GDPR and PCI DSS: What's 'appropriate'

This paper considers the relationship between the Payment Card Industry (PCI) Data Security Standard (DSS) and the General Data Protection Regulation (GDPR). It considers whether compliance with PCI DSS may help an organisation meet GDPR's requirement to "*implement appropriate technical and organisational measures*" in respect of the security of cardholder data.

This paper assumes the reader is broadly familiar with GDPR and with PCI DSS.

This paper does not constitute legal advice. It is a general summary of the requirements of GDPR and enforcement action taken by the UK Information Commissioner's Office.

Readers are encouraged to obtain legal advice from a qualified solicitor in their jurisdiction in respect of their organisation's obligations within GDPR.

1 Executive summary

- Cardholder data is Personal Data as defined by GDPR.
- Organisations compliant with PCI DSS are likely to meet the requirements of GDPR in respect of protecting the confidentiality and integrity of cardholder data and so would satisfy a regulator that they had taken 'appropriate measures'.
- Organisations need not comply with PCI DSS to meet the requirements of GDPR but could take their own-risk based approach to protect the confidentiality and integrity of cardholder data. This should be documented and formally accepted by the organisation in accordance with the organisations governance processes. In the event of a breach of confidentiality of cardholder data the organisation would have to justify its choice of control framework to a supervisory authority.
- Compliance with PCI DSS will not meet the requirements of GDPR in respect of the availability and resilience of systems processing cardholder data. If a lack of availability or resilience of systems processing cardholder data is likely to affect the fundamental rights and freedoms of cardholders or other data subjects, organisations should take additional technical and organisational measures.

2 Is cardholder data personal data?

GDPR defines personal data as "information relating to an identified or identifiable natural person". Cardholder data may consist of primary account number (PAN) on its own or PAN in combination with expiration date, cardholder name and service code. Generally, a PAN is related to an identified or identifiable cardholder and therefore would constitute personal data. Expiration date and service code when processed together with PAN would also be treated as personal data.

There are notable exceptions such as single-use and virtual PANs, some forms of corporate cards and proxy card numbers (tokens) that do not relate to an individual – these are outside the scope of this analysis. It has also been suggested that because a PAN may be related to two individuals (e.g. primary and secondary cardholders) that it is not personal data – this would be a brave and courageous interpretation, and not recommended!

3 ICO enforcement action

The Information Commissioner's Office has taken enforcement action (within the auspices of the 1998 Data Protection Act) on a number of occasions where cardholder data has been compromised. In all cases compliance (or the lack of compliance) with PCI DSS has been mentioned. The seventh data protection principle (in the 1998 Act) for a data controller to take "*Appropriate technical and organisational measures*" to protect the security of personal data is sufficiently similar to the requirement in Article 32(1) of GDPR that ICO commentary in enforcement action under the 1998 Act is a good indicator of what the Commissioner's position will be in relation to GDPR.

3.1 Lush (2011)

Lush suffered a compromise of cardholder data from its website. Lush signed an undertaking (a formal commitment) that it would outsource its payment processing to a "PCI Compliant Service Provider". The ICO's press release gave the first indication that the ICO considered PCI DSS as providing appropriate technical and organisational controls for the protection of cardholder data.

> *"Lush took some steps to protect their customers' data but failed to do regular security checks and did not fully meet industry standards relating to card payment security. Had they done this, it may have prevented the fraud taking place and could have saved the victims a great deal of worry and time invested in claiming their money back. This breach should serve as a warning to all retailers that online security must be taken seriously and that the Payment Card Industry Data Security Standard or an equivalent must be followed at all times"*

3.2 Think W3 (2014)

Think W3 lost some 1.1 million card numbers stored in a database (about 7 years' worth). In the monetary penalty notice the Commissioner highlighted a number of failings in Think W3's technical and organisational controls including:

> *"In particular the data controller failed to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data by failing to:[…]*
>
> - *Fully comply with the Payment Card Industry - Data Security Standard."*

3.3 Worldview (2014)

Worldview lost some 3,800 card numbers and CVV2 via a SQL injection attack. The monetary penalty notice this time did not equate compliance with PCI DSS as meeting the 'appropriate' test but the Commissioner stated:

> *"The data controller should have been aware of the risks associated with any compromise of card data due to the nature of the data being collected. The data controller was also aware of the Payment Card Industry – Data Security Standard covering security related issues, and that there was a risk in storing CVV numbers."*

3.4 Staysure.co.uk (2015)

Staysure suffered a data breach of around 110,000 card numbers with CVV2. The ICO's monetary penalty notice was brief and although it did not call out non-compliance with PCI DSS in respect of the many control failings, it highlighted:

> *"…Storing payment card CVV numbers on its database in breach of the Payment Card Industry Data Security Standard. ..."*

Further, in the Commissioner's analysis of whether Staysure ought to have 'known' that a breach was possible, he observed:

> *"The data controller should have been aware of the risks associated with any compromise of payment card and cardholder data due to the nature of the data being collected. The data controller was also aware of the Payment Card Industry Data Security Standard covering security related issues, and that there was a particular risk in storing CVV numbers."*

3.5 Carphone Warehouse (2018)

A data breach compromised 18,000 PAN and CVV2 (along with 3.3 million personal data records). The loss of cardholder data was minor in relation to the size of the personal data breach, but in the monetary penalty notice the Commissioner observed:

> *"The processing of credit card data should have alerted Carphone Warehouse to the need for security measures that at least achieved compliance with the Payment Card Industry Data Security Standard. It was working to achieve that compliance, but a data controller in its position should have done so much earlier."*

3.6 Summary of ICO enforcement

In all data breaches where cardholder data was present and the Commissioner took enforcement action, PCI DSS is referenced. In Lush and Think W3, non-compliance with DSS (or an equivalent) was stated as a clear breach of the seventh principle. In Talk Talk the Commissioner was clear, given the size and maturity of the company, it should have been compliant.

It cannot be said that the Commissioner's view is that non-compliance with PCI DSS automatically means that the data controller has not taken the appropriate technical and organisational measures to protect cardholder data. However, in the event of a data breach, a data controller's knowing non-compliance, in the absence of documented risk-based equivalent controls, would be regarded as a breach of the seventh data protection principle and under GDPR, a breach of Art. 32.

Perhaps the most important observation that can be taken from an analysis of the Commissioner's enforcement action is this. If you read the ICO's description of the vulnerabilities that allowed each of these data breaches to happen, none would have occurred if the organisation had implemented the requirements of PCI DSS.

4 Matching GDPR's security requirements

The following table analyses the text of Article 32 of GDPR and considers the compliance that PCI DSS delivers in respect of the protection of cardholder data.

4.1 What GDPR requires	4.2 What PCI DSS provides
32(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement **appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, including inter alia as appropriate:	PCI DSS provides a high standard of technical and organisational measures to ensure a level of security. Regulatory statements indicate that the ICO considers PCI DSS as appropriate technical and organisational measures to protect cardholder data. However, DSS cannot always said to be appropriate to the risk, as the standard applies uniformly irrespective of the volume or type of cardholder data processed. For example within Europe, given all the safeguards in the payment system, unauthorised access to a PAN alone poses less of a risk to the data subject (cardholder) than unauthorised access to the combination of PAN, expiration date and CVV2 which in themselves presents less risk than unauthorised access to an entire magnetic stripe (for as long as magnetic stripe acceptance exists). As such the application of all of PCI DSS's requirements in certain environments may be over and above what GDPR would consider appropriate. Compliance with a cut-down set of PCI DSS requirements (e.g. via card scheme or acquirer's risk-based approach) would be seen as appropriate. Organisations that have a low tolerance for regulatory risk may consider that applying PCI DSS to a low-risk environment would at least provide a higher degree of regulatory certainty.
(a) the pseudonymisation and encryption of personal data;	PCI DSS requires cardholder data to be encrypted at rest [3.4] and in transit over public networks [4.1]. Tokenisation (pseudonymisation) is

4.1 What GDPR requires	4.2 What PCI DSS provides
	frequently used in payments to create a value that would have less risk to the data subject (cardholder) if the data was lost.
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	Although PCI DSS provides appropriate controls to ensure the confidentiality (and as a by-product the integrity) of cardholder data, it provides no technical or organisational measures to ensure availability or resilience.
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;	PCI DSS has no requirements to support this requirement.
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	PCI DSS contains many appropriate measures for testing and assurance [requirement 11] which, when coupled with a card brand's compliance programme that for example requires external QSA audit, provides a high level of assurance.
32(2). In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.	Although PCI DSS includes the requirement for a risk assessment [12.2], this is undertaken from the perspective of the organisation and not the risks that a personal data breach would pose to the data subject (cardholder).
32(3) Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.	Although PCI DSS has the quality of a code of conduct, it has not been put forward for approval by the PCI SSC and so would provide no assurance in respect of this requirement.
32(4) The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	PCI DSS requires organisations to train all personnel processing cardholder data in the security of cardholder data [12.6] and requires personnel to be screened [12.7]