

# CHILDREN AS CONNECTED CONSUMERS

PhonepayPlus' plans and priorities for  
empowering and protecting children



# CONTENTS

## Section

1	INTRODUCTION	<a href="#">03-04</a>
2	CHILDREN AS CONNECTED CONSUMERS	<a href="#">05-06</a>
3	POTENTIAL RISKS TO CHILDREN	<a href="#">07-11</a>
4	PROTECTING AND EMPOWERING CHILDREN AND PARENTS	<a href="#">12-13</a>
5	STRATEGIC PRIORITIES	<a href="#">14-15</a>

## [PhonepayPlus – who we are and what we do](#)

PhonepayPlus is the independent regulator of premium rate services (PRS – see opposite) in the UK. We are a non-statutory, industry-funded body with over 25 years' experience of regulating PRS. Our vision is that everyone should be able to use PRS with absolute confidence.

Under the Communications Act 2003, Ofcom has strategic responsibility and accountability for the regulation of PRS. PhonepayPlus, which has been regulating the market since its introduction in 1986, has been appointed to carry out the day-to-day regulation using a Code of Practice, which is approved by Ofcom (the Code). The Code gives us a range of powers to investigate and address consumer harm (such as the harm caused by those who run 'scams') through robust sanctions, including fines for breaches of the Code.

Rather than just dealing with harm and scams after they occur, we place emphasis on pre-emption and prevention of harm by working with industry to drive up standards in the market and by taking swift action to tackle emerging risks before they set in. This approach has increased consumer confidence in the market, which is essential for growth and a competitive and fair market. For example, consumer confidence in pricing transparency on PRS has increased by nearly 60% over the past two years, which is good news both for consumers and for businesses.

# 1. INTRODUCTION

## Children, the digital marketplace, connected devices and PhoneyPayPlus

This plan sets out PhoneyPayPlus' approach to protecting and empowering young people who use premium rate telephone services (PRS). These are services that are charged to people's phone bills or pre-paid accounts and can include voting in TV broadcast competitions, playing online games, downloading music or downloading apps on to a smartphone.

Children are increasingly and inevitably engaging in a lifestyle that is digitally connected through the use of smartphones and other connected devices. Children's connected lifestyles mean that they are increasingly exposed as 'connected consumers' to a wide range of content and purchasable services. Whilst there are many benefits to children from being connected to other people and to services in this way, this degree of connectivity also gives rise to potential risks to children.

Our children's plan is intended to:

- **Set out PhoneyPayPlus's role in child protection and where we fit alongside others working in this area;**
- **Describe how we see children's use of digital services changing as a result of new technologies – including the shift from fixed-line internet to the mobile internet – and the potential risks that this can give rise to; and**
- **Set out what PhoneyPayPlus is doing within our remit to protect and empower children and what we see as our main priorities in this area over the coming year.**

In setting out this plan and related priorities, we do not intend to discourage children from using premium rate services or other digital services. Clearly, these services can offer substantial benefits to children in terms of entertainment, social networking and education and most children use them without experiencing harm. However, we believe that children and their parents should have the information to understand and safeguard against potential risks and that regulators, industry and other bodies with an interest should remain vigilant and engaged on these matters.

We would welcome input and feedback from interested parties on the analysis and priorities set out in this document. We would also be keen to hear from any further bodies active in this area with whom we could work in taking forward these priorities.

## PREMIUM RATE SERVICES

PRS are added-value services that consumers purchase by charging the cost to their phone-bill or mobile (pre-pay) account. Convenience, spontaneity and value are the primary factors why consumers use PRS. Some current and popular examples include voting in TV competitions, directory enquiries, donations to charity via text messages and playing online games.

PRS started out as higher-rate fixed line numbers (i.e. 09, 118 and 0871/2/3 number ranges) that could be used to access a range of services. The industry then developed into mobile text shortcodes – five- and six-digit mobile numbers used, for example, to enter competitions or download mobile content. The latest evolution of the PRS market is into the apps arena, with consumers downloading digital content and services from apps stores (such as Google Play) onto their smartphones and charging the app or the cost of using the app to their phone bills.

In 2011, the UK PRS market was worth an estimated £800m, with almost 4,000 registered providers located across 75 countries, reflecting the global nature of the industry we regulate. In short, whilst the traditional sectors of the PRS market remain, PRS is now (and in future will become increasingly more) a micropayment for purchasing digital content and services.

### PhonepayPlus' role in protecting and empowering children

The protection of children online is a wide area that covers a number of issues and where a large number of organisations have important roles to play.

The UK Council for Child Internet Safety (UKCCIS), under the leadership of the Department for Education and the Home Office, brings together over 180 organisations and individuals from government, industry, law enforcement, academia, charities and parenting groups to deal with these issues.

We recognise that our role in online child protection is relatively niche. We are a general consumer regulator, rather than a child protection body, and one that is limited to PRS. Many issues in this area – for example the current debate around what content controls should be installed on the internet to protect children – therefore go substantially wider than our remit. And our powers are civil not criminal, so we rely on law enforcement agencies and bodies like the Child Exploitation and Online Protection Centre (CEOP) to take the lead where criminal activity, such as fraud or child abuse, takes place and also uses premium rate services.

However, we believe that we do have an important role to play, alongside other bodies and industry, in helping to protect children online. The value we can bring to the wider online child protection effort includes:

- Our expertise in how children are using PRS and other digital services and how risks to children are evolving in light of developing technologies and business models;
- Our co-operation with the PRS industry, including mobile and fixed line networks, aggregators and content providers, with whom we work closely and collaboratively to protect consumers;
- Our Code of Practice, which requires PRS providers to meet a range of consumer outcomes and is backed up by statutory enforcement powers. A unique feature of our Code is that it covers all aspects of the consumer experience, including how services are promoted to consumers, pricing transparency, harmful or inappropriate content, bill shock, invasion of privacy, the delivery and functioning of content, refunds and customer care. This means we can protect children and other consumers throughout their consumer journey. Our Code also includes specific rules relating to premium rate services aimed at children; and
- Our award-winning children and young people's education programme called PhoneBrain, which is aimed at giving children and young people the information they need to use PRS safely and which we have rolled out to schools and youth clubs nationwide.

We work closely with a range of bodies that play important roles in child protection, including the Internet Watch Foundation, law enforcement agencies, Get Safe Online and Childnet International, and also with other regulators that have relevant remits, like the Information Commissioner's Office, the Gambling Commission and the Advertising Standards Authority.

Our child protection strategy is intended to help us to take forward our efforts in this area and also to support our engagement and co-operation with the other bodies that work on these issues.

## 2. CHILDREN AS CONNECTED CONSUMERS

Their experience of using connected devices and digital services

In recent years, PhonepayPlus has built up a picture of how children interact commercially with the mobile internet, drawing on our own experience of complaints, investigations and research commissioned by us, as well as wider research and discussion about children, commercialisation and the mobile internet.

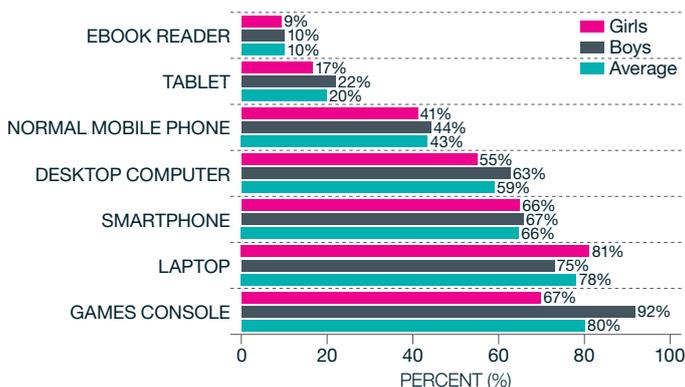
Our annual PRS market review, published last year, included in-depth research of how children use PRS and other micropayments, comprising of both quantitative and qualitative elements. The overall picture is of children who are more than ever connected to the mobile internet and to the wide range of services it offers.

### Children's ownership of connected devices

Our research showed that children increasingly have access to and use a range of connected devices to access digital content and services.

Whilst games consoles and laptops remain the most common devices, smartphones are rapidly catching up and have now overtaken desktop computers – with 66% of children surveyed saying they own smartphones for their own use, compared to 59% for desktop computers. Smartphone ownership is highest amongst those who say they also have a tablet – among tablet-owning children, 87% said they also had a smartphone. Ofcom's Children and Parents: Media Use and Attitudes Report published in late 2012 reflects a similar picture, with smartphone ownership in the 12–15 age group increasing from 41% in 2011 to 62% in 2012.

### DIGITAL DEVICE OWNERSHIP (FOR OWN USE), CHILDREN 11–16 YEARS OLD



Source, PhonepayPlus in-school quantitative survey of children 11–16 years old, December 2011. Base: 416 children

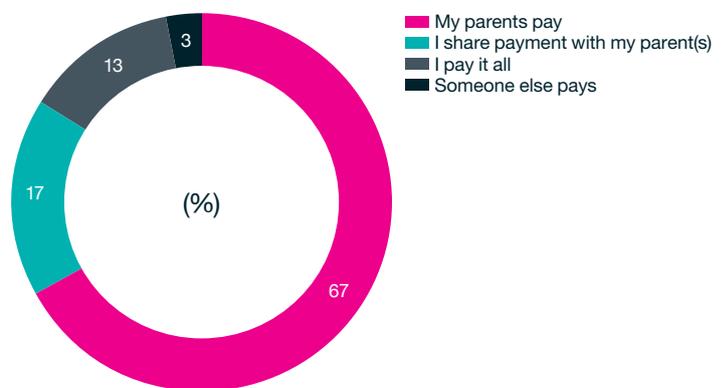
Our interviews with children suggested they see having a mobile phone as important to their freedom and independence, enabling them to be in constant contact with their friends and with what is going on. Consistent with this, the vast majority of children in our survey had BlackBerry devices, reflecting the fact that their primary use of the phone was to keep in touch with their friends via BlackBerry Messenger (alongside Facebook).

Most of the parents we interviewed said that they bought their children a mobile phone when they first went to secondary school, so that they could keep in touch with their children when they had to start travelling further from home. The parents said that they were not very concerned about how their children were using their mobile phones. Any concern shown by parents we spoke to was primarily focused more on physical risks, for example that a smartphone might attract muggers. This suggests that parents may underestimate other risks that children may be exposed to, for example sharing their personal details with strangers or running up excessive phone bills on digital content and services.

### Parental control over billing

Our survey suggested that most parents (67%) took responsibility for paying their child's phone bills. This rose to 72% for children owning smartphones.

### WHO PAYS FOR YOUR MOBILE BILL OR PAY-AS-YOU-GO CREDIT?



Source, PhonepayPlus in-school quantitative survey of children 11–16 years old, December 2011. Base: 416 children who have mobile phones.

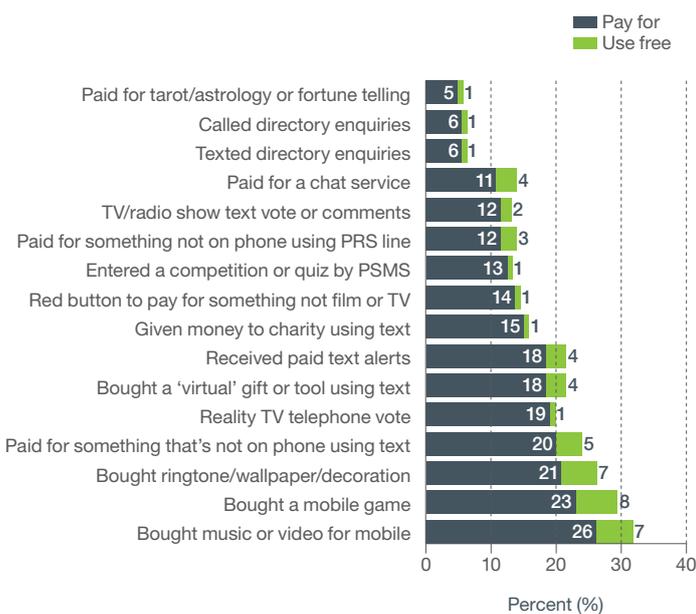
According to Ofcom research, 23% of parents do not allow their children to call premium rate lines, while 21% do not allow the use of premium texts. These figures remained more or less static between 2011 and 2012 (23% and 22% respectively). There has, however, been an increase in parents checking their child's activity on a mobile phone, with 18% of parents of 12–15 year olds now checking compared with 10% in 2011. This was also reflected in our survey. The majority of children said they would ask their parents before doing something they knew would cost money outside their regular communications contract. In some cases, this was at the discretion of the child. However, in other cases, it was within the context of rules set by their parents or through a spend limit set in their mobile contract.

Most children said that primarily they were looking first and foremost for free content – e.g. free apps in app stores. This is not particularly surprising. However, as we will outline later in this document, free services can contain hidden costs and risks that children (and their parents) may not be well aware of and should pay greater vigilance to. Seemingly free content and offers sought out and promoted on social media are an area of particular concern.

**Types of services used**

Of the mobile phone owning children in our survey, 65% said that they had used a premium rate service. Not surprisingly, the most common services purchased included downloading music or video content, buying a mobile game, buying a ringtone or wallpaper, or voting in a reality TV show. 15% indicated that they had given money to charity by text, suggesting that this relatively new giving mechanic is helping to reach people (in particular young people) who wouldn't normally give to charity through other means.

**PRS USAGE, CHILDREN 11–16 YEARS OLD**



Source, PhonepayPlus in-school quantitative survey of children 11–16 years old, December 2011. Base: 416 children

**Of the children we surveyed:**

- 12% said that they had used virtual currencies (such as PlayStation points) to make purchases;
- 31% had downloaded and paid for an app on their phone; and
- 63% had downloaded a free app on their phone.

**Children's trust in digital services**

Most of the children surveyed demonstrated some knowledge of the potential risks around using digital channels. For example, many said they took care not to click on links on sites on their mobiles. They tended to automatically trust sites from brands that they considered "well known".

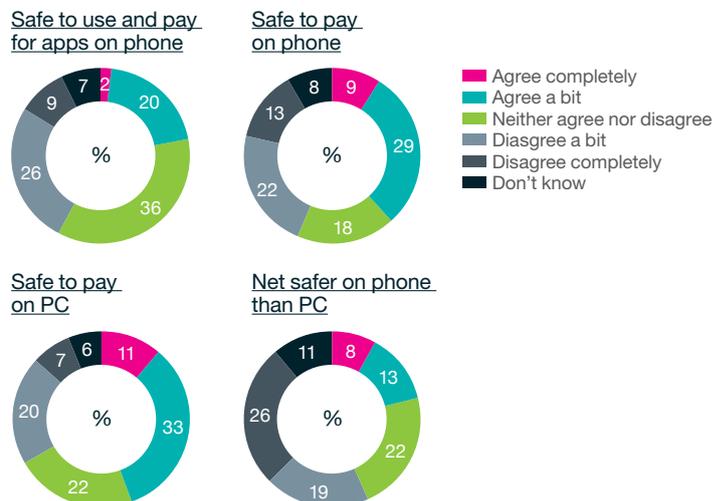
Some but not all had been taught at school about how to use the internet, but this focused on personal safety and viruses rather than on financial risks.

It was relatively common that the children felt quite confident that they knew what they were doing and how much things would cost them. Nonetheless, a significant number would at some point have a problem with being charged for something they had not expected, or with being charged more than they thought they would be.

Our qualitative and quantitative surveys highlighted the different perspectives that children can have around risk. In the qualitative survey, many children felt that the internet on their phone was safer to use than on their PC, perhaps because they have a closer relationship with their phone and this breeds greater trust. They also tended to be completely comfortable with downloading apps, on the basis that they assumed that major brands such as BlackBerry app store would be safe because it was a big brand.

However, the quantitative survey suggested a different view, with children more evenly split about whether the mobile internet was safer than the PC and about whether it was safe to use and pay for apps on their phone.

**PERCEPTION OF SAFETY – MOBILE VS. PC**



Source, PhonepayPlus in-school quantitative survey of children 11–16 years old, December 2011. Base: 416 children with mobile phones.

### 3. POTENTIAL RISKS TO CHILDREN

#### Assessing the risks to children who connect as consumers

As stated earlier, it is important to remember that PRS and other digital services can bring social, educational and entertainment benefits to children and that most children have a safe and enjoyable experience when using these services.

At the same time, we need to bear in mind that children's activity online can also expose them to risks. Many of these risks are already familiar from the PC environment.

However, in some respects the mobile internet can pose even greater challenges for child protection than the PC environment. Two points of difference in particular stand out which both make the mobile internet more practical, but also potentially more risky, to children:

- **Children using the mobile internet are less easily supervised by their parents than when they are at home using a PC; and**
- **Unlike the PC, the phone is a payment mechanism as well as a computer, so children are able not only to access services on their phone, they can pay for them – in contrast on a PC they will typically need access to their parents' credit card or other payment account to make purchases.**

We also need to consider that children's use of smartphones is happening in an environment that is becoming increasingly commercialised for young people.

#### [Commercialisation, children and digital content](#)

The rise in children's use and ownership of smartphones and other connected devices has occurred in the wider context of an increasingly commercialised culture, which the Bailey Review (Letting Children be Children, Report of an Independent Review of the Commercialisation and Sexualisation of Childhood) describes as the "wallpaper of children's lives".

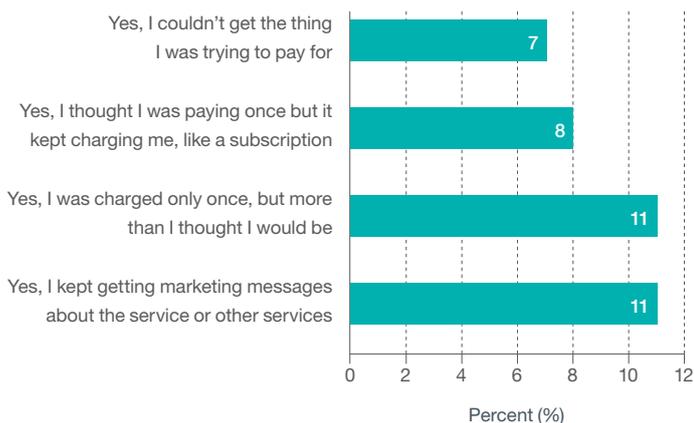
The Bailey Review, published in June 2011, found that "children are under pressure from a range of sources to act as consumers". The Review explicitly states that the aim should not be to cut children off from the commercial world but rather parents should be empowered to manage the issues for themselves supported by appropriate regulation.

However, the Review also identifies new digital media as one of the areas that parents feel most uncertain about. While parents are fairly confident in helping their children understand advertising and marketing in the 'traditional' media (television, radio, billboards, print), the Review's qualitative research found some parents were uneasy about some of the newer marketing techniques used in digital media, such as advertising by phone or text, the use of 'Like' or 'Favourite' buttons on websites, or internet advertising generally. This distrust and unease around mobile phones, advertising and children's commercial activity is reflected in the findings of the Bailey Review's omnibus survey. In the TNS Omnibus survey for the Review, the marketing and advertising tool that most parents thought should not be used to promote products to children was advertisements sent to mobile phones (35%).

### Children's experience of harm using premium rate services

In our survey of children, 27% said that they had had some problems with the PRS services they had used; 69% said they had had no problems. For those who had problems, the most common issues were unwanted marketing messages and over-charging. From an analysis of our own complaint data, the number one issue parents complain about is unexpectedly high-bills or 'bill shock'.

#### PROBLEMS WITH PRS



Source, PhonpayPlus in-school quantitative survey of children 11–16 years old, December 2011. Base: 272 PRS users.

The key risks we have identified for children using PRS and other digital services are:

- Risks arising through social media, where children's trust in social networks can make them vulnerable to unscrupulous and misleading promotions;
- The risk of being confused by less transparent pricing models, such as virtual currencies, in-app billing and hidden subscription services;
- The risk of being targeted by malware – malicious coding on apps that can charge you or access your data without your consent; and
- The risk of accessing services or content that are inappropriate for their age.

### Risks arising through social media

As social networking develops, the opportunities to promote and monetise digital content have expanded. The target audience for such content and promotion includes children as well as adults. Ofcom's report into children's media use shows that one in five 8–11 year olds have a social media profile, with that figure rising significantly to four in five in the 12–15 age group. These young people are prolific social media users, with the average number of listed friends for a 12–15 year old being 286. The potential for children to engage with paid-for digital content via social media promotion is considerable. The consumer survey for PhonpayPlus' 2010 market review revealed that 9.1% of survey respondents had purchased one or more items of digital content via their mobile phone whilst accessing a social network. While 25–34 year olds were likeliest to do this, they were closely followed by 11–15 year olds and 18–24 year olds.

There are three main potential risks we have identified for children when using PRS or other digital micropayments on social networks:

- A risk that children may purchase PRS services without realising the cost, especially when they are encouraged to do so by their friends without proper pricing information (for example, voting in PRS competitions that are promoted virally on social networks);
- A risk that children may be tricked into handing over phone credits or personal information by people posing on social networks as friends, when they are not who they appear to be; and
- A risk that children will be misled into purchasing PRS through misleading digital promotions run by affiliate marketers. In the last year, PhonpayPlus has seen a significant increase in this type of harm. Between the last six months of 2011 and the first six months of 2012, PhonpayPlus saw a 474% increase in consumer complaints about premium rate quizzes and competitions, many of which had been promoted using affiliate marketers.

These risks and the need for parents to understand their children's activity on social networking sites have been highlighted in two recent cases that PhonpayPlus has adjudicated on (please see opposite).

## SOCIAL MEDIA CASE STUDIES

### CASE STUDY 1

Trading on trust? Children as connected consumers on social networking sites – Gangster Paradise

Gangster Paradise is an online game in which codes for digital items can be bought and sold. Young people were targeted to pay for and send these codes to 'friends' on social networks. The below transcript of a mother's complaint to us is indicative of how children's trust can be abused via social media.

*"Apparently her 'friend' contacted her on a chat service and said that she had no phone credit and her grandmother was dying and needed to make a phone call. She was told to text the shortcode and give the 'friend' a code to make the phone call possible. Apparently the 'friend's' account had been hacked"*

Mother of 14 year-old girl who was billed £31

PhonepayPlus fined the Gangster Paradise provider £65,000 for failing to put in place mechanisms that could have prevented rogue users promoting and misusing the game in this way.

### CASE STUDY 2

Trading on trust? Children as connected consumers on social networking sites – Rogue promoters on Facebook

Amazecell Limited employed affiliate marketers to promote their premium rate competitions online. These promotions took advantage of social networkers' trust in what their social media friends 'share' or 'like' on sites such as Facebook. Consumers would see that their friends had 'shared' a particular promotion.

These promotions included the promise of a voucher worth up to £175 for major retailers, including Tesco and Asda. In some cases, misleading content was automatically posted onto consumers' Facebook walls without their knowledge. In other cases, to take part in the competition the consumer was required to also 'share' the promotions, which would appear on their personal wall. In this way, the promotions traded on users' trust in each other to spread virally through various social networks.

After clicking on the promotion consumers were misled into participating in premium rate competitions.

Following an investigation, PhonepayPlus fined Amazecell Limited £300,000.

Children were attracted to the Amazecell promotions, with 1 in 7 complaints involving children. The youngest affected was 11 years old, with children affected being typically aged between 12–14 years old.

The following excerpt from a parent's complaint illustrates how young people can be misled by social media promotions, even when there is a significant sense of trust and shared responsibility between children and parents:

*"My daughter has not received anything from this company... we have no knowledge of agreeing to or using this service. Her itemised bill shows a charge... this has flagged up as it is the only charge outside her monthly allocation. She does not exceed her limit... I am requesting a refund as it has been charged without my authority".*

Such cases also highlight the need for parents to give careful consideration to the age at which children become active on social networking sites and how they educate their children about how they use social networking sites, including what they spend and consume via these sites.

It is important to stress that these risks are not caused by social networks and nor are they unique to them – for example, we have seen harm posed by misleading affiliate marketing occurring in other environments as well.

Nonetheless, there are certain factors that make social networks a potentially high-risk environment for these sorts of harm to children. One is the increasing use of social media as a channel for promoting PRS. Last year's annual market review showed that 23% of PRS users we surveyed came across the service through social media, compared to only 4.3% of PRS users in the previous year.

Social networks aim to provide a familiar and trusted environment for their users. This is a key ingredient of their success, but can also leave children vulnerable to promotions or other contacts that may be misleading and trade on their trust – bearing in mind that children often lack the maturity and knowledge to identify risks in an online environment where they feel safe talking to friends.

Particular concerns arise where promotions manipulate the use of 'like' and 'share' buttons, so that children (or other consumers) are encouraged to purchase services in the belief that they have been recommended by their friends, when in fact this is not the case.

Clearly, social networks are aware of these risks and generally have policies and procedures in place that are designed to address them. We believe it is important that social networks work closely with regulators, such as ourselves, and other bodies to help protect consumers – and in particular vulnerable consumers – using their networks. We have recently put in place a framework for co-operation with Facebook in addressing these issues and we are looking to extend this to other social networking sites.

### Risks posed by less transparent pricing models

#### Virtual currencies

Whilst only 12% of children surveyed had used virtual currencies (for example PlayStation points or Smurfberries), 24% of those said that they had "no idea" how much real money they were spending and 18% said they were "a bit uncertain". Virtual currencies can carry particular risks for children if conversion rates are unclear, if pricing in real currency isn't displayed alongside the virtual currency and if the branding and promotion of the virtual currency makes it appear less like real money to children (this can be influenced for example by what the virtual currency is called).

#### In-app billing

In-app billing is a means by which apps can be downloaded and used for free, but then purchases can be made within the app, for example to get extra levels of service or functionality. In-app billing is becoming an increasingly popular form of monetising apps. Research by Distimo suggests that about 21% of all free games in Apple's app store feature in-app purchases, but when looking at the 300 most popular free applications in each category in the United States in June 2012, 77% of those games feature in-app purchases.

In-app purchasing environments are likely to be particularly attractive to children: firstly, because they are increasingly common in games that are either marketed at or popular with children; and secondly, because (as indicated earlier) children are drawn to free content and services. Therefore, the initial attraction of the app being free to download and use may draw children in, without them realising that they will be charged if they buy additional content or capabilities within the game. Risks around in-app billing may be a driver behind the significant rise in complaints about children's use of apps that we have received in the past year – complaints to PhonepayPlus related to children and mobile apps increased 300% from 2010/11 to 2011/12.

#### Subscription services

Services that sign children up to subscriptions without them realising it or knowing how to exit the service can be a major cause of bill shock. Our children's survey suggested that 8% of children who had had problems with PRS had expected to pay once for a service but had been charged on an ongoing basis. This issue can be tackled through a combination of consumer literacy campaigns where the regulator and industry work to help consumers of all ages understand the importance of reading information about a service before they engage with it. In a 'spoof' banner advertisement campaign run by PhonepayPlus and Get Safe Online in 2012, 72% of consumers who engaged with the promotion did not read the terms and conditions before inputting their phone number. At the same time, PhonepayPlus is committed to enforcing rules in its Code of Practice related to clear pricing, particularly where vulnerable consumers such as children are concerned.

#### Risks from malware

Malware involves the insertion of malicious coding into computer programmes or applications. This can result in 'trojanised' apps that may appear totally normal to consumers, but are, for example, programmed to dial premium rate numbers from the consumer's handset without their knowledge or consent. Malware has been around in the PC environment for a number of years. PRS malware in the mobile environment is relatively new and is still small in scale compared to malware on PCs. However, the rapid development and penetration of smartphones clearly creates opportunities for malware on mobiles to become more prevalent. The House of Commons Science and Technology Select Committee's recent report on malware and cybercrime states that while approximately one in three adults use a smartphone, "there is a distinct lack of understanding around related security issues". The report also noted that there was an 85% increase in malware detections on one platform in the first six months of 2011.

In the last year, we have worked together with the PRS industry and mobile networks to take robust action against the growing threat of malware on smartphones that fraudulently charge consumers via PRS.

We have identified several mobile malware attacks active in the UK market, most of which were propagated through free to download applications. As described in PhoneyPayPlus' research into children's engagement with PRS using connected devices (see section two above), many children actively seek out free applications and digital content. But this can come at a cost.

### Risks from inappropriate content

The PRS industry, which originated in fixed line adult entertainment chat lines, is well practised in dealing with the risk of children accessing adult content and services. Network operators have a range of options available allowing users (or bill payers) to bar access on phones to adult content or services, or more generally to premium rate services.

PhoneyPayPlus' Code of Practice and guidance to industry also puts in place a number of controls around access to adult content and services. Providers of adult services are required to age verify users and immediately terminate a service should an operator suspect a user is under-age. Providers of children's services are additionally required to ensure that all promotions of their services are age appropriate.

These industry and regulatory controls have generally been effective in preventing children and young people from accessing adult content and services when using PRS. However, we have to be mindful that these controls alone cannot prevent all risks.

Some children or young people may be tempted to try to circumvent age verification controls on adult services. More generally, as smartphones give children ever wider access to the mobile internet, there is a risk that even if they don't access adult services, they may come across general content or promotions (not necessarily related to PRS services) that may not be appropriate to their age. A number of children in our survey said that they had experienced this when browsing the internet, in particular when looking for free services that are more likely to rely on banner promotions to make money.

We think that the education of children, and importantly of their parents, in how to use the internet safely is essential to help manage these risks. This issue goes well beyond our remit, and bodies like Get Safe Online and Childnet International have an important role to play here. Within our remit (and as set out later in this document), we will be putting a strong focus on continuing to educate children and their parents about how to use PRS safely and in doing so, we will work closely with other bodies who have an interest in this area.

As detailed above, PhoneyPayPlus has in place a number of regulations that help to protect children using PRS, as well as a range of activities and programmes to educate children and inform parents. In the next section we explain what we do to protect and empower children as well as engage with parents.

## CASE STUDY 3

### Children, free apps and malware – RuFraud

Fake apps of popular brands including Angry Birds, Assassin's Creed and Cut the Rope were posted to Android app stores. These fake apps were advertised as free but contained malicious coding (malware) that charged the phone's account £15 every time the app was opened (usually charged through three £5 premium rate texts). The malware suppressed the sent and received text messages that notify users they have been charged. It was only when consumers received their bill that they were alerted to the fraudulent charges.

PhoneyPayPlus investigated and took action against the provider who had control of, and responsibility for, the premium rate payment system which enabled the malware to fraudulently charge consumers' mobile phone accounts. This provider was issued a fine of £50,000, and ordered to make refunds directly to ALL consumers within three months, whether or not they had complained.

Several complaints to PhoneyPayPlus involved children aged upwards from 11 years old. The following transcript of a father's complaint is typical of parents' experience of this malicious app downloaded to their child's smartphone.

*"I checked the bill on my son's phone and discovered that yesterday there were 3 instances of an outgoing text charged at 10p followed by an incoming text charged at £5, total cost £15.30. All texts were generated within a few seconds of each other and none of the texts appear in the text messages on the phone so I believe they have been generated by an application on the phone. . . this is obviously a scam of some sort due to the hidden nature of the texts."*

## 4. PROTECTING AND EMPOWERING CHILDREN AND PARENTS

### PhonepayPlus – what we do to protect and empower children and parents

PhonepayPlus has a number of effective measures in place that help to protect children and to empower them when they engage in the digital marketplace. These measures include:

#### *Code of Practice*

Our Code of Practice, which all PRS providers in the UK market must abide by, has several stipulations in relation to children. These rules are supported by robust sanctioning powers under the Communications Act 2003 and an effective investigations and adjudications procedure. In general, our Code requires that PRS must not take advantage of vulnerable consumers. Where services are specifically aimed at children, or are likely to be attractive to them, the benchmark test our Code applies is what a reasonable parent would think is appropriate for their child to see or hear. The Code also includes rules relating to age verification and spending caps.

#### *Enforcement*

PhonepayPlus is proactive in enforcing the Code of Practice and has a range of procedures by which it resolves issues involving consumer harm. The most serious of these is a formal investigation that is then adjudicated on by an independent Tribunal. The Tribunal can impose sanctions of £250,000 per breach of our Code of Practice, prevent services from operating and bar named directors from involvement in the UK PRS market for up to five years. The vulnerability of the consumers involved in the harm is a consideration for the Tribunal when imposing sanctions.

#### *Policy*

Our enforcement under the Code of Practice is supported by guidance and advice to industry, particularly in relation to developments in the market and best practice. While the Code rules in relation to children have proven robust, we look to supplement these with guidance on issues where the market is developing in a way that may pose risks to children and other consumers. A good example of this is the guidance we issued on in-app billing in February 2012.

#### *Research and intelligence*

Analysis of our complaint data helps us to understand where children are vulnerable in their use of PRS. As reported elsewhere in this document we have carried out research specifically into children's use of PRS as a digital micropayment. We have a team dedicated to tracking market developments so that we can prevent and pre-empt bad practice that can lead to consumer harm, particularly in relation to vulnerable groups such as children.

#### *Industry collaboration*

We work closely with the PRS industry we regulate and the wider telecoms industry to understand the risks to consumers, particularly vulnerable groups such as children, and take joint action to limit these risks. PhonepayPlus' Industry Liaison Panel (ILP) brings the regulator and industry together to address issues in the market, including discussions of consumer complaint data, with the ILP's Futures Group working to understand and take action on emerging risks such as malware. PhonepayPlus regularly contributes advice for parents to best practice industry publications, such as Vodafone's Digital Parenting magazine. We want to develop such positive relationships with all mobile networks and their consumer literacy teams to ensure parents and young people have clear information about digital micropayments such as PRS.

#### *Educating and engaging*

PhonepayPlus runs an award-winning programme for young people, PhoneBrain, in schools and youth clubs nationwide (see box opposite for further details). Our Consumer Literacy Working Group brings together industry and consumer experts to advise on how we educate and engage consumers in relation to PRS use.

#### *Cross-agency working*

We work and share information with a number of agencies interested in the protection of children and in their digital engagement, including the Internet Watch Foundation, Get Safe Online, Childnet International and other regulators.

## CASE STUDY 4

### Empowering children as connected consumers – PhoneBrain

PhoneBrain is a free-to-participate, award-winning national education programme. PhoneBrain equips young people with the knowledge and skills to use services they pay for with their phone bill or pay-as-you-go account confidently and safely. Launched three years ago, PhoneBrain delivers a programme of learning resources, an interactive website and a nationwide competition.

PhoneBrain offers curriculum lesson plans supporting the teaching of business and enterprise, ICT and PSHE skills. These include video resources to help teachers in their classrooms.

The resources are also adapted for extra-curricular learning too. Through a partnership with Clubs for Young People, PhoneBrain works with youth clubs up and down the country, reaching out to over 3,500 youth clubs.

PhoneBrain encourages young people to be confident in engaging with phone technology and recognise the opportunities involved. In the PhoneBrain Awards, entrants submit an idea for a phone-paid service. Working together with a range of partners, Award prizes include business and technical mentoring as well as cash investment to help young people further develop their ideas.

### What next?

PhonepayPlus believes it has a robust regulatory system in place to protect and empower children and that its partnership work helps to pre-empt and prevent harm to children using PRS. However, we also believe that in a fast-moving technology sector and with the development and increased consumer uptake of the mobile internet, we cannot be complacent in what we do to protect children as connected consumers. In the next section, we lay out our priorities for protecting children in the next year.

## 5. STRATEGIC PRIORITIES

### Children as connected consumers

Consistent with the risks we have identified concerning children (as set out in section three earlier), we have identified the following areas that we intend to prioritise as we take forward our child protection work over the next year.

#### **Strategic area 1:**

##### *Misleading promotions on social media*

PhonepayPlus has seen a growing number of cases where children have been misled into engaging with services and suffered financial detriment because of misleading promotions in the digital marketplace, particularly on social media.

PhonepayPlus recognises the potential of such harm to grow through the increased use by children of both social media and connected devices, and we are committed to working with providers and with social networks to prevent such harm.

*Over the next year we will:*

- **Consult on and issue industry guidance on the digital marketing of PRS, with a focus on social media and on potential harm to young people and how these risks should be mitigated and avoided;**
- **Work with Facebook and other social media providers such as Twitter to cut off rogue promotions and misleading affiliate marketing as quickly as possible – PhonepayPlus has started to work productively in this area with Facebook and we will continue to actively seek and encourage such collaboration with social media providers;**
- **Work with social media providers such as Facebook on information initiatives aimed at younger social media users that help them make informed choices about their commercial activity on social media sites; and**
- **Continue to take effective enforcement action where appropriate.**

#### **Strategic area 2**

##### *Keeping pace with the evolution of the digital market*

As the digital market evolves, we believe that many of the risks we have seen emerge in the delivery and promotion of PRS may migrate to the wider digital market. This reflects the fact that PRS is now increasingly just one of a range of different micropayments that can be used to purchase digital content and services; and that in our view, the digital micropayments market has certain characteristics that, if uncorrected, may give rise to a propensity for consumer harm. We set out these concerns in a recent submission to the DCMS on the Communications Review.

We believe it is necessary to put in place future-proofed protection for children in this converged market, where the potential risks and harms we have seen in children's use of PRS is likely to be replicated by other digital micropayments. We also remain committed to addressing areas in the digital marketplace within our remit where we have seen that children can be particularly vulnerable, such as in-app billing and malware.

*Over the next year we will:*

- **Work with Government, industry and other regulators in considering how the regulatory system should evolve to keep pace with changes in the digital market and with emerging risks to consumers, including children;**
- **Conduct a review into developments in the apps market and consider whether further guidance is needed to help protect consumers using apps charged to phone bills;**
- **Work with industry, security experts and law enforcement agencies to pre-empt the threat of mobile malware. This will include addressing risks around 'free' passed-off apps, which are particularly attractive to children; and**
- **Continue to take effective enforcement action where appropriate.**

### Strategic area 3

#### *Empowering and informing*

PhonepayPlus believes that prevention should always be a priority for an effective regulator and that we have a responsibility to give consumers the knowledge and advice that empowers them to make informed choices about their use of PRS. More and more, these consumers include parents and children. PhonepayPlus recognises that parents are key in guiding and controlling children in their use of connected devices and we are committed to disseminating clear, simple, useful and effective messages to parents that will help them to guide and advise their children.

*Over the next year we will:*

- **Increase the participation of young people in PhoneBrain, our award-winning programme for schools and youth clubs;**
- **Develop our partnerships with Get Safe Online, Childnet International, Citizens Advice, Money Advice Service and other bodies to ensure that our information and advice about using PRS reaches a wider audience of consumers, including parents and children; and**
- **Work with industry to continue to improve customer care, so that PRS users are able to obtain speedy redress, where appropriate, when problems arise.**

### Input

We would welcome any input from interested parties in the analysis and priorities we have set out in this document. And we would be keen to hear from any other bodies which we could co-operate with in taking forward these actions.



PhonepayPlus  
Clove Building  
4 Maguire Street  
London  
SE1 2NQ

+44 (0) 20 7940 7474  
[www.phonepayplus.org.uk](http://www.phonepayplus.org.uk)