GENERAL GUIDANCE NOTE

Consent to Charge and Payment Platform Security

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?

This Guidance is provided to assist networks and providers in their understanding of the relevant rules and how PSA interprets and applies them.

This Guidance should be read in conjunction with the Phone-paid Services Authority's other pieces of guidance. Specifically, the Guidance on Promoting Premium Rate Services and Guidance on Due Diligence Risk Assessment and Control:

The relevant rules

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.

Section One: informed and robust consent

What is informed consent?

1. Informed consent refers to consumer consent given only when the consumer has the key information they need to make a decision as to whether to make a purchase or not.

2. The PSA would generally regard the consumer's consent as having been informed if it can be demonstrated via genuine, easily auditable records that have not been tampered with in any way since they were created, 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 in relation to free trial periods).

What is robust consent?

3. 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 thefollowing:

   - **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, their phone number, the mobile shortcode to which the text was sent, 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 http headers) 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.

4. In all three cases above, creation and storage of such records must be clear, and able to be independently and easily auditable (including by the PSA). Providers should be able to demonstrate that such records show genuine consumer consent and have not been tampered with in any way since they were created. The provider should be able to provide PSA with raw opt-in data (i.e. access to records, not an Excel sheet of records which have been transcribed) and real-time access to this opt-in data, upon request. This may take the form of giving the PSA password-protected access to a system of opt-in records.

Why informed and robust consent is important

5. Phone-paid services allow a charge to be generated to a consumer’s phone bill.

6. Ensuring consumers are only charged when they have requested or consented to a purchase is of critical importance to the PSA. Any charging without the consumer’s informed and auditable consent can lead to financial detriment and have a wider effect on consumer trust in phone payment as a mechanism. Any lack of trust can also reduce consumer engagement with phone payment in the future. The PSA wants to support a healthy market that is innovative and competitive.

7. 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.

Section Two: Expectations around robust consent and consumer purchase journeys

8. This section sets out the PSA's 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 wifi connection or their network IP to connect to the internet
    - charges incurred each time the consumer views a new webpage, image or video on a website.

Third-party consent verification

9. Where verification is undertaken by a third party, this party should be independent of the Level 2 provider[1]. This verification should only be undertaken on behalf of the Level 1 provider. Where a Network operator contracts directly with a Level 2 provider the verification function can be undertaken by the Network operator.

10. As part of any contract between a Level 1 provider and a third-party consent verification platform, the Level 1 provider should satisfy themselves that the platform meets the standards and expectations on staff roles and responsibilities and risk management and control, as well as those set out at Appendix A.

11. 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. Mobile network operators should have in place 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.

12. In any event, where a Level 1 provider contracts with a third-party consent platform, the Level 1 will remain responsible for the verification.

Calls to voice-based premium rate numbers

13. In the case of calls to non-geographic numbers used for phone-paid services

[1] This means that neither party should be controlled or influenced in any way by the other, including through officers, staff, representatives or others with significant control within or connected to either party.

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.

14. UK networks have technical safeguards in place 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).

15. When a consumer disputes such a charge, if the originating network provides PSA with their record of the call, we will generally accept that the charge was valid if there is no other evidence that would lead us to investigate further.

16. We note that this does not mean 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 where necessary.

Text messages sent to a mobile shortcode

17. Where a consumer sends a message to a mobile shortcode promoted in print, on television, or on a website, the message is known as a Mobile Originating (MO) message. As 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, providing there is no other evidence that would lead us to investigate further, for example evidence that a consumer’s mobile handset was infected with malware which initiated the MO message without their consent.

18. Again, the sending of an MO message by a consumer does not mean that the consumer’s consent was informed or that the promotional material the consumer saw before sending the MO message complies with the Code, and we will investigate this where appropriate.

Entry of a consumer’s mobile number into a website – where the consumer is using wi-fi or their Network IP

19. Some phone-paid service charges are initiated by a consumer entering a mobile number on a website. Consumers do not always appreciate that entering their number in this way can initiate a purchase which carries a charge to their mobile bill. There is a risk of harm if a consumer enters a mobile number belonging to someone else (either by mistake or deliberately), which could lead to a second consumer being charged.

20. In addition, where a consumer uses their Network IP, an encrypted version of

their mobile number can be passed through to the payment platform of the website where the consumer is browsing, enabling a charge to be made to their bill.

21. The PSA's expectations for providers obtaining robust consent from a consumer are the same, whether the consumer is using their Network IP or using wifi.

22. Normally in both of these circumstances, a consumer enters their mobile number into a field on the website, which initiates a Mobile Termination (MT) message from the service provider to the consumer's handset. Where a provider wishes to use this process, the PSA's expectations are as follows:

- 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 should be sent to the related handset containing a PIN. The PIN should be initiated and confirmed by the Level 1 provider[2] through interaction with the consumer. We recommend the PIN is alphanumeric and contains no less than four truly random 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.

23. 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.

24. 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. 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.

25. 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 the charge. Where this is the case, we would expect that the message also contains the service name (and brand where different), and the

[2] This function may be undertaken by an independent third party on behalf of the Level 1 provider. Where a Network operator contracts directly with a Level 2 provider (i.e. there is no Level 1 provider involved in the provision of the service), the function may be undertaken by the Network operator.

cost and frequency of charging, in such a way as to make clear to the consumer that replying with the keyword will result in a charge.

26. Providers may also use a password-controlled account, with the consumer entering a password which they have selected and control to first confirm their identity, and then confirming consent to payment on a second screen, or by using biometric technology such as fingerprint or facial recognition.

27. Following the above steps will assist providers in achieving and demonstrating robust consent to charge in consumer journeys. However, where providers and/or specific services are subject to other PSA regulatory requirements, such as Special conditions, compliance with the above steps may not be sufficient to meet those requirements and therefore providers should ensure that they take all further steps necessary to achieve compliance with such requirements.

Charges incurred each time the consumer views a new webpage, image or video on a website[3]

28. In some circumstances, charges can be generated once consumers click on a 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. In the alternative, 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.

Section Three: Expectations around robust payment and verification platforms

What are robust payment and verification platforms?

29. Payment and/or consent verification platforms (and related web interfaces) which have adequate technical and risk control procedures, that demonstrate 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

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

[3] 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 expectations
- staff roles and responsibilities
- risk management and control.

31. The expectations set out under the headings below apply to all platforms. This includes payment/consent platforms provided by any 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

32. In setting Technical Expectations for payment and consent verification platforms, the PSA notes it is possible to arrive at robust proof of informed consent via different approaches depending on the design of a platform's technical architecture. Nonetheless, there are universally accepted standards regarding the underlying software platforms use to operate, and the protocols they use to interface with web pages and other external systems. The Technical Expectations which we set focus on these universal standards. These are set out at Appendix A.

33. To ensure our expectations remain up to date, and prevent them being rendered obsolete by evolving technology, we will review them in conjunction with the mobile network operators on an annual basis and consult on any proposed revisions.

Staff roles and responsibilities

34. Payment/consent platforms can be compromised by bad judgement on the part of those who are responsible for them. The likelihood of this 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. To ensure that any risk is adequately identified, communicated, and controlled, the PSA has set out expectations around roles and responsibilities, and staff training.

35. The PSA recognises that staffing decisions are a matter for the company concerned. However, given the importance to the consumer interest of maintaining a sufficient level of platform security, the PSA's expectation is that all platform providers have adequate resource, either internal or externally contracted, focused on security and fraud. The PSA recommends that security staff should be suitably qualified (such as a degree in computer science or a related discipline) and/or experienced such that they are able to meet the following competencies:

- 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.

36. The PSA's expectation is that all platform providers have an assigned "Head of Security" or other equivalent senior role. The PSA recommends that a Head of Security or equivalent senior person should be suitably qualified and/or experienced such that they are able to meet the below competencies:

- demonstrable knowledge of the latest security thinking and threat modelling-methods
- ability to manage complex IT platform overhaul projects, if required
- significant knowledge and experience of IT/web security to enable the effective identification, management and control of security and fraud risks
- we recommend that the Head of Security or other equivalent senior person has significant knowledge and experience of security management systems and processes. Examples might be, but are not limited to, experience of working towards ISO/IEC 27001 certification and the National Cyber Security Centre (NCSC) "Cyber Essentials Plus" assurance, or current equivalent.

Where such a role is vacant as a result of staff departure or absence, then responsibility should shift upwards to a more senior member of staff.

37. The PSA's expectation is that each platform provider should have a nominated Single Point of Contact (SPoC) whose details have been shared with the various industry stakeholders such that when an incident does occur, no time is wasted in investigating and rectifying issues.

38. We recommend that all providers ensure that platform development staff are trained in secure development techniques and have an understanding of relevant risks and threats to an appropriate level, which we recommend is at least at or akin to the NCSC "Cyber Essentials" level or current equivalent. Training should be undertaken periodically, to take account of threat and risk evolution and to keep skills current.

39. Our expectation is that all platform development staff should build their understanding of relevant risks and threats into any development work they carry out. Providers will be expected to be able to demonstrate this upon request or direction by the PSA.

40. The PSA's expectation is that all platform or other systems development – including but not limited to new protocols for phone-payments – should have their functionality reviewed by the security team before they go live.

41. The PSA recommends that the Head of Security (or equivalent senior person) should have the authority to veto any protocols or solutions and be able to make go-live subject to an audited assessment and approval from the security team. Where the decision is taken not to follow this recommendation, the provider should be able to demonstrate how they achieve an equivalent level of assurance. An example template for recording such assessment is attached at Appendix C. The use of this template is entirely voluntary and is intended to set out the level of detail the PSA would expect to receive about assessments where relevant to an investigation.

Risk management and control

42. It is important that all organisations involved in payment or consent verification have adequate processes to quickly identify, record, communicate, and control risk, and to incorporate lessons learned into processes.

43. All parties involved in provision of phone-paid services 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.

44. In addition, the PSA recommends that active threat monitoring measures are implemented to monitor systems and alert staff in real time. These measures should aggregate data from across the platform, understand traffic patterns, 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

    - analysing Level 2 provider behaviour – e.g. what kind of data they access and how frequently, whether apps are requesting payment pages

    - 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.

45. All parties involved in the provision of phone-paid services 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 Appendix 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 security breaches or attempted breaches where relevant to an investigation.

46. The PSA recommends that each payment and/or consent verification platform should 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. 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) may be in breach of the relevant Code rules[4] until the fix has been completed, as independently verified by the tester.

47. In line with current due diligence and risk assessment obligations, Level 1 providers should have contracts in place which allow them to suspend or terminate payment facility to any Level 2 providers or third-party consent verification platforms on the basis of non-compliant activity, such as charging consumers without informed and robust consent, or where they reasonably suspect that such activity has or is occurring.

48. Also in line with current due diligence and risk assessment obligations, Mobile network operators should have contracts in place which allow them to suspend or terminate Level 1 providers in circumstances where non-compliant activity is discovered. In addition, they should take effective action against Level 1 providers whose platforms facilitate non-compliant activity, such as charging consumers without consent or where they reasonably suspect this to be the

[4] Only platforms which are part of the value chain may be considered by a PSA Tribunal to be in breach of 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 by a PSA Tribunal to be in breach of Rule 2.3.3 of the Code.

case.

49. 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 warrants suspension or contract termination.

50. The PSA recommends that 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.

51. For the avoidance of doubt, we would be unlikely to consider the end of a direct contract to be a sufficient risk control measure on its own, if the Level 1 provider in question were still permitted to operate within the value chain through another Level 1 provider's platform – i.e. we would expect further assurance and risk control to be able to be demonstrated.

52. The PSA's Guidance on Due Diligence Risk Assessment and Control provides further guidance on the PSA's expectations in respect of risk management and control.

Appendix A – Technical Expectations

The following are a list of Technical Expectations which the PSA expects all payment and/or consent verification platforms to have in place while 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.

Where a provider's platform does not explicitly meet one or more of the specific expectations listed below, the PSA expects that the provider will be able to demonstrate on request how the objective expressed in that expectation is otherwise achieved. The expectations are as follows:

- all platforms should be hosted strictly independently of any Level 2 provider[5]. Where a Level 1 provider wishes to offer services on its own platform then it must retain ownership, control and responsibility for all aspects of the service
- all platforms should use the current version of the Transport Layer Security (TLS) protocols or as a minimum 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
- payment pages should protect against click-jacking, for example by use of HTTP Headers
- any phone-paid transaction should only occur over correctly validated HTTP connections
- payload protection should be implemented in order that it cannot be edited part way 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 and expire within a reasonable amount of time.[6]

[5] This means without the control, or influence of any Level 2 provider, including their officers, staff, representatives or other persons with significant control.

[6] We recommend that providers refer to the Information Commissioner's Office (ICO) to ensure that any authentication cookies and expiry times are in line with relevant legislation and the ICO's expectations.

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). 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.

Council for Registered Ethical Security Testers (CREST)

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)

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.

Common Vulnerability Scoring System (CVSS)

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 one to ten, with ten being the most severe.

Hyper Text Transfer Protocol (HTTP)

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.

HTTP Strict Transport Security (HSTS)

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 a 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.

National Cyber Security Centre – (NCSC)

The NCSC is an organisation of the UK Government that provides advice and support for the public and private sector on 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 Confederation of British Industry and a number of insurance organisations which are offering incentives for businesses. From 1October 2014, the Government has required 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 organisation 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".

Open Web Security Application Project (OWASP)

OWASP is a worldwide not-for-profit charitable organisation focused on improving the security of software, so that individuals and organisations 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

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.

Personal Identification Number (PIN)

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.

Transport Layer Security (TLS)

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.

Uniform Resource Locator (URL)

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?*