analysys mason

www.analysysmason.com

Report for PhonepayPlus

International-scale issues of non-compliance with premium-rate services

22 October 2012

Nico Flores, Helen Karapandzic and Jyotin Chhatwal Roy

Contents

This study aims to categorise international-scale PRS malpractice, assess regulatory strategies, and consider relevant lessons from adjacent sectors

Background and objectives

- Preliminary evidence from investigations by PhonepayPlus and other authorities responsible for regulating PRS around the world has highlighted issues around non-compliant PRS services that are targeted at users in multiple countries simultaneously
- PhonepayPlus has commissioned Analysys Mason to study these issues, ahead of discussions with other regulators.
- This study had the following objectives:
  - Survey and categorise cases of PRS malpractice into a **typology**
  - Identify the key **enablers** of these problems in terms of promotional methods, business practices and service mechanics
  - Identify the key factors that lead to the different types of malpractice gaining **international traction**
  - Identify relevant points of strength and weakness in different countries' **regulatory regimes**, and (if applicable) potential opportunities for reinforcement
  - Identify relevant **read-across** lessons and implications from other areas of the digital economy

Typology

- We have developed a typology for malpractice involving PRS by looking at (i) how payments are triggered and (i) what type of monetisation mechanism is used
- We look at two types of payment trigger:
  - **Social engineering (scams)** whereby victims are manipulated into giving consent for PRS payments – wittingly or unwittingly
  - **Technical malpractice (malware / hacks)** whereby technical means are used to generate payments without victims' direct involvement ('malware' or 'hacking')
- We consider three types of PRS monetisation mechanism:
  - Voice PRS
  - Premium SMS (PSMS)
  - Pay-per-page WAP
- Combining the above leads to a six-fold typology

analysys mason

Malpractice involving PRS is going mobile, social and, increasingly, international; we have identified eight key enablers

- We have identified eight key enablers behind PRS malpractice
- Enablers can broadly be grouped into three key areas based on whether they are specific to PRS and to their international spread:

  A ***Enablers that are not specific to PRS monetisation***

  – These call for regulatory focus on key players (legitimate or not) and, in some cases, collaboration with regulators from other areas beyond PRS (e.g. advertising)

  B ***Enablers that are specific to PRS monetisation but do not necessarily involve cross-country activities***

  – These require mainly national-level regulatory responses

  C ***Enablers that are specific to PRS monetisation and involve cross-country activities***

  – These call for routine processes for case-by-case international co-operation

- In addition, all types of enablers call for best-practice sharing by PRS regulators

Enabler groups and regulatory approaches

Stage	Description	Relevance to int'l spread	
Promotion	❶ Deep value chains in online advertising networks	●	
	❷ SMS and email spam	●	
	❸ Social media spam	◑	A
Pre-sales	❹ Deep value chains in affiliate websites	◔	
	❺ Smartphone vulnerabilities and third-party app stores	◕	
Monetisation	❻ Deep value chains in PSMS short-code provision	◔	B
	❼ Trans-national value chains in PSMS short-code provision	●	C
	❽ Multi-national PSMS intermediaries	●	

analysys mason

In future, PRS regulators will need to look beyond their traditional areas and coordinate internationally on key aspects

Beyond PRS

- A number of related trends beyond PRS are set to become increasingly important to PRS regulators:
  - **Direct carrier billing (DCB)** is emerging as an alternative to PSMS. Although so far malpractice is less common than for traditional PRS, this may change as the sector matures, especially if some of the patterns seen in PRS malpractice translate to DCB (e.g. long value chains)
  - **Virtual currencies** can potentially cross borders easily, and be used for money laundering. One type of virtual currency can already be purchased using direct carrier billing, and there is no reason to expect this not to become the norm
  - More generally, **fast innovation** is blurring the lines between multiple types of mobile money, mobile payments and mobile remittances. New players are "mixing and matching" different payment methods in new ways, comingling funds
  - Finally, a nascent move from **'closed loop' to 'open loop'** systems has the potential to blur the lines between new and traditional payment methods

Implications for PRS regulators

- PRS regulators are likely to need to increasingly work with regulators responsible for other areas – from online advertising to financial services and money-laundering
- In some cases, PRS regulators may need to seek modifications to their jurisdictions in order to operate effectively
- The regulation of PRS – and related issues – looks set to become an increasingly international affair, and PRS regulators are likely to need to cooperate internationally ever more closely, both on specific cases and through knowledge-sharing

Contents

This study aims to categorise international-scale PRS malpractice, assess regulatory strategies, and consider relevant lessons from adjacent sectors

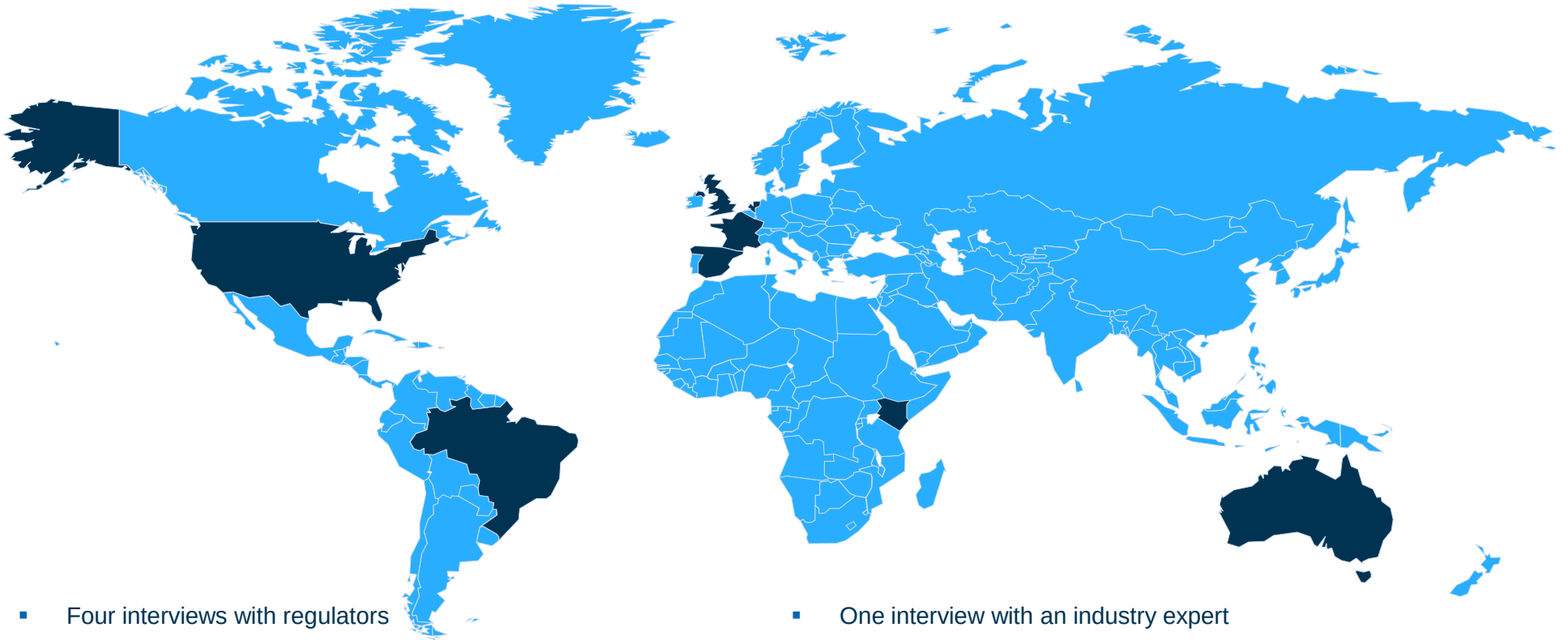
Background

- PhonepayPlus is the regulatory body for premium-rate telecommunications services ('PRS') that are accessible in the UK
- PRS include information and entertainment services paid for or accessed via premium SMS and WAP sites on mobile handsets, within smartphone applications, and via landline phones, faxes, email modems, alarm modems and interactive digital TV (premium-rate red button etc.)
- PhonepayPlus is also responsible for overseeing Payforit, the scheme offering direct operator billing services in the UK
- Preliminary evidence from investigations by PhonepayPlus and other authorities responsible for regulating PRS around the world has highlighted the issue of **non-compliant PRS that are targeted at users in multiple countries simultaneously**
- PhonepayPlus has commissioned Analysys Mason to study these issues, ahead of discussions with other regulators

Objectives and overview of this report

Objective	Description
Develop a typology	Survey and categorise cases of PRS malpractice
Identify enablers	Identify the key causes of these problems in terms of promotional methods, business practices and service mechanics
Develop epidemiology	Identify the key factors that lead to the different types of malpractice gaining international traction
Assess regulation	Identify relevant points of strength and weakness in the regulatory regimes of different countries and (if applicable) potential opportunities for reinforcement
Look beyond PRS	Identify relevant lessons and implications from other areas of the digital economy

This study was informed by ten expert interviews with regulators, operators and industry bodies in eight countries, and extensive secondary research



- Four interviews with regulators
- Three interviews with operators (two multinational)
- Two interviews with payment providers
- One interview with an industry body
- One interview with an industry expert
- Round table with members of the International Audiotex Regulator's Network (IARN)
- Documents provided by interviewees

Because several interviewees requested anonymity, we are only disclosing the countries covered. Target geographies were chosen in consultation with PhonepayPlus so as to reflect a broad range of perspectives. At interviewees' request, some interviews were conducted by email. Quotations have been paraphrased for succinctness. Secondary research included: a review of public and confidential documents kindly supplied by PhonepayPlus as well as interviewees; discussions with Analysys Mason experts; and other desk research.

analysys mason

Contents

Definitions

- For the purposes of this research, we have adopted the following key terms (a full glossary is provided in the annex):
  - **Premium-rate service (PRS)** – a content service charged by a third party (not an operator) to consumers' phone bills, triggered by consumers
    - calling premium-rate phone numbers;
    - sending or receiving SMS messages to/from premium SMS numbers or short-codes; or
    - visiting pay-per-page WAP pages
  - **PRS malpractice** – unless the context implies otherwise, means a **specific instance of non-compliant PRS services**; that is, a scheme involving a combination of promotional techniques, business practices and service mechanics that results in users being illegitimately billed for PRS
    - "Illegitimately" here means without the users' consent, or in a way that involves deceit
  - **Malpractice originator** – a party responsible for orchestrating the process whereby PRS malpractice is targeted at users; generally the party receiving the bulk of the resulting PRS revenues
  - **Scam** – PRS malpractice that relies on deceiving users into giving consent for PRS payments, or unwittingly performing an action that is interpreted as such
  - **Victim** – an end user who suffers financial harm through his/her phone bill as a result of PRS malpractice
  - **PRS regulator** – a regulator with responsibility for PRS, possibly among many other areas
- The definitions above cover a wide spectrum of malpractice – from outright fraud to merely questionable practices that may ultimately be found to be legal

Like any consumer service, PRS malpractices rely on a ‘sales cycle’, with discrete stages from promotion to content / service delivery

Promotion

- Users respond to promotional material or links, which eventually leads them to the PRS scam
  - *Examples include: online and in-app ads, spam (email, social media, SMS), listing in an app store, a QR code, print ads*

Pre-sales

- In some cases, victims are enticed to follow links to third-party websites, play a game, fill in forms, download software, etc. – all before PRS harm is triggered
  - *Examples include: following links to affiliate websites, filling in forms/quizzes online or via SMS (not PSMS)*

Payment

- At some point, an action is performed that leads to funds leaving the victim’s account; this may be on a recurring basis. This can be triggered by the user or by software on his/her device, typically without the user’s knowledge
  - *Examples include: scams, whereby the user sends PSMS or gives consent in an app or the mobile web; malware-based PRS malpractices, whereby an app or virus in the user’s device triggers payments*

Monetisation

- Eventually, funds are transferred from the victim’s account to the malpractice originator. This may involve various interim stages and intermediaries
  - *Examples include: PRS, direct carrier billing, virtual currencies, others (including credit card and bank transfers)*

Delivery

- The victim may or may not receive content or services associated with the scam or PRS malpractice
  - *Examples include: non-delivery of content, delivery of ‘broken’ content*

Players involved in different stages may or may not be knowingly involved in PRS malpractice

We have developed a typology of PRS malpractices based on the combination of payment trigger and monetisation mechanisms employed

- Before commencing the stakeholder interviews, we developed a typology of PRS malpractices that we validated with interviewees
- The typology was based on both the payment trigger and the monetisation mechanism employed
  - We identified two categories of payment trigger: (a) those that rely on manipulating the victim by exploiting personal vulnerabilities and/or social connections ('scams'); and (b) those that rely on technical means ('malware' or 'hacking'). In practice, (a) and (b) are often combined
  - PRS malpractices can be further subdivided according to whether the monetisation mechanism employed is voice-, SMS- or WAP-based PRS
- This gives six possible types of PRS malpractice:

Monetisation mechanism	Payment trigger: (a) Social engineering (scams)	Payment trigger: (b) Technical malpractices (malware / hacks)
PRS: Voice	Voice scams I	Voice hacks II
PRS: SMS	PSMS scams III	PSMS hacks IV
PRS: WAP	WAP scams V	WAP hacks VI

Most interviewees were concerned about PSMS, but two respondents cited concerns about malpractice involving voice-based PRS

PBX hacks are a concern for some operators; however, direct victims are typically businesses, not consumers

Interviewees reported a shift towards technical PRS malpractices, as technology advances

analysys mason

Illustrative* examples of PRS malpractices

	I Wangiri' calls a voice scam	II 'Diallers' a voice hack	III 'Win an iPad' a PSMS scam	IV PSMS trojans a PSMS hack	V Pay-per-page WAP scams	VI Pay-per-page WAP hacks**
Promotion	Victim receives a missed call – possibly from hacked PBX	Victim follows a link in an online ad or looks for PC software	Victim clicks on ad in mainstream website, or follows link in email or SMS spam	Victim sees seemingly legitimate games app in third-party app store	Victim receives SMS scam inviting him/her to follow a link	Victim sees seemingly legitimate games app in third-party app store
Pre-sales		Software is installed with or victim's knowledge	In second website, victim is enticed into entering a quiz or competition	Victim downloads pirated copy of a legitimate game, with malicious 'trojan' inside	Victim follows link, not knowing that this will incur PRS fees	Victim downloads pirated copy of a legitimate game, with malicious 'trojan' inside
Payment trigger	Victim calls back – to an international revenue share number (IRSN)	Software causes modem to call premium-rate voice numbers	Victim is persuaded to send a PSMS to have a chance of winning a prize	Trojan sends PSMSs without the victim's knowledge	Link points to pay-per-page WAP site; victim incurs PRS fees	Trojan loads pay-per-page WAP pages in background, unbeknown to victim
Monetisation	Scammer receives a share of the termination revenue	Malpractice originator receives a share of the PRS fees	Scammer receives a share of the PSMS fee	Malpractice originator receives a share of the PSMS fee	Malpractice originator receives a share of the pay-per-page WAP fee	Malpractice originator receives a share of the pay-per-page WAP fee
Delivery	No legitimate call was missed; victim's return call was unnecessary		There is no prize at stake, or the fees incurred are similar to the prize itself	App delivers the gaming functionality as advertised – through pirated software	Content promised in original SMS message may or may not be delivered	App delivers the gaming functionality as advertised – through pirated software

** Provided for illustrations purposes; many variants of these examples have been observed*

*** Hypothetical only; not reported by our interviewees*

Contents

Enablers of PRS malpractice today: summary

- We have identified eight key enablers behind PRS malpractice; each can be associated with a particular stage in the 'sales cycle' (see right)
- It is important to note that PRS malpractices often exploit several enablers simultaneously. For example:
  - Smartphone vulnerabilities can be used to disseminate PSMS malware in multiple countries, and
  - A chain of PSMS intermediaries that is both international and long can help the party behind the malware above to collect the resulting revenue in a way that is difficult to trace and which makes redress impractical
- Although not all the enablers listed are direct relevant to the international spread of malpractices, they are all involved in international-scale PRS malpractices
- Implications for regulators are discussed in the next section

Enablers grouped by stage in 'sales cycle'

Stage	Description
Promotion	❶ **Deep value chains** in online advertising networks
	❷ SMS and email **spam**
	❸ Social media **spam**
Pre-sales	❹ **Deep value chains** in affiliate websites
	❺ **Smartphone** vulnerabilities and third-party app stores
Payment trigger and monetisation	❻ **Deep value chains** in PSMS short-code provision
	❼ Trans-national **value chains** in PSMS short-code provision
	❽ Multinational PSMS **intermediaries**

Eight key enablers are driving malpractice involving PRSs; not all enablers are relevant to each type of scam or PRS malpractice

- In the course of our research and discussions with industry stakeholders, we identified eight key enablers – promotional methods, business practices and service mechanics – which contribute to the incidence of malpractice involving PRSs
- As shown below, not all of these enablers are contributing factors in the four types of malpractice identified in the previous section

Promotion

Pre-sales

Monetisation

Enablers	Voice scams I	Voice hacks II	PSMS scams III	PSMS hacks IV
❶ **Deep value chains** in online advertising networks			✓	✓
❷ Rise of **spam**, notably SMS spam			✓	✓
❸ **Social media** as a new channel for spam			✓	✓
❹ **Deep value chains** in affiliate websites			✓	✓
❺ **Smartphone** vulnerabilities and third-party **app stores**				✓
❻ **Deep value chains** in PRS number provision	✓	✓	✓	✓
❼ Trans-national **value chains** in PRS number provision	✓	✓	✓	✓
❽ **Multinational** PRS intermediaries	✓	✓	✓	✓

analysys mason

❶ Deep value chains in online ad networks allow malpractice originators to place advertisements without dealing with media owners

- Online ad networks act as intermediaries between websites and advertisers. This helps those responsible for PRS scams or malware, because
  - Due diligence is impractical: mainstream websites selling inventory to ad networks rely on them to carry out due diligence on advertisers; adherence to good practice may fall when inventory is resold
  - It may be hard to identify the author of an advertisement
  - Regulation is difficult because of the complexity of business arrangements, extra-territoriality issues and limited jurisdiction for telecoms regulators
- Problems are exacerbated by
  - Affiliate websites (see Enabler #4 below)
  - Ad exchanges and retargeting services, which allow ad space inventory to be sold and resold in real time across a wide range of parties
- Both of these increase the length of the chain between advertiser and website

Key points

Relevance to PRS scams	**Strong**, as users may follow links to third-party websites with scam details
Relevance to PRS malware	**Strong**, as users may follow links to malware downloads
Link to international spread	**Strong**, as narrowing the target audience of an ad network to one country is actually more costly than targeting all international audiences

Value chain

analysys mason

❷ The proliferation of managed spam services allows malpractice originators to target an international audience in a cost-effective manner

- Recent years have seen a rise in SMS and email spam, potentially exposing recipients to malicious links, malicious payloads and fraudulent propositions
- Key drivers include:
  - The proliferation of **managed spamming services**, which allow spammers to create highly targeted propositions based on mobile numbers, a specific mobile number range, or based on a specific carrier or geography (country/city)
  - The availability of **DIY SMS spammers**, some of which allow spammers to send spoofed SMS messages internationally
  - **Managed localisation and proofreading services**, enabling mass spamvertised campaigns, with localised messages delivered via SMS/MMS or fax in the language of the prospective recipients
  - The ready **availability of low-cost harvested email databases**. Security blog Webroot identifies a Russian underground market proposition (shown right) offering harvested email databases for sale. As an example, 130,000 UK-based harvested emails cost USD100

Key points

Relevance to PRS scams	**Strong** – potentially exposes users to malicious links and fraudulent propositions
Relevance to PRS malware	**Strong** – potentially exposes users to malicious payloads
Link to international spread	**Strong** – increasing internationalisation of spam services, allowing malpractice originators to target international audiences in a cost-effective way

Screenshot of a Russian underground marketplace offering harvested email databases for sale

❸ Social networks provide powerful new channels for spammers, who exploit social connections and consumer trust in personal recommendation

- Social networks are built on strong trust and reputation systems, and it is precisely these foundations (and the social connections that underpin them) that spammers exploit when they use social media to drive traffic to – often malicious – third-party websites through links placed on social media services
- Social media has emerged as a key channel for the promotion of affiliate marketing scams leading to PRS. One survey suggests that 57% of users claim to have been spammed via social networking sites, and 36% claim they were sent malware via these sites[1]
- Social media spam may use technical hacks to inflict harm without users having to follow a link. In a high-profile case in 2010 (known as "onMouseOver"), hackers embedded JavaScript code into Twitter messages which had the capability of retweeting, activating pop-ups, and redirecting users to pornography sites
- **'Likejacking'** is another form of social scam, which tricks Facebook users into 'liking' pages which may include malicious links, malicious payloads and fraudulent propositions. When a user 'likes' a page, his/her entire contact list is notified in a network effect
- Social networking sites are also famous for their **'widgets'** (third-party apps that can be added to accounts) – which represent a potential source of malware

Key points

Relevance to PRS scams	**Strong**, as users may follow links to third-party websites with scam details
Relevance to PRS malware	**Strong**, as users may follow links to malware downloads
Link to international spread	**Moderate**, as social networks are themselves highly international

[1] *Source: Sophos, February 2010*

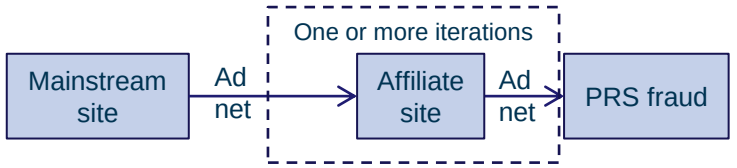
❹ Affiliate websites further separate malpractice originators from the mainstream websites where the 'sales cycle' often begins

- Ads that appear on affiliate websites may have been placed through ad networks with **little or no due diligence**
- It is often difficult to identify the source of the scam, because **malpractice originators often use multiple affiliate websites in sequence**. By hiding malpractices behind a number of business entities, it becomes unclear whether a given affiliate network or the promoters themselves are aware of the fact that they are promoting illegitimate or grey activities
- Affiliate website operators are rewarded each time a user sees and/or clicks an advertisement listed by them
- Users typically first arrive at affiliate advertising websites after following a link (advertisement or spam) on a mainstream, content-based website or social network; to entice users to visit them (and search engines to list them), affiliate sites often offer low-quality, free 'content' in addition to adverts – e.g. games
- PRS malpractice is typically perpetrated by a third party – i.e. not the affiliate advertising site's owner, but a party who advertises on it (see right). However, the distinction is not always clear:
  - some scam sites (e.g. "win an iPad" type quizzes) also list adverts on the side, and
  - some adverts conduct scams or hacks *in situ* without the user having to visit the malpractice originator's website

Key points

Relevance to PRS scams	**Strong**, as users may follow links to third-party websites with scam details. Affiliate websites are far more likely to advertise scams and malware than mainstream sites
Relevance to PRS malware	**Strong**, as above. Additionally, ads on affiliate sites may have direct links to malware downloads – or even trigger them without user interaction
Link to international spread	**Strong**, as affiliate websites may facilitate cross-national value chains between malpractice originators and the websites where users may enter the 'sales cycle'

User journey



analysys mason

❺ Device/OS vulnerabilities and third-party app stores are key enablers for PSMS hacks, with Android particularly vulnerable

- In the last 12 months, there has been a rapid rise in SMS malware (including both bogus apps and trojanized versions of, or updates to, legitimate apps), which run in the background and send premium SMS without users' authorisation
- This relies on key vulnerabilities in mobile devices and their operating systems. These include:
  - allowing the installation of software with no credentials
  - weaknesses in authentication checking, failing to identify whether downloaded software is authentic
  - availability of OS APIs allowing applications to send and intercept SMS without users' knowledge
- Vulnerabilities vary across mobile operating systems – Android is perceived as more vulnerable than iOS
  - In the last 6–12 months, Google has increased security features on Google Play, including launch of the "Bouncer" malware detection system in February 2012. This may lead to an increase in malicious apps on third-party markets, as well as an increase in malware variants trying to bypass these new security measures in the Android Market
- App stores are just one way in which mobile malware can be spread; malicious payloads and fraudulent propositions can also be triggered by users clicking on malicious links on websites and social media sites

Key points

Relevance to PRS scams	**Limited –** users whose devices can be hacked often don't need to be deceived into accepting PSMS payments
Relevance to PRS hacks / malware	**Strong** – this is an essential enabler for PSMS malware
Link to international spread	**Moderate** – not a major enabler in itself, but certain third-party independent stores in jurisdictions with poor regulation play a key role in spreading malware

Third-party app stores – screenshots

analysys mason

❻ Deep value chains in PSMS short-code sub-letting and chaining can obstruct due diligence, regulation, enforcement and redress

- Malpractice originators of PRS scams and fraud are generally unlikely to deal directly with operators or aggregators – as they would be unlikely to pass due diligence processes
- Instead, they rely on intermediaries who have themselves been vetted, and who in turn 'sublet' a short code while applying less stringent vetting procedures. This process is often iterated
- Under a variant of this practice, an information provider will sub-let a given PSMS short code to multiple tenants, with prefix keywords in the SMS body used to identify which tenant a message is meant for
  - in a recent development, tenants may in turn sub-let their prefix to multiple sub-tenants, each of which is identified by a second prefix which is also included in the SMS body
- These (in themselves, legitimate) practices can hamper:
  - **Due diligence**, as upstream providers must rely on their customers for vetting, who must do the same – and so on. The longer the value chain, and the smaller the downstream players, the more problematic this is
  - **Redress and enforcement**, as it can be difficult to identify or contact the ultimate actor behind a malpractice
  - **Regulation and legislation**, given the cross-border nature of many of these relationships (we discuss this below)

Key points

Relevance to PRS scams	**A key enabler** – allows malpractice originators to evade the vetting processes of operators and PSMS aggregators
Relevance to PRS hacks / malware	**A key enabler** – for the same reasons as above
Link to international spread	Only when supply chains cross borders (these cases are covered in the next slide)

analysys mason

7 Cross-border supply chains in PSMS short codes make regulation and enforcement difficult, even when only one country is targeted

- Supply chains in PSMS short codes are not only long. Crucially, often they also **cross borders** once or more between aggregators and scam/fraud malpractice originators
- For regulators this raises key challenges:
  - It makes investigating issues a highly challenging task
  - Investigation and enforcement require international co-operation
  - In some cases, jurisdictional limitations mean that regulators cannot even investigate
- These regulatory challenges mean that cross-country approaches can help scammers even when they target a single country – even if the malpractice originator is in the same country as the victim
- Interviews suggest that a significant percentage of PRS scams are cross-border

Key points

Relevance to PRS scams	**Strongly relevant** – a key way for malpractice originators to escape enforcement – for both single- and multi-country scams
Relevance to PRS hacks / malware	**Strongly relevant** – as above
Link to international spread	**Strongly relevant** – a necessary condition for any international scam

"International content providers account for about 40% of content providers in our country. They are based in China, Middle East, England, Ireland etc. They can register online and contract with an aggregator. […] Imagine the difficulties trying to issue a notice to a content provider in a country that does not recognise your legal system." – *A regulator*

analysys mason

❽ Multi-country PRS aggregators have the potential to act as 'one-stop shops' for malpractice originators – but evidence so far is limited

- Multi-country PRS aggregators allow content providers to target multiple countries simply, by providing
  - local PSMS short codes or voice numbers for each country
  - centralized monetisation
  - all through a single contract
- This has the potential to greatly simplify malpractice originators' work. While cross-country supply chains are a key enabler for multi-country PRS malpractice, multi-country PSMS aggregators are a one-stop shop
- Multi-country aggregators tend to be larger businesses – they are relatively visible to regulators and so may have more to lose from sanctions
- Nonetheless, there is concern among some regulators that international PRS aggregators (wittingly or unwittingly) facilitated international-scale PRS malpractice in the past

Key points

Relevance to PRS scams	**Strongly relevant –** but only in PRS malpractices' international dimension|
Relevance to PRS hacks / malware	**Strongly relevant –** but only in PRS malpractices' international dimension|
Link to international spread	**Strongly relevant** – potentially a key facilitator

"Many of the companies that perpetuate the fraud are international companies […] these have opened local operations in [our country]"
– Industry body

analysys mason

Contents

Epidemiology and regulation: summary

- In the previous section we identified eight key enablers; these can broadly be grouped into three key areas based on whether they are specific to PRS and to their international spread:

  A ***Enablers that are not specific to PRS monetisation***

  – These call for regulatory focus on key players (legitimate or not) and, in some cases, collaboration with regulators from other areas beyond PRS (e.g. advertising)

  B ***Enablers that are specific to PRS monetisation but do not necessarily involve cross-country activities***

  – These require mainly national-level regulatory responses

  C ***Enablers that are specific to PRS monetisation and involve cross-country activities***

  – These call for routine processes for case-by-case international co-operation

- In addition, all types of enablers call for best-practice sharing by PRS regulators

Enabler groups and regulatory approaches

Stage	Description	Relevance to int'l spread	
Promotion	❶ Deep value chains in online advertising networks	●	
	❷ SMS and email spam	●	
	❸ Social media spam	◑	A
Pre-sales	❹ Deep value chains in affiliate websites	◔	
	❺ Smartphone vulnerabilities and third-party app stores	◕	
Monetisation	❻ Deep value chains in PSMS short-code provision	◔	B
	❼ Trans-national value chains in PSMS short-code provision	●	C
	❽ Multi-national PSMS intermediaries	●	

analysys mason

A Non PRS-specific enablers call for regulatory focus on key players and, in some cases, collaboration with regulators from other areas beyond PRS

- Issues related to the **promotion** of PRS scams, and also to the **spreading of malware**, are important to counter PRS malpractice. However:
  - The relevant industries are large, complex and go well beyond PRS (e.g. online advertising, social networks)
  - The same issues are relevant to addressing malpractice involving ID theft, credit card fraud, money laundering, counterfeit goods, etc.
  - Our interviews suggest that jurisdiction sometimes falls outside the agencies responsible for PRS – e.g. on those responsible for trading standards or advertising
- Because of this, PRS regulators should consider
  - Working closely with regulators responsible for other areas (e.g. advertising, financial fraud), when appropriate
  - Focusing strategically on some of the key relevant players (many of whom may be legitimate – e.g. social networks), fostering intelligence-sharing and helping to ensure that malpractices are dealt with efficiently and effectively
  - When these players are international, PRS regulators may benefit from a co-ordinated approach
- In all cases, international sharing of best practices would be appropriate

Enablers not specific to PRS monetisation

1. **Deep value chains** in online advertising networks
2. SMS and email **spam**
3. Social media **spam**
4. **Deep value chains** in affiliate websites
5. **Smartphone** vulnerabilities and third-party **app stores**

analysys mason

B PRS-specific enablers that are not international in scope call for national-level responses – but also for sharing of best practices

- Adequate regulation and enforcement concerning PRS malpractices can reduce their incidence at a national level – and, by extension, also internationally
- While addressing these issues does not always call for a concerted international approach, regulators can benefit from sharing best practice
- We have noted significant disparities in the extent to which the regulatory set-up behind PRS prevents malpractice
  - For example, in some countries it is possible for third parties to arrange for operators to bill subscribers for services with only minimal (and potentially false) evidence of consent
- There are similarly wide variations in the institutional set-up
  - For example, to our knowledge the UK is the only country with formal regulation for direct carrier billing (discussed separately below)
- Knowledge about PRS malpractice varies widely among regulators

Enablers that are specific to PRS monetisation but do not necessarily involve cross-country activities

⑥ **Deep value chains** in PRS number provision

Other national-level PRS-specific enablers, such as

- Poor due diligence requirements
- Lack of minimal delay for funds release

"Continued collaboration [is necessary] at industry level on matters related to fraud intelligence and fraud prevention"
– An operator

"The problem with [PRS malpractice] is that so many parties win from it – operators do, aggregators do, malpractice originators do – and nobody is incentivised to stop it"
– A regulator

analysys mason

C PRS-specific enablers that are international in scope call for routine processes for case-by-case international co-operation

- Interviews suggest that a large and growing proportion of cases of PRS malpractice involves cross-border supply chains. Although regulators are aware of the problem, some feel that the situation is beyond their control or outside their remit. This is due to:
  - Logistical complications in investigating international cases
  - Inability to issue or enforce rulings
  - Doubts about whether regulators are legally allowed to investigate internationally
- Although evidence of problems involving multi-country PSMS aggregators is inconclusive, the scope for malpractice is clear
- These issues require international case-by-case co-operation. In turn this would be facilitated by internationally agreed, **routine processes** for intelligence-sharing and enforcement

Enablers that are specific to PRS monetisation and involve cross-country activities

7 Trans-national **value chains** in PRS number provision

8 Multinational PRS intermediaries

Overseas content providers are responsible for a large and growing proportion of problems in our country. However, because of jurisdictional limitations we cannot even investigate these issues – let alone issue and enforce rulings
– Based on discussion with an Industry body

"International content providers account for about 40% of content providers in [country]. They are based in China, Middle East, England, Ireland etc. They can register online and contract with an aggregator. […] imagine the difficulties trying to issue a notice to a content provider in a country that does not recognise your legal system."
– A regulator

"Regulatory and other efforts [are required] to ensure that some of the exposures in the global voice marketplace are not repeated for other services"
– An operator

analysys mason

Contents

Summary: A number of trends mean that PRS regulators will increasingly need to deal with issues beyond their traditional remit

- A number of related trends beyond PRS are set to become increasingly important to PRS regulators:
  - **Direct carrier billing (DCB)** is emerging as an alternative to PSMS. Although so far malpractice is less common than for PSMS, this may change as the industry matures, especially if some of the patterns seen in PRS malpractice translate to DCB
  - **Virtual currencies** can potentially cross borders easily, and be used for money laundering. One type of virtual currency can already be purchased using direct carrier billing, and there is no reason to expect this not to become the norm
  - More generally, **fast innovation** is blurring the lines between multiple types of mobile money, mobile payments and mobile remittances. New players are “mixing and matching” different payment methods in new ways, comingling funds
  - Finally, a nascent **move from ‘closed loop’ to ‘open loop’ systems** has the potential to blur the lines between new and traditional payment methods

Direct carrier billing is emerging as an alternative to PSMS – so far malpractice is less common than for PSMS, but this may change

- **Direct carrier billing (DCB**) allows merchants to bill consumers through their mobile phone bills by interacting with operators' technical systems – usually through an intermediary – without the use of premium-rate voice or text
- A typical set-up involves an accredited payment intermediary (API) acting between operators and merchants. Also, APIs often provide services to "stores" (e.g. Facebook, Blackberry), which in turn allow their merchants to charge consumers
- Traditionally, DCB has been used mainly to sell virtual goods and digital content, but that is now changing. For example, in February 2012, Boku launched physical in-store payments
- Key players tend to be global in scope; they have deals with many operators around the world and provide a "one-stop shop" for merchants
  - Although the risks from this are obvious (see enabler #8 earlier in this document), we have not seen evidence of related international-scale scams
  - This is likely due to self-policing; high transaction costs; adequate technology; small number and large size of players; and short value chains
  - However, as the sector develops these barriers may diminish, raising the possibility that today's PRS scams may migrate to DCB

Key points

Link to PRS	Operator-facilitated payments make this a natural area for PRS regulators. Some key players (e.g. Boku) started in PSMS space and are making the transition transparent for their merchants
Malpractice and regulatory challenges	In general, malpractices are rare and of the "scam" variety (and we are aware of no multi-country cases). However, all of this may change as the sector develops
Regulatory approach	Very varied. UK is the only country (to our knowledge) with formal regulation through Payforit scheme
Key players	Boku, Bango, Zong

"Our technology makes DCB hacks impossible" – *An operator*

"Direct carrier billing flattens the world for merchants – and potentially for perpetrators of PRS malpractice" – *Industry source*

"DCB players spend a lot on risk control – this is costly but necessary and has paid off" – *An operator*

analysys mason

Virtual currencies can be purchased using direct carrier billing – they can potentially cross borders easily, and be used for money laundering

- **Virtual currencies** are electronic tokens that can be purchased using real money. They can be used within certain online environments to purchase virtual goods (e.g. a "house" in Second Life) or services (e.g. the right to play a game in Facebook) or digital content. Some virtual currencies may also be exchanged person-to-person (p2p)
- There are serious risks of financial malpractice, including money laundering and illicit international remittances, when
  - Users can trade virtual currencies in exchange for virtual goods among themselves
  - Virtual currencies can be converted back into real money
- To counter these risks, some platforms have sought to restrict internal trading and/or convertibility; however, these efforts have given rise to black markets
- Some currencies can be openly traded in organised, third-party exchanges such as WirWox
- Bitcoin is a unique case in that it is fully decentralised and does not rely on a centrally managed platform. Further, its technical architecture is designed to guarantee anonymity. All of this makes it a uniquely attractive option for criminals

	Key points
Link to PRS	PSMS and DCB can be used to purchase virtual currencies – for example, in Facebook, using Bango Virtual currencies can cross national borders easily – potentially facilitating international PRS scams
Malpractice and regulatory challenges	Money laundering – although nascent, cases have been documented*
Regulatory approach	Limited regulation. In principle, this is within financial regulators' jurisdiction
Key players	• Platforms: Facebook, Second Life, World of Warcraft • Platform-independent currencies: Bitcoin, e-gold • Exchanges: WirWox, FirstMeta, Bitcoinica

"At this stage, the misuse of digital currencies and virtual worlds for money laundering is still very much an emerging vulnerability"
– AUSTRAC CEO John Schmidt, Computerworld Australia 15 Aug 2012

** Financial Action Task Force: "Money laundering using new payment methods" Oct 2010; AUSTRAC: "Typologies and case studies report" 2012*

Fast innovation is blurring the lines between multiple types of mobile money, mobile payments and mobile remittances …

- New mobile-based payment methods (both B2C and P2P), remittances and stored-credit systems are emerging and evolving with increased speed across the world
- In emerging markets, mobile payments are a key opportunity for providing basic financial services to the unbanked:
  - In Kenya, mobile payments platform M-PESA (launched in March 2007) is used by around 36% of the population
  - In some markets, mobile airtime has emerged as a tradable currency
- Innovation is not limited to emerging markets. For example:
  - eBay provides both payments and stored credit
  - Operators (through projects such as ISIS in the USA and OSCAR in the UK), credit card companies and Internet companies (e.g. Google via Google Wallet) are racing to bring NFC payments to retail
  - New providers Point of Sale solutions for merchants (Square, iZettle, Paypal Here) may transform payments, for example offering consumers alternatives to credit cards
- New players are "mixing and matching" different payment methods in new ways, comingling funds. As this happens, a more holistic approach to regulation is required, requiring cooperation between different regulatory bodies

Key points

Relevance to PRS	Boundaries between new payment methods are blurring. In particular, DCB may in future be used as a top-up-mechanism for stored-value payment systems
Malpractice and regulatory challenges	New payment methods afford numerous opportunities for money laundering, tax evasion, etc. As these come into contact with PRS and DCB, they become relevant to PRS regulators
Regulatory approach	In general, non-PRS systems are currently the focus of interest by global monetary institutions, as well as national and international anti-money laundering bodies

"Regulators take different views in different countries – in one, the government got so fed up with the lack of innovation by the banks that it allowed them to handle up to $500 worth of transactions without regulation. India is at the other extreme – very controlling." – *Industry source*

"In emerging market countries prepay airtime can often be sold by one customer to another at close to face value. This, together with the provision of peer to peer airtime transfer services in these markets, creates a potential opportunity for fraudsters" – *Industry source*

** World Bank: "Protecting mobile money against financial crimes", 2011*

… and a nascent move from ‘closed loop’ to ‘open loop’ systems has the potential to blur the lines between new and traditional payment methods

- In the physical retail environment, there has been a rise in prepaid stored-value cards not limited to a particular merchant or to a customer’s bank account
  - Stored value card providers partner with banks to include PANs (primary account numbers i.e. 16-digit numbers) in prepaid cards, which allows them to be used in the worldwide ATM network as well as retail outlets that accept Visa or MasterCard
  - In industry parlance, this is a move from ‘closed loop’ to ‘open loop’ systems, as credit can be used in the wider economy and not with affiliated merchants
- Recent developments have seen the extension of this trend to the mobile payment industry, with providers offering users “virtual PANs” without physical debit cards:
  - Visa’s acquisition of Fundamo in June 2011 aims to “expand the utility of closed-loop systems, enable them to be interoperable, make financial services available to more consumers and offer merchants access to new customers”*
  - MTN signed a deal with Fundamo VISA in November 2012 to convert its closed-loop operations into VISA open-loop offerings

Key points

Relevance to PRS	Inasmuch as PRS and DCB are part of this movement, they will also increasingly come into contact with the wider economy
Malpractice and regulatory challenges	If PRS or DCB are used as topping-up mechanisms for universal-purpose payment systems, the contexts and types of harm from associated malpractice may multiply
Regulatory approach	As with new payment methods generally, the move to open loop is a topic of interest from global, national and regulatory bodies. However, PRS regulators are only beginning to be aware of the issues

“Facilitating the opening of formerly closed loops will be a key business opportunity in the developing world – lots of money will flow this way”
– Industry source

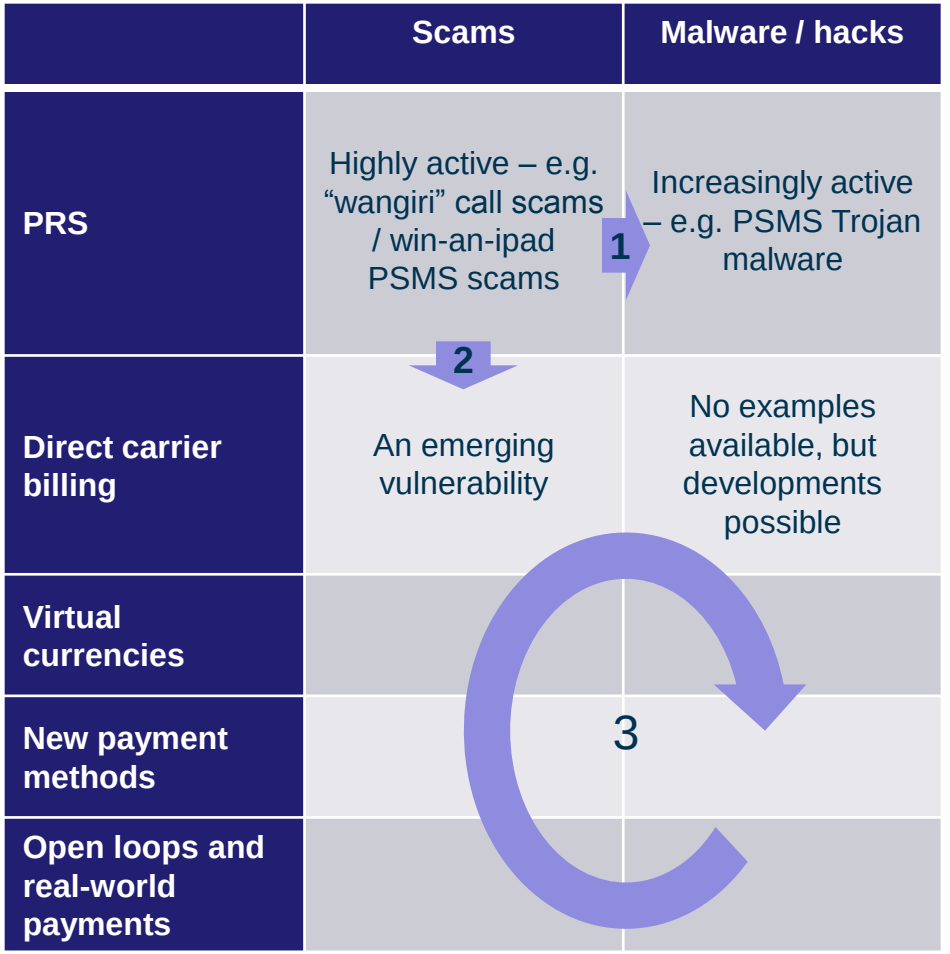
*Visa press release

Contents

Rapid changes in technology and business models mean that PRS regulators will increasingly need to look beyond their traditional areas

- **PRS regulators**
  - **are likely to need to increasingly work with regulators responsible for other areas – from online advertising to financial services and money-laundering**
  - **in some cases they may need to seek modifications to their jurisdictions in order to operate effectively**
- Traditional demarcations of premium-rate services are likely to come under increased strain:
  1. The spread of smartphones (especially in developing markets) is likely to drive malware-based scams of all types – in PRS and beyond
  2. Issues that started around PRS may propagate to direct carrier billing
  3. The lines between new payment methods (including DCB) are likely to become blurred, as payments made with one method may find their way to another, and new business models combine payment methods in new ways
- Additionally, effectively tackling PRS and similar issues requires acting at the promotional stage of the 'sales cycle' – that is, in the worlds of online advertising and social networks

PRS and related areas – the present



analysys mason

PRS malpractice and related issues are becoming increasingly international – and call for correspondingly international responses

- **The regulation of PRS – and related issues – looks set to become an increasingly international affair, and PRS regulators are likely to need to cooperate internationally ever more closely, both on specific cases and through knowledge-sharing**
- The growing prevalence of cross-border, multi-country PRS malpractice calls for international collaboration on a case-by case basis.
  - In turn, this calls for internationally agreed, routine process for intelligence-sharing and enforcement
  - The urgent need for better arrangements is keenly felt by some of the regulators we spoke to
- Additionally
  - The key role played by certain large, legitimate international players in unintentionally facilitating malpractices (in all stages of the 'sales cycle', from promotion to monetisation) calls for joined-up action by PRS regulators from multiple countries
  - The complexities of the issues involved and their rapidly evolving character call for regular sharing of best practices by regulators

Contents

Glossary [1/2]

Term	Definition
Affiliate website	For the purposes of this report, an affiliate website is a website whose main purpose is to advertise, and provide links to, other websites, from which it receives payment each time a user follows a link. Ads to other websites may be provided by advertising networks, which act as intermediaries between websites. Affiliate websites get their own traffic from other affiliate websites, from ads placed on mainstream websites via ad networks, from search engines and from spam.
Aggregator	An SMS aggregator is a company with agreements with multiple operators (sometimes in multiple countries) to send and receive data in and out of the operator's short message service centres , acting as an intermediary between companies (i.e. information providers) who want to interact with end users (through their mobile phones) and mobile operators
Authentication	The process of establishing that (a) a user request is genuine before placing a charge on the user's account; or (b) an app is genuine before it is accepted by an app store, downloaded or executed
Closed-loop payment system	A payment or stored value system that can only be used to redeem goods or service from owner of the payment system (e.g., an iTunes gift card) or affiliated third parties
Direct carrier billing (DCB)	A set of technologies and standards that allow merchants to bill consumers via their mobile bills. Consumers give consent on the mobile web or within smartphone apps, and authorizations and payments are channelled through an Approved Payment Intermediary. In the UK, Direct Carrier billing is regulated under PhonepayPlus' Payforit scheme
Malvertising	The abuse of legitimate systems and processes employed to mislead users into viewing products or services that they would not otherwise view
Malware	Executable code running on a consumer device (e.g. a smartphone or a PC) that performs a malicious act, e.g. steal personal information or send unauthorized premium-rate messages. Includes viruses, trojans and fake apps.
Near field communications (NFC)	A short-range wireless technology standard. It uses an initiator (an RF field) to activate a passive target (e.g. a tag, sticker or card) to initiate data exchange or an application, such as contactless payment

Glossary [2/2]

Term	Definition
Open-loop payment system	A payment or stored value system that can be used not only with the system's originating party (e.g. an iTunes gift card) or with affiliated merchants (e.g. Paypal credit), but with merchants in the wider economy. Payment systems achieve this by partnering with banks to include PANs (Primary Account Numbers – i.e. 16-digit numbers) which can be used in the worldwide ATM network as well as with any merchant who accepts Visa or Mastercard
Premium-rate service (PRS)	For the purposes of this report, PRS denotes a content service charged by a third party (not an operator) to consumers' phone bills, triggered by consumers calling premium-rate phone numbers; sending or receiving SMS messages to/from premium SMS numbers or short-codes; or visiting pay-per-page WAP pages.
PRS malpractice	A scheme that results in users being billed for PRS without their consent, or in a way that involves deceit
PRS regulator	A regulator with responsibility for PRS, possibly among many other areas
QR (quick response) code	A type of two-dimensional code commonly used in consumer advertising and packaging that can be read using a barcode scanner on a smartphone and used to load any recognised web URLs on the device's web browser
Scam	A PRS malpractice that relies on deceiving users into giving consent for PRS payments, or unwittingly performing an action that is interpreted as such
Short code	A special telephone number, significantly shorter than a full telephone number, which can be used to address SMS and MMS messages from certain service providers' mobile phones or fixed phones. Short codes are widely used for value-added and premium-rate services
Victim	An end user who suffers financial harm through his/her phone bill as a result of PRS malpractice
Virtual currency	Electronic tokens that can be purchased using real money, and can be used within certain online environments to purchase virtual goods (e.g. a "house" in Second Life), services (e.g. the right to play a game on Facebook) or digital content, and can be exchanged person to person.