well as the FCACP and the EFC and their members, in order to be prepared for any new developments impacting mobile services.

**FURTHER READING**

European Financial Coalition against Commercial Sexual Exploitation of Children Online, *Commercial Sexual Exploitation Online: A Strategic Assessment* - prepared by the European Cybercrime Centre (EC3), Europol
**http://www.europeanfinancialcoalition.eu/private10/images/document/5.pdf**

INHOPE Annual Reports **http://www.inhope.org/tns/resources/annual-reports.aspx**

IWF Annual Reports **https://www.iwf.org.uk/accountability/annual-reports**

1.2

# RISK ASSESSMENT OF MOBILE PAYMENTS BECOMING A PREFERRED METHOD OF MONETISING CSAC

## 1.2.1 RESEARCH PROCESS AND FINDINGS

To understand whether mobile payment services are at risk of becoming a preferred payment mechanism for commercial CSAC, the Mobile Alliance examined how mobile payments compare to traditional payment services (e.g. credit / charge / debit cards) and Stored Value Accounts or SVAs (e.g. PayPal) in terms of:

- Due diligence on merchants / content providers prior to launch
- Level of information on end user / purchaser
- Proactive checking of merchants / content providers post-launch
- Industry-level collaboration and information sharing
- Commercial considerations

The assessment did not consider other 'non-industry' online payments options (e.g. digital currencies, or 'money laundering' techniques such as the exchange of calling card numbers) which are not comparable due to lack of regulation or mainstream consumer usage.[1]

### GENERAL CONTROLS

Some controls against misuse of payment services are standard across all payment service providers: Terms and Conditions (T&Cs) uniformly forbid illegal usage of services, and even payment providers who do not proactively monitor or vet merchants can respond reactively to reports of illegality and misuse by third parties.

However, beyond such basic minimums, there is enormous variety in the way in which potential points of control are used by different payment option providers. Although practices also vary from country to country and organisation to organisation, common themes are discussed below.

### DUE DILIGENCE ON MERCHANTS / CONTENT PROVIDERS PRIOR TO LAUNCH

**Traditional payments providers:** Traditional payments providers and the most responsible SVAs have developed thorough processes for vetting merchants prior to acquisition. In addition to gathering information such as trading history, principal's name, address, bank accounts and URLs up front, many also collect full business plans and marketing collateral, contact the service's web hosting company, and visit the merchant's business location. Many banks and schemes rely on third parties to collect this information, and although some of these third parties are less rigorous than others, they do risk substantial fines from the payments networks such as MasterCard and Visa in the case of their merchants' non-compliance with the rules.

**SVAs:** SVA rules and vetting vary by provider. PayPal, for example, invests in proactively screening merchants while other SVAs are more 'relaxed'. Even though SVA provision is subject to anti-money laundering rules, typically there are lower levels of due diligence on merchants relative to the traditional payments providers. Many SVAs are run by small businesses with little brand equity to lose and a focus on short term revenues. They typically enable third party merchants to set up SVAs and be operational within minutes. Inevitably, this opens the way to abuse.

**Mobile payments:** As with traditional payments providers, mobile operators often rely on third parties, aggregators,[2] to vet content partners on their behalf. In many countries, operators and aggregators have similar vetting processes to the traditional payments providers. Operators typically require the principal's name, address and bank account details as a minimum, but some operators also insist upon aggregators collecting specific additional information e.g. multiple screen shots of the content that the merchant offers. Anti-money laundering rules also apply. However, there is huge variation between different countries, as well as between individual operators and aggregators, and whilst all aggregators are subject to the same rules

1. The findings are summarised below. GSMA members wishing to read the risk assessment report in full, should email sam.lynch@gsma.com to request a copy
2. Aggregators provide a platform which sits between mobile operators and content / service providers (i.e. organisations that create / manage and promote content or services) and enables the latter to sell their content / service to consumers who can pay using credit / balance on their pre-paid mobiles or charge to their mobile bills. Examples of international aggregators include Zong and Boku.

from the operators, some aggregators will do the bare minimum and others put compliance at the heart of their business.

**At its best, the mobile payments community is as diligent as traditional payments providers; however, in some cases the mobile community is significantly less diligent. Generally though, the mobile payments community has more checks in place than 'small brand' SVAs, some of which will enable merchants with little more than a valid email address.**

## LEVEL OF INFORMATION ON END USER / PURCHASER

**Traditional payments providers:** Know Your Customer (KYC) rules mean the purchaser's identity is known to traditional payments providers. However, 'pre-paid credit cards' allow the buyer to be anonymous as they can be bought over-the-counter for cash without registration.

**SVAs:** Whilst some SVAs follow standard KYC processes, others can be completely anonymous using real-world cash payments to buy vouchers which can be spent online.

**Mobile payments:** Pre-pay mobile can also be anonymous.

**As it is possible to transact anonymously through all payment options, mobile payments are arguably no more or less vulnerable than other options. However, mobile is the only option which would enable anonymous users to make an 'impulse' purchase using existing credit / balance on their phones without having to first buy credit 'offline' and then set up an account online.**

## PROACTIVE CHECKING OF MERCHANTS / CONTENT PROVIDERS POST-LAUNCH

**Traditional payments providers:** Post-launch, the principle ongoing defence mechanism of traditional payments providers is to monitor and investigate unusual activities such as variations in deposit frequency, transaction volume, average ticket price (ATP) of each sale transaction, and so on. Unusual activities provide an early warning of potential misuse. However, this sector is increasingly taking additional steps to protect their services by proactively checking merchant sites or using central 'web spidering' techniques to monitor sites where their scheme is accepted, referring any suspicious URLs to hotline organisations. Others have 'mystery shoppers' who will investigate sites a few months after they have launched. Further examples of all these types of activities can be found in the FCACP best practice document.[3]

**SVAs:** Although PayPal invests resource in proactively monitoring its merchants, this is atypical of SVAs generally, the vast majority of which rely solely on reports or complaints from 3rd parties to detect misuse; a minority are even alleged knowingly to 'turn a blind eye' to misuse.

**Mobile payments:** Mobile operators sometimes monitor sites themselves (in-house or through external agencies) and apply penalties to aggregators whose merchants are non-compliant, to encourage them to monitor as well. Some operators and aggregators randomly check enabled content providers for anything in breach of T&Cs. Although this is standard in a number of markets it is not yet standard from a global perspective. Some aggregators monitor and investigate unusual activities in the same way as traditional payments providers. Generally though, complaints by third parties and customers are the most likely means of detecting misuse.

**In spite of the excellence demonstrated in post-launch monitoring by a number of operators and aggregators, many others rely solely on reports from third parties to detect misuse. The mobile payments community as a whole is generally behind credit / debit card providers and more responsible SVAs, but is more active than the majority of smaller brand SVAs who take a reactive stance but do no proactive monitoring.**

3. See: Further reading, below.

## INDUSTRY-LEVEL COLLABORATION AND INFORMATION SHARING

**Traditional payments providers:** Many major banks and credit card providers are members of the FCACP through which they are sharing best practices on combating misuse of their services to monetise online CSAC. Through the CyberTipline (US hotline), NCMEC operates a central 'clearinghouse' which accommodates information from the FCACP. A member of the public or a FCACP company which suspects a service is being used for CSAC will alert the CyberTipline. NCMEC staff review the publicly available webpage and confirm the site is commercial in nature and also appears to contain sexually abusive images of children. The CyberTipline information is then made available to US law enforcement who may choose to conduct a test transaction on the webpage with live credit cards donated by FCACP members. Once the transaction occurs, NCMEC notifies the company, in real-time, so they can follow the money. The newly acquired information is then shared by the company through the NCMEC clearinghouse so law enforcement can review and choose to initiate an investigation. If law enforcement declines an investigation, FCACP members will move rapidly to prevent their services from being used by the merchant in question.

**SVAs:** Some SVAs—notably PayPal and Google Checkout—are members of the FCACP and therefore contribute and have access to the clearinghouse. Most are not members however, and do not collaborate with the wider SVA or financial services community in this area.

**Mobile payments:** Some national premium services regulators[4] maintain blacklists of content providers who have breached rules (e.g. false advertising, over-charging) and this includes illegal activities. In some markets there are processes in place, designed primarily for fraud, which enable operators to share information about misuse directly with each other. In many cases, a merchant who has been discovered transgressing rules and had its service taken down, could simply switch aggregators or change its business details and continue to operate. There is no structure in place to share information cross-border.

**In some markets, there are standard national approaches for vetting and monitoring; Mobile Alliance operators and mobile payments aggregators have collaborated to produce good practice recommendations that can be applied internationally (see Part 2 of this document). Current low levels of misuse for commercial CSAC suggest that a structure for sharing mobile payments information on CSAC (such as the CyberTipline clearinghouse used by the FCACP) would not provide benefits beyond those already afforded by national premium service regulators and inter-operator fraud fora at this time.**

## COMMERCIAL CONSIDERATIONS

**Traditional payments providers:** The main commercial advantage of credit / debit card payment mechanisms, with regard to CSAC, is also the main weakness: enabling merchants to sign-up once and then transact with a global cardholder base is as attractive to illegal businesses as it is to legitimate businesses. In addition, banks keep a comparatively small percentage (typically around 2-5%) of merchant revenues, and settle on a weekly or daily basis.

**SVAs:** Some SVAs have allegedly been set up to mask questionable transactions, and as such are attractive to merchants looking to sell illegal content. As initiatives such as the FCACP clearinghouse help to make traditional payment options less vulnerable to misuse, SVAs may become more attractive to illicit merchants seeking an alternative option.

**Mobile payments:** Mobile payment options still represent a relatively unattractive payment solution for merchants seeking to sell CSAC due to factors including:

- Slower payouts: Operators typically pay out after a minimum of 30 days, versus weekly / daily for the banking sector and 'instant' for SVAs. This makes mobile payments services hostile to illicit businesses wishing to make money quickly and then exit.

- Higher service charges (i.e. revenue share) than credit cards and SVAs – this varies, but in many markets content providers can receive less than half the revenue of a PSMS.

- Relatively slower provisioning of new services, typically days compared to minutes with SVAs, although this does vary and in some cases provisioning can happen more quickly.

4. Premium Rate Services (PRS) are typically, but not always, regulated at national level, sometimes through an organisation with a specific remit for PRS, sometimes by the overall national regulatory authority. Typically, a PRS code of conduct is the main vehicle for regulating PRS, and punitive measures (e.g. warnings, service suspension, fines, being banned from providing PRS) are applied to content providers in breach of PRS regulation.

**For mobile payment service providers who do not yet have thorough vetting and monitoring processes in place, commercial considerations are probably their best defences from being misused for monetising illegal content.**

### 1.2.2 CONCLUSIONS AND IMPLICATIONS

Although mobile payments are being offered on commercial CSAC websites, this is still only in a small minority of cases and the availability of several less hostile payment options makes it unlikely, in the short to medium term, that mobile will become a preferred method of monetising CSAC content.

In spite of the many examples of excellence that exist across the mobile industry with regard to vetting and monitoring content providers, this standard is not yet universal across all players in all countries. Given this variation, it is likely that commercial considerations (e.g. slower payout times and higher revenue shares) are currently, from a global perspective, providing mobile payments services with their greatest defences.

Recognising the positive effect that proactive vetting and monitoring approaches have had for traditional payment providers and FCACP members, the Mobile Alliance against Child Sexual Abuse Content has collated approaches that have proven successful in deterring and detecting illegal or illicit use of mobile payment services. These are outlined in Part 2 of this document.

The Mobile Alliance urges mobile payments players—both operators and aggregators—to take advantage of the recommendations that have been shared within this document and to ensure that their due diligence processes are thorough. Not only will this help to keep the mobile environment hostile to those wishing to profit from the sexual exploitation of children, it will also help to maintain trust in mobile payments systems as they continue to evolve.

2.

# Guidelines for mobile payments providers

The processes described below were not developed specifically to prevent the misuse of mobile payment systems for the sale of CSAC: they are general approaches that serve to combat and detect any illegal or illicit activities, which would of course include those involving monetising CSAC.

2.1

## GENERAL CONTROLS AGAINST ILLEGAL ACTIVITY

Mobile payments providers should review their Terms and Conditions to ensure that they clearly prohibit all illegal content, including CSAC, and outline the steps that will be taken and the likely consequences for any content provider who attempts to misuse their services for this purpose.

Mobile payments providers must ensure that they have the necessary external relationships (e.g. law enforcement and hotlines) and internal processes in place to enable them to move decisively in cases of illegal activity.

## 2.2

# WORKING WITH EXTERNAL STAKEHOLDERS

### HOTLINES:

Operators should work with the hotline organisation in their country to ensure that any complaints or reports of potential CSAC content can be passed to the hotline for assessment, ideally without any operator staff having to look at it themselves.

- *Note: Not all countries have a hotline. INHOPE provides a list of current member hotlines on its website (www.inhope.org), and the INHOPE Foundation and the IWF's back-office solution (IWF International) are currently working to enable hotline facilities in a number of underserved markets. The GSMA can provide operators with current information on any planned activities by either of these organisations in a particular country. Please email sam.lynch@gsma.com to request an update.*

In countries without hotline facilities, operators should pass on reports to national law enforcement, or else, if given legal clearance from government and law enforcement, operators should develop internal processes for content to be assessed internally if a notification or complaint is received:

- Internal processes could build on any existing Notice and Take Down processes and should include a commitment to liaise with law enforcement. Operators should ensure that responsibility lies with a designated team of experts, that exposure to the content is kept to a minimum and that staff involved in this process are suitably cleared, trained and given appropriate support.

### PAN-INDUSTRY COLLABORATION:

It is important that operators and aggregators can coordinate their actions and move rapidly to disable any content provider discovered to be selling illegal content using their services.

- *Note: In many markets, there are channels in place already which would facilitate such information sharing and coordination. In some cases, this could be managed through existing inter-operator processes for sharing information on fraudulent usage of payment services; in others, the premium services regulator would take the necessary steps. For example, in 2012 when the IWF discovered a UK SMS shortcode being used for CSAC they notified PhonepayPlus, the UK premium services regulator, who contacted the aggregator directly and made them aware that their service was being abused. The IWF reports that within days the commercial CSAC website removed the UK shortcode from its website and has since ceased to offer SMS payment.*

In countries where neither of these options would apply, operators should seek to develop a connected group from within the relevant organisations who could alert each other to any discoveries of transgression, enabling swift and coordinated action to be taken.

## 2.3

# RESPONSIBILITY ACROSS THE MOBILE PAYMENTS VALUE CHAIN

In order to keep the mobile payments ecosystem free from misuse, both mobile operators and aggregators have a responsibility to carry out due diligence on the players they enable in other parts of the mobile payments value chain.

Mobile operators typically do not have a direct relationship with content providers for whom they enable billing; rather they work through national and / or multinational aggregators who manage the relationships on their behalf.

Therefore, just as operators will expect aggregators to carry out due diligence processes on the end content and service providers, so mobile operators should carry out their own due diligence on aggregators prior to partnering.

### 2.3.1 PARTNERING WITH AGGREGATORS:

**Mobile operators should hold a range of information on all aggregators with whom they partner, for example:**

- Address and contact details of the aggregator's place of business
- Names and addresses of the owners / directors / shareholders
- The details of any parent company / holding company, if applicable
- The 'Doing Business As' or trade name
- The legal structure of the company

In addition, when considering a new partnership, the following types of question could help the mobile operator to make an initial assessment of an aggregator's capabilities:

- Does the aggregator have solid up-to-date knowledge of the PRS regulatory backdrop for the market(s) in which the operator proposes to partner with them?
- How long has the aggregator been active in the market? In the case of new entrants in particular, are they fully aware of and prepared for their responsibilities with regard to vetting and monitoring?
- What processes does the aggregator already have in place to vet content providers before launch and to monitor them on an ongoing basis after launch?
- If their current approaches are less robust than required by the operator, how will they address this gap?
- Does the aggregator have a compliance team that is proportionate to the size of its business operation?
- In markets where a centralised register of premium rate service players exists, does the register show that the aggregator in question has been associated with any significant breaches by the content / service providers they have enabled?
- Is the aggregator proposing to enable any higher risk categories of content service (e.g. live adult entertainment)? If so, how does the aggregator demonstrate enhanced vigilance in vetting and monitoring processes for this service type?

Mobile operators should be clear to aggregators about the consequences for them of compliance breaches by the content providers they have enabled:

- Different penalties will most likely apply depending of the level and nature of the breach but could include, for example, suspension or removal of service, fines, revoking of 'direct-to-bill' privileges, and so on. One UK operator, which carries out its own additional auditing of content partners through an agency, shares its auditor guidelines with the aggregators. The guidelines explain what the auditor will be checking for and how the operator views the severity of different offences – i.e. what would cause the operator to issue yellow cards (warning), red cards (service suspension) or even remove the service completely.

In addition to the areas outlined above, some operators have further measures in place to enhance their due diligence, such as:

- Carrying out physical audits of the aggregator's business premises to confirm, for example, that client data is held securely; and
- Aggregator accreditation programmes / training courses covering vetting, monitoring and auditing requirements which must be completed before the aggregator is allowed to submit content providers for approval.

### 2.3.2 PRE-LAUNCH VETTING OF CONTENT / SERVICE PROVIDERS

**It is likely that aggregators, rather than mobile operators, will carry out the pre-launch vetting of content / service providers. Some mobile operators may also wish to review the information gathered by the aggregators and approve / reject individual content providers depending on the findings.**

Aggregators should hold a range of information on all content partners that they enable, for example:

- Address and contact details of the aggregator's place of business;
- Names and addresses of the owners / directors / shareholders, plus previous trading history, where applicable;
- The details of any parent company / holding company, if applicable; and
- The 'Doing Business As' or trade name.

In addition, when considering enabling a new content provider, the following could help the mobile operator / aggregator to assess the content provider's risk profile:

- What type of content and service(s) does the provider offer?
- Does the content provider offer any higher risk categories of content service (e.g. live adult entertainment)? If so, what controls / policies does the content provider have in place (e.g. moderation processes)?
- Does a general review of the content provider's site provide evidence of a legitimate business? For example, does customer support work? Is it possible to register for and successfully use the service?
- In markets where a centralised register of premium rate service players exists, has the content provider in question got a record of any breaches?

For certain categories of content provider (e.g. new entrants, providers of higher risk categories of content), aggregators may wish to take additional steps, both pre-launch and potentially on an ongoing basis, such as:

- Advance review of new content;
- Advance review of draft promotional material, particularly for higher risk types of advertising such as web-based affiliate advertising; and
- Enable the content provider but with a low limit initially until trust has been fully established.

### 2.3.3 POST-LAUNCH MONITORING OF CONTENT / SERVICE PROVIDERS

**Even where pre-launch due diligence processes show that content providers are running legitimate businesses, once services are launched there could be attempts to process illegal activities through the original 'legitimate' account. Consequently, robust monitoring and auditing processes complement pre-launch vetting by helping to detect potential misuse and also acting as a deterrent to potential misuse.**

Aggregators can undertake a number of ongoing measures to help detect illicit activity once a content provider has been enabled. These include:

- Being alert to unusual patterns of activity relating to a particular content provider—such as spikes of traffic, or unusual and concerning customer complaints—and investigating the cause promptly;
- Hiring a 'web-spidering' company to trawl the web searching for where the aggregator's payment mark is offered and checking that the site is compliant with the aggregator's rules;
- Carrying out audits (in-house or through an external auditor) and 'mystery shopping' exercises to check for breaches and illicit activity; and
- Where relevant information is available to the aggregator, being alert to unusual consumer behaviours—for example, a disproportionately high percentage of pre-pay users making purchases from a given content provider, or a series of new pre-pay SIMs associated with a single handset which might suggest that a consumer is trying to hide illicit activities—and investigating whether these behaviours may be linked a potential breach by the content provider the consumer is purchasing from.

Tips for making 'mystery shopping' more robust and less easy to detect by the content and service providers being audited include:

- Change handsets used for testing sites; use a variety of pre-pay SIMs;
- If accessing sites from a computer, take steps (e.g. setting up a TOR network) to prevent sites visited from being able to recognise the auditor's internet connection and physical location; and
- Carry out testing at different times of day and night.

**FURTHER READING**

Financial Coalition Against Child Pornography: Internet Merchant Acquisition and Monitoring Best Practices for the Prevention and Detection of Commercial Child Pornography
**http://www.icmec.org/en_X1/pdf/InternetMerchantAcquisition.pdf**

European Financial Coalition best practice
**http://www.europeanfinancialcoalition.eu/document.php**

GSMA Mobile Alliance Against Child Sexual Abuse Content / INHOPE: Hotlines: Responding to reports of illegal content online – a guide to establishing and managing
**http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/Hotlines_WEB.pdf**

## ACKNOWLEDGEMENTS:

**The Mobile Alliance members would like to thank the following individuals and organisations for sharing their time and expertise to help us produce this paper:**

Homeland Security Investigations (HSI) Child Exploitation Investigations Unit (CEIU):
Neil J. O'Callaghan – Section Chief

International Centre for Missing & Exploited Children (ICMEC):
Catherine Cummings – Senior Director

Internet Watch Foundation (IWF):
Sarah Smith – Technical Researcher

National Bureau of Investigation, Sweden:
Björn Sellström – Detective Superintendent / Teamleader Cyber Crime Unit,
Johan Landström – Internet investigator

National Center for Missing & Exploited Children

PayPal: Kenny Logan – Brand Risk Management

Zong: Brian Wey – Director of Product Management

**Contact:**

For further information about this document or the Mobile Alliance Against Child Sexual Abuse Content, please email Samantha Lynch:
**sam.lynch@gsma.com**

**GSMA Head Office**
Level 7, 5 New Street Square, New Fetter Lane
London, EC4A 3BF, United Kingdom
Tel: +44 (0)207 356 0600

**www.gsma.com**