GENERAL GUIDANCE NOTE

Consent to Charge

Who should read this?
All network operators and providers involved in the provision of premium rate services to consumers.

What is the purpose of the Guidance?
To assist networks and providers by clarifying the Phone-paid Services Authority's expectations by way of the fulfilling the following Rules of the Phone-paid Services Authority's Code of Practice:

2.3.3

Consumers must not be charged for premium rate services without their consent. Level 2 providers must be able to provide evidence which establishes that consent.

and where relevant to achieving the aim of rule 2.3.3, the following Rules contained within Part 3 of the Code:

3.1.1

Network operators, Level 1 and Level 2 providers must ensure that PSA regulation is satisfactorily maintained by:

Taking all reasonable steps in the context of their roles, including the adoption and maintenance of internal arrangements to ensure that the rules set out in Part Two are complied with and the outcomes achieved in respect of all PRS with which they are concerned, and

Carrying out their own obligations under the Code promptly and effectively, and

Taking all reasonable steps to prevent the evasion of, and not to undermine, the regulation of PRS,

3.1.3

Network operators, Level 1 and Level 2 providers must assess the potential risks posed by any party with which they contract in respect of:

The provision of PRS, and

The promotion, marketing and content of the PRS which they provide or facilitate

and take and maintain reasonable continuing steps to control those risks.

3.1.6

Network operators, Level 1 and Level 2 providers must carry out reasonable monitoring of PRS provided by any Level 1 or Level 2 provider with which they have contracted.

3.1.7

Network operators, Level 1 and Level 2 providers must use all reasonable endeavours in the context of their roles to ensure that all of the PRS with which they are involved are of adequate technical quality, including the mechanisms used to deliver services to an to enable exit from services by consumers.

What are the key points?

This Guidance covers the following areas:

- Why informed and robust consent is important
- Expectations around informed consent and consumer purchase journeys
- Expectations around robust payment and verification platforms

1. Why informed and robust consent is important

1.1 Phone-paid services allow a charge to be generated to a consumer's phone bill. This facility is available whether the phone is pre-paid/Pay as you Go, (where the charge would then be taken from credit already added to the phone), or post-paid, (where the charge would be added to the bill which the consumer pays as part of a fixed-term contract with a network).

1.2 Ensuring consumers are only charged when they have requested or consented to a purchase is of critical importance to the PSA, and past examples of such incidents have led us to previously put in place a specific Code provision and accompanying Guidance. Any charging without the consumer's informed and auditable consent can lead to individual financial detriment and have a wider effect on consumer trust in phone payment as a mechanic. Any lack of trust can reduce consumer engagement with phone payment in the future, and in turn lessen opportunities for market growth and development.

1.3 For these reasons, it is essential that providers at all stages of the value chain can supply robust, auditable records of informed consumer consent for every charge that is applied to a phone bill.

What is informed and robust consent?

1.4 Informed consent refers to consumer consent given only when the consumer has all the key information they would need to make a decision as to whether to purchase or not. If it can be demonstrated via tamper-proof, independently and easily auditable records, that a consumer has seen:

- clear and legible pricing
- service information (a clear explanation of what the service is)
- charging frequency (such as whether the charge is a recurring subscription or a one-off)
- any other relevant information (such as free trial periods)
- an absence of any misleading information or inferences

then the PSA would generally regard the consumer's consent as having been informed.

1.5 Robust consent refers to consumer consent to a transaction, which can be properly audited in such a way as to prove that the consent could not have been given in any other way than by the consumer's specific actions. Robust consent can be proven through the following:

- in the case of calls to voice-based services, records which clearly set out the date, time and number which was called, and the consumer's number
- in the case of text messages sent by a consumer to purchase services which are promoted in print, on television, on websites, or other forms of advertising, records which clearly set out the date and time when the consumer sent the text, and their phone number, and also identifies the mobile shortcode to which the text was sent, and

the dates and times when that shortcode received the consumers' message, and any other relevant messages the shortcode then sent in reply

- in the case of purchases initiated via websites, records which clearly set out the dates, web addresses (including genuine x-header requests) and exact times when (and where) a consumer purchased, and also record the pricing and other key information that the consumer saw on the relevant website at the time that they initiated and confirmed that purchase. For purchases resulting in a charge to a mobile phone bill records should also include the consumer's device and mobile network.

In all three cases above, creation and storage of such records in a way that is clear, and ensures they are independently and easily auditable (including by the PSA), and demonstrably tamper-proof once they have been created. Providers should be aware that a PSA Tribunal is unlikely to deem as sufficient records that have been exported from a database and only then supplied as being demonstrably tamper-proof.

2. Expectations around robust consent and consumer purchase journeys

2.1 Expectations will vary according to the type of phone-paid service being purchased. For example, a voice call will have different expectations to a digital purchase which is initiated on a website and charged to the phone bill. This section sets out guidance on PSA expectations in relation to the following purchase initiation routes:

- calls to voice-based premium rate numbers
- text messages sent to a mobile shortcode
- entry of a consumer's mobile number into a website
- where the consumer is using a wi-fi connection
- where the consumer is using their network to connect to the internet
- charges incurred each time the consumer views a new webpage, image or video on a website.

Calls to voice-based premium rate numbers

2.2 In the case of calls to non-geographic numbers used for phone-paid services under PSA's remit (such as 118, 09, 087, or 084 in limited cases) or to voice shortcodes, robust verification can take the form of an originating Network operator's record of the consumer's initiation of the call.

2.3 UK networks put in place technical safeguards so that no charge can take place for a voice call until a consumer has dialled a number, and either picked up a receiver or pressed a call button on their phone. In addition, charging consumers to receive a call is generally prohibited by all consumer-facing networks in the UK (with the exception of "reverse charge" calls to a local or national number where the reversal is accepted by the called party).

2.4 Overcoming the technical barriers which networks have put in place would be extremely challenging for any rogue provider, at any other point within a value chain of a service which is charged using a premium rate voice call. As such in cases where a consumer disputes such a charge we will generally accept that the charge was valid, if the originating network provides their record of the call. This relies on all other circumstances being equal, and there being no other evidence which would lead us to investigate further. This does not imply that the consumer's consent was necessarily informed – i.e. the promotion may have been inadequate or misleading – and in such cases we will investigate this as a separate consideration where necessary.

Text messages sent to a mobile shortcode

2.5 Where a consumer sends a message to a mobile shortcode promoted in print, on television, or even on a website – for example, to donate to charity, or to vote or enter a competition in relation to a TV show – the message is known as a Mobile Origination (MO) message. Because this message has been initiated by the consumer, we will generally accept the mobile network's record of the message being sent as robust consent.

2.6 This is subject to two other factors. The first is that any promotional material the consumer sees before they send the MO message complies with the Code. For more information on PSA's expectations around clarity and key information in promotional material, please see our Guidance on Promoting Premium Rate Services. The second is that in extremely rare occurrences a consumer's mobile handset may have been infected with malware which initiates an MO message without the consumer's knowledge, such messages often being sent at times when the consumer would be expected to be asleep. In circumstances where the PSA has reason to believe that a handset may be infected in this way, or that an MO message has been generated in a different way without the consumer's knowledge, we may conduct further enquiries on a case-by-case basis.

Entry of a consumer's mobile number into a website – where the consumer is using wi-fi

2.7 Some phone-paid service charges are initiated by a consumer entering a mobile number on a website. They may be browsing the website via their desktop PC, laptop, tablet, or mobile handset. Consumers do not always appreciate that entering their number in this way can initiate a purchase which carries a charge to their mobile bill.

2.8 The risk of harm is further increased if a consumer enters a mobile number belonging to someone else (either by mistake or deliberately), which could lead to a second – unwitting – consumer being charged.

2.9 Generally a consumer enters their mobile number into a field on the website, which initiates a Mobile Termination (MT) message from the service provider to their handset. Where a provider wishes to use this process, the PSA's expectations are as follows[1]:

All key information, including cost and charging frequency (where the service carries a recurring charge), and the fact that the consumer will be charged to their mobile phone bill, should be clearly and prominently stated, and be proximate to the field where the consumer has to enter their number.

Providers should make it clear to the consumer what the service is and who is providing it.

After a number has been entered, a free MT message must be sent to the related handset containing a PIN. We recommend the PIN is alphanumeric and contains no less than four truly random[2] digits. The message should contain the PIN, the service name, the cost and frequency of charging, and that the PIN should be deleted if received in error. Other than this, the MT message should not contain any other content, and especially not content which could act as instructions for a consumer who had not previously visited the relevant website.

Instructions on the website should make clear that the consumer has to enter the PIN which they received within the MT message into a second field, which should be located beneath the first field where the consumer entered their number. Once the PIN is entered the consumer should be required to click on a confirmation button, where pricing and frequency of charge information are prominent and proximate to, or contained on, the button.

If the PIN entered matches the PIN which was sent by MT message to the consumer, then provided the platform on which this reconciliation has taken place is robust (see section 3 of the Guidance below), the PSA would ordinarily consider this to evidence of consent to a charge provided the platform on which this reconciliation has taken place is robust and providing there is no other evidence that would require us to investigate further.

Any PIN sent to a consumer via an MT message should expire if after three attempts the consumer has not entered it correctly. In any event, a PIN should also expire within a reasonable time of being sent, and any purchase which has not been completed should be shut down and erased from the provider's records. Evidence of all PIN entry attempts, whether successful or not, should be recorded.

2.10 Some websites which promote phone-paid services invite the consumer to enter their number, and then send them an MT message containing a keyword. The consumer must then text a reply containing the keyword in order to consent to a charge. Where this is the case, we would expect that the message also contains the service name (and brand where different), and the cost and frequency of charging, in such a way as to make clear to the consumer that

---

[1] Providers should note that Subscription Services, Recurring Donations, Society Lotteries, Pay Per View Services, and Adult Services and Competition Services which are principally discovered online, are subject to Special conditions regimes and must comply with the conditions within these regimes. The expectations at paragraph 2.9 take account of relevant conditions within those regimes.

[2] "Truly random" can be defined in this case as an algorithm which is able to generate sequences of numbers whose properties approximate the properties of random numbers, and where new sequences are not predictable from earlier outputs.

replying with the keyword will result in a charge.

Entry of a consumer's mobile number into a website – where the consumer is using their network IP

2.11 Where a consumer uses their mobile network's internet provision (IP) to visit websites, then the mobile network is able to match their activity to their mobile number. In this way, the mobile network can independently verify any consent to a phone-paid charge.

2.12 Where a consumer uses their IP, an encrypted version of their mobile number can be passed through to the payment platform of the website where the consumer is browsing. In these circumstances, the PSA would not consider it necessary for a consumer purchasing a phone-paid service to enter their mobile number (and trigger a PIN as above), provided that the following was also true[3]:

- any phone-payment platform to which the website is directly or indirectly linked controls the display of web pages which contain payment consent buttons
- the point of purchase is clearly signposted, and distinctive from other aspects of the service (for example, by design and colour)

Consumers should initiate a purchase by clicking a consent button on a first screen, and then confirm the purchase by clicking a further consent button on a second, separate screen. The first screen should contain such wording that requires the consumer to acknowledge that the purchase implies an obligation to pay, and that the charge will be added to their mobile phone bill. The second screen should contain prominent pricing (and frequency of charge information where relevant), either proximate to the confirmation button or on it.

- the payment platform is robust (see section 3 of the Guidance below).

2.13 Providers should note that even where a consumer has used their network IP to browse and purchase, they should either:

- send an MT message containing a PIN (as at para 2.9), and have the consumer enter the PIN into a field on a payment page and click a button in order to confirm the charge
  or
- use a password system, with the consumer entering a password which they have selected and controlled to first confirm their identity, and then confirming consent to payment on a second screen (as at para 2.12)
  or
- use biometric technology, such as fingerprint or facial recognition, to confirm a purchase once the consumer has initiated it on a first screen (as at para 2.12).

[3] Providers should note that Subscription Services, and Adult and Competition Services which are principally discovered online, are subject to Special conditions regimes and must comply with the conditions within these regimes. The expectations at paragraph 2.12 and 2.13 take account of relevant conditions within those regimes.

Charges incurred each time the consumer views a new webpage, image or video on a website[4]

2.14 In some circumstances, charges can be generated once consumers click on a mobile website – often to view an image or a new page. The PSA's expectation is that each charge – i.e. each time the consumer clicks on a new image or page that triggers a charge - must be subject to robust consent verification, as set out above, depending on whether the consumer's number is known to the mobile network or not when they enter the website. Consumers can give their consent to all subsequent charges when they enter the website, but they must be clearly and prominently informed, in very close proximity to the consent buttons, that this is what they are doing.

3. Expectations around robust payment and verification platforms

What are robust payment and verification platforms?

3.1 Payment and/or consent verification platforms (and related web interfaces) which are proven to have such standards in place, both technical and in terms of risk control procedures, that categorically demonstrate that any records of charging cannot have been initiated in any way other than from the informed consent of a consumer.

Types and Scope of Expectations

3.2 Expectations around a robust payment/consent platform (and related interfaces), can be split into three general categories:

- technical expectations
- staff roles and responsibilities
- risk management and control.

3.3 It is important to note that the following expectations apply to all such platforms. This includes payment/consent platforms provided by an Level 1 provider who is part of a value chain, and consent verification platforms provided by third parties (whether they sit within a value chain, or have been contracted by a Level 2 provider, Level 1 provider or network within it, or indirectly provide consent verification services to it).

Technical Expectations

3.4 In setting technical expectations for payment and consent verification platforms, the PSA has taken two considerations into account. Firstly, that it can be possible to arrive at robust proof of informed consent via different approaches to the design of a platform's

[4] Providers should note that services which charge per page or Image viewed are subject to Special conditions regimes and must comply with the conditions within these regimes.

technical architecture. However, there still exist universal standards as to the underlying software which that platform uses to operate, and the protocols with which it communicates and interfaces with web pages and other external systems. As such, the technical expectations which we set focus on these universal standards.

3.5 Secondly, that universal standards will constantly evolve. In order to prevent any expectations we set being rendered obsolete by evolving technology, we have set them out at Appendix A to this document, and will review them in conjunction with mobile network operators on an annual basis and consult on any proposed revisions.

Staff roles and responsibilities

3.6 Payment/consent platforms, no matter how carefully developed, can be compromised by bad judgement on the part of those who are responsible for them. The likelihood of bad judgement is heightened in an emergency, or when people do not have a clear idea of their responsibilities in relation to the platform and how to discharge them. In order to ensure that any risk is adequately identified, communicated, and controlled, the PSA has the following expectations around roles and responsibilities, and staff training:

All platform providers should have adequate, full-time staffing focused on security and fraud. Security staff would be expected to have the following qualifications and experience as a minimum:

- degree in computer science or related discipline, or equivalent experience
- proven ability to evaluate risks in platforms and software, and research security incidents
- good understanding of web security and internet security tools
- understanding of threat modelling.

All platform providers should have an assigned "Head of Security" or equivalent role. Where such a role is unfilled by staff departure or absence, then responsibility should shift upwards to a more senior member of staff. A head of security would be expected to have the following qualifications and experience as a minimum:

- between 5-10 years IT/web security experience
- project lead experience related to achieving ISO/IEC 27001 certification and National Cyber Security Centre (NCSC) "Cyber Essentials Plus" assurance
- demonstrable knowledge of the latest security thinking and threat modelling methods
- a proven record of dealing with complex IT platform overhaul projects.

Each platform provider should have a nominated Single Point of Contact (SPoC) for emerging security issues. This will usually be the Head of Security or equivalent role. Where the SPoC is absent, the responsibility should move to a more senior member of staff.

All providers should ensure that platform development staff are adequately trained in secure development techniques and have an adequate understanding of relevant risks and threats to at least NCSC "Cyber Essentials" level. This training should be ongoing, to take account of threat and risk evolution.

All platform development staff should build their understanding of relevant risks and threats into any development work they carry out. Providers should be able to demonstrate this is the case.

All platform or other systems development – including but not limited to new protocols for phone-payment - should have a review of functionality by the security team before they go live. The Head of Security (or equivalent), or most senior member of the security team in their absence, must have a veto over any protocols or solutions which are not secure enough, such that they cannot go live without an audited assessment and consent from the security team. An example template for recording such assessment is attached at Annex C. The use of this template is entirely voluntary; however it does set out the level of detail the PSA would expect to receive around any previous assessments which were relevant to an investigation.

Risk management and control

3.7 As well as staff who are fully aware of their roles and responsibilities, and adequately trained to discharge them, it is also important that all organisations involved in payment or consent verification have adequate processes to quickly identify, record, communicate, and control risk, and to also ensure lessons are properly learned afterwards. This can refer to an emerging issue, or to an identified risk which will need to be assessed and mitigated. The PSA has the following expectations around such processes as part of wider risk management and control:

All parties involved in phone-payment should maintain a security risk/issues register. The register should record any identified risks or issues on an ongoing basis, and set out as a minimum the following:

- an explanation of the risk or issue – in the case of an issue, the explanation should also set out exactly when and how it was discovered, and by whom
- the actions taken to mitigate/resolve the risk/issue – with a timestamped record of who has signed them off as being complete and when
- any further, ongoing actions (which can be transferred to "actions taken" as above, once they are complete and signed off)
- the individuals within the organisation responsible for ongoing actions.

All parties involved in phone payment should implement active threat monitoring measures, which can monitor systems and alert staff in real time. These measures should aggregate data from across the platform, understand traffic patterns across the platform, and provide detailed information about potential attacks or exploits. This should include, but not be limited to:

- leveraging threat intelligence from previously seen attacks
- analysing consumer behaviour – e.g. transaction logs, transaction times, user agent/device, x-header requests, associated URLs, IP addresses, time deltas between double opt-ins, repeat transactions, unfinished transactions, repeat unfinished transactions and their frequency etc.
- analysing Level 2 provider merchant behaviour – e.g. what kind of data they access and how frequently, whether apps are requesting payment pages etc.
- performing "Attacker Behaviour" analytics
- setting intruder traps – e.g. decoy network services or credentials
- conducting proactive threat hunts
- conducting "Red Team/Blue Team" penetration testing using discovered malware.

All parties involved in phone payment should act on any security alerts or flags, whether from their own monitoring or information shared by others, in a timely manner. An example template for recording security breaches, or attempted breaches, is attached at Annex C. The use of this template is entirely voluntary; however, it does set out the level of detail the PSA would expect to receive around any previous breaches or attempted breaches which were relevant to an investigation.

Each payment and/or consent verification platform must be tested by a CREST accredited third party on an annual basis. Testing should identify and score exploits according to the OWASP taxonomy and the CVSS scale. The results of these tests should be made available to all mobile network operators and provided to the PSA upon direction. Any identified exploit with a CVSS score of 4.0 or over should be fixed immediately and the platform and services that are using it (or in the case of third-party consent verification platforms, just the services that are using them) will be considered to be non-compliant[5] until the fix has been independently verified by the tester.

All Level 1 providers should ensure they have contracts in place which allow them to suspend or terminate payment facility to any Level 2 providers or third-party consent verification platforms, as soon as any non-compliant activity, such as charging of consumers without informed and robust consent, is identified or where they reasonably suspect that such fraudulent activity has or is occurring.

All mobile network operators should take effective action against Level 1 providers whose platforms repeatedly facilitate non-compliant activity, such as charging of consumers without

[5] Only platforms which are part of the value chain may be considered non-compliant under Rule 2.3.3 of the Code – i.e. the requirement to have and provide upon request robust, auditable consent – and requirements at Part 3.1 of the Code for adequate risk control and technical quality. Third party verification platforms are not part of the value chain, and therefore not registered parties with us. However, any services using a platform which does not comply may be considered non-compliant under Rule 2.3.3 of the Code.

consent or where they reasonably suspect this to be the case. This should include clear, documented consideration of whether Level 1 providers should be suspended or have their contracts terminated in relation to more serious incidents and clearly documented consideration of whether a sequence of incidents warrant suspension or contract termination. Mobile network operators should have contracts in place which permit them to conduct further random CREST-accredited testing at any time on any Level 1 provider payment platform, and to document any findings, and when and how improvements are made as a result of them.

More generally mobile network operators should ensure they have contracts in place which allow them to suspend or terminate Level 1 providers where serious or repeated non-compliant activity is discovered. For the avoidance of doubt, we would be unlikely to consider the end of a direct contract to be a sufficient risk control measure if the Level 1 provider in question was still permitted to operate within the value chain through another Level 1 provider's platform.

3.8 Evidence of how a payment and/or consent verification platform has met the expectations at paragraphs 3.6 and 3.7 and Appendix A, should be available for immediate, independent assessment by the PSA and mobile network operators upon request.

Third party consent verification

3.9 Where a consent verification platform is operated by a third-party, who is not directly involved in the value chain, then the PSA will be unlikely to accept as compliant any payment verification which is not initiated by a Level 1 provider, with whom the third-party provider has contracted. As part of any contract between a Level 1 provider and a third-party consent verification platform, the Level 1 provider must satisfy themselves that the platform meets the standards and expectations at paragraphs 3.6 and 3.7 and Annex A. In addition, the third-party will be expected to provide data of payment records and other relevant information to mobile network operators and the PSA upon request. As at 3.7.f), mobile network operators should have in place such contracts with Level 1 providers which allow for the random testing of third-party platforms at any time and should retain the right to refuse to accept verification by any third-party platform at their discretion.

3.10 In any event, where a Level 1 provider contracts with a third-party consent platform as per paragraph 2.9, the Level 1 will remain responsible for the verification.

APPENDIX A – Technical standards

The following are a list of technical standards which the PSA expects all payment and/or consent verification platforms to have in place whilst operating any phone-payment transactions. In order to prevent depreciation of the standards as technology and attack vectors evolve, this list will be reviewed and updated with consultation as appropriate by the PSA on an annual basis:

- all platforms should be hosted strictly independently of any Level 2 provider
- all platforms should use Transport Layer Security (TLS) protocols at version TLS 1.2
- all platforms should have in place a strong Content Security Policy (CSP) to restrict resource usage
- browser Cross-site Scripting (XSS) mitigations should be enabled on all platforms by default
- HTTP Strict Transport Security (HSTS) headers should be enabled on all platforms by default
- HTTP headers should protect against clickjacking
- any phone-paid transaction should only occur over correctly validated HTTP connections
- payload protection should be implemented in order that it cannot be edited partway through a transaction
- rate limiting should be in place for login attempts, in order that “brute force” password guessing is prevented
- authentication cookies should be encrypted by default on all platforms.

Appendix B - Glossary of technical terms

Attacker Behaviour Analytics

Where web and payment platforms analyse previously known patterns of cyber-attacker behaviour and use the trends in that data to identify repeats of those attacks, or the next potential variants of those attacks.

Authentication cookies

A cookie is a small piece of data sent from a website and stored on the user's device by the user's web browser while the user is browsing. This is usually to remember information such as any items a user has added to a shopping cart, or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past). They can also be used to remember information that the user previously entered into form fields such as names, addresses, passwords, and card details or phone numbers for payment.

Authentication cookies are the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in with.

Content Security Policy – (CSP)

CSP is a computer security standard introduced to prevent various types of attacks where malicious code is injected into a trusted web page. CSP works by providing a standard method for website owners to declare approved origins of content that browsers should be allowed to load on that website. Anything which is not approved cannot be loaded.

CREST – (Council for Registered Ethical Security Testers)

CREST is an international not-for-profit accreditation and certification body that represents and supports the technical information security market. CREST provide internationally recognised accreditations for organisations, and professional level certifications for individuals providing various types of cyber-security services.

Cross-Site Scripting – (XSS)

Cross-site scripting (XSS) is a type of computer security vulnerability which typically exploits known vulnerabilities in web-based applications, their servers, or the plug-in systems in which they rely. An attacker "injects" malicious coding into the content being delivered by the web application. When the resulting "combined" content arrives at the user's web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system.

CVSS – (Common Vulnerability Scoring System)

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities, created following research by the US National Infrastructure Advisory Council in 2003/04. Vulnerabilities are rated on a scale of 1 to 10, with 10 being the most severe.

HTTP – (Hyper Text Transfer Protocol)

HTTP is the underlying protocol used by the World Wide Web, which defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.

HSTS – (HTTP Strict Transport Security)

HSTS is a web security policy mechanism that allows web servers to declare that web browsers (or other complying user agents) should interact with it using only secure (HTTPS) connections, and never via the insecure HTTP protocol. A website using HSTS must never accept clear text HTTP and either not connect over HTTP or systematically redirect users to HTTPS.

Mobile Origination message – (MO)

A text message which has been originated on, and sent from, a mobile device. These can be either free – i.e. the cost of sending the message is that of sending a standard text – or charged at a premium when the text is received by the mobile shortcode to which it was sent.

Mobile Termination message – (MT)

A text message which is received by a mobile device. These can either be free – i.e. receiving the message costs the recipient nothing – or charged at a premium when the device receives the message. In the context of phone payment, MT messages are usually generated by an Level 1 provider in response to consumer interaction with a Level 2 provider merchant. Where they are not, it may be that the message and any associated charge was unsolicited.

NCSC – (National Cyber Security Centre)

The National Cyber Security Centre is an organisation of the UK Government that provides advice and support for the public and private sector in how to avoid computer security threats. One of their products is the NCSC Cyber Security Essentials certification, a set of basic technical controls to help organisations protect themselves against common online security threats.

Cyber Essentials is backed by industry including the Federation of Small Businesses, the CBI and a number of insurance organisations which are offering incentives for businesses. From 1

October 2014, the Government requires all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

Network internet provision

An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Where a consumer uses the internet access provided by their mobile network to browse the web with their mobile device, this is known as "Network IP".

OWASP – (Open Web Security Application Project)

OWASP is a worldwide not-for-profit charitable organization focused on improving the security of software, so that individuals and organizations are able to make informed decisions. Operating as a community of like-minded professionals, OWASP issues free, open-source software tools and knowledge-based documentation on application security.

The OWASP Top 10 is a project to document the ten most critical categories of security risk to web applications. It represents a broad consensus of a variety of security experts from around the world, who share their expertise to revise the list on a regular basis.

Payload protection

In web security terms, the payload is any message sent by a user's device to a website or other web application, where that message contains, or has had added, malicious coding. Payload protection is any action or system which seeks to identify and block messages containing malware.

PIN – (Personal Identification Number)

A PIN is a numeric or alpha-numeric password used to authenticate a user so they can access a website, web application, or any other system.

Rate limiting

Rate limiting is used to control the rate of traffic sent or received by a network interface controller. In the context of phone payment, it prevents repeated attempts by an attacker to send the same message or execute the same action. A common example is the rapid, and sequential, entry of every possible four-digit PIN until the correct one is entered, thus allowing an attacker who does not know the PIN to gain access through repetition.

Red Team/Blue Team testing

Where a security function divides into two teams in order to conduct penetration testing. One, the Red Team, uses malware the team has discovered to try and execute that malware on a "sandboxed" version of the platform, with the Blue Team attempting to identify and prevent any attempts.

Threats

Known malicious indicators that appear together during specific cyber-attacks. By recording and aggregating intelligence about threats, payment platforms and web applications can identify and prevent further attacks using the same methods and look to predict what variations on previous attacks may appear next.

TLS – (Transport Layer Security)

TLS is an encryption protocol that protects data when it moves between computers or other devices. When two devices send data they agree to encrypt the information in a way they both understand. This prevents data being intercepted by a third party, or "injected" with malicious code.

Time delta

Where a user interacts with a website or web application, and in particular where they click on-screen buttons, the time delta between clicks is an important way of ascertaining whether the interaction is genuine or is potentially being carried out by a device infected with malicious code. Sometimes an infected device will "click" more rapidly than a human being could or will click on the exact same pixel within a sequence of buttons which are presented.

URL – (Uniform Resource Locator)

The formal term for a web address.

X-header request

The instruction sent by a device in order to "pull" a specific website or webpage to it and display the page so a user can browse it. In effect the X-header request ID correlates the HTTP request between a user's device and the website or web application's server.

Appendix C – Example templates for security records

Assessment of New Platform or Systems Developments

Description of the proposed update/new protocol/development				
Person (s) responsible for security assessment				
Summary of the security assessment (e.g. methodology used to assess and test)				
Pass or Fail?				
If "pass", were there any dissenting views? Please provide details	*Person(s) who dissented*	*Reasons for dissent*	*Relevant OWASP category*	
If "fail" please provide details of the reasons for failure	*Description of the identified issue/weakness/risk*		*Relevant OWASP category*	
Will the proposal be re-submitted?				
If it will, what improvement actions are required?	*Description of the action*	*Who is responsible for the action?*	*Date the action is assessed as complete*	*Who signed it off as complete?*

Record of identified security incident

Description of identified breach or attempted attack	*Breach or Attempted Attack?*	*Description*	*Relevant OWASP category*	
When and how was it identified?	*Date*	*Time*	*How was it flagged?*	*Who was the SPoC?*
Person(s) who performed the initial assessment				
Summary of the incident and the SPoC's assessment				
Was the incident reported to:				

MNOs?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*
PSA?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*
ICO?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*

What immediate actions were required?	*Summary of action*	*Who is responsible for the action?*	*When was the action completed? (date and time)*	*Who signed the action off as complete?*
What remedial actions were required?	*Summary of action*	*Who is responsible for the action?*	*When was the action completed? (date and time)*	*Who signed the action off as complete?*