

North Lanarkshire Council Report

Audit and Scrutiny Panel

approval noting

Ref KH/RL/GL

Date 03/09/20

PCI-DSS compliance – Progress Report

From Katrina Hassell, Head of Business Solutions

Email HassellK@northlan.gov.uk **Telephone** 01698 302235

Executive Summary

The purpose of this report is to provide the Panel with an overview of the Council's compliance with the Payment Card Industry Data Security Standard (PCI DSS).

This report summarises the existing status of PCI DSS compliance, provides assessment of the current environment, outlines recommended actions to improve the nature of the network topology, and notes required works to align the Council with PCI DSS and ensure ongoing compliance.

In particular this report notes both the risks associated with non-compliance and to any planned programme of works seeking to achieve compliance.

Recommendations

The Panel is invited to:

- (1) Note the content of the report, and planned improvement actions, and;
 - (2) Note that significant work is still required to achieve and maintain compliance.
-

The Plan for North Lanarkshire

Priority All priorities

Ambition statement All ambition statements

1. Background

- 1.1 Elected members are aware that the council permits payment for a wide range of services to be made using credit and debit cards. During 2019/20 the council processed nearly 330,000 credit and debit card payments collecting over £42M, a total which doesn't include North Lanarkshire Leisure (NL Leisure) or Culture North Lanarkshire (Culture NL).
 - 1.2 In 2006 those companies which provide payment card banking services formed the Payment Card Industry - Security Standards Council (PCI SSC). The SSC in turn created a set of security standards for safe payments worldwide, known as the PCI Data Security Standard (DSS). The standard focuses on securing the ICT systems which support card transactions. Applying PCI DSS should protect and benefit all parties involved in making credit and debit card transactions: cardholders, retailers/merchants, the acquiring banks which clear transactions, and the card-issuing companies themselves. Acquiring banks have informed organisations that they must comply with PCI DSS requirements in order to continue accepting card payments.
 - 1.3 As of the October 2019 PCI DSS assessment, a lack of formal ownership within council services saw the council fall into a state of non-compliance. The issue was highlighted during a change of Merchant Acquiring Bank, with Lloyds Cardnet – who now handle all card transactions – highlighting non-compliance could lead to potential contract termination. Given this would result in the council being unable to process card transactions, steps were taken to address immediately.
 - 1.4 Remedial action was undertaken jointly by Financial Services and Business Solutions, which with the aid of Lloyds Cardnet PCI DSS Compliance team, resulted in sufficient compliance being achieved to enable card transactions to continue. However this solution is short-term, and further actions and governance must be implemented to maintain compliance longer-term.
 - 1.5 Initial examination of the card payment landscape within the council has illuminated the complexity of its current payments structure. All payments must be associated with a 'merchant ID' which the council has six of. In addition, it has responsibility for the merchant IDs used by both NL Leisure and Culture NL. In essence, the council, together with NL Leisure and Culture NL, has a number of card payment systems, together with a range of payment streams and supporting processes, each of which must comply with a potentially complex set of PCI DSS requirements.
 - 1.6 It is evident that PCI DSS must be addressed and joint responsibility for this has been agreed between Financial Services and Business Solutions. A PCI project group is now convened consisting of representatives from Financial Services and Business Solutions, along with representation from Culture NL and NL Leisure. This group will consider the requirements levied through the PCI DSS and agree actions which enable the council to ensure and maintain future compliance.
 - 1.7 It should be noted that any breach of cardholder details, which PCI DSS compliance aims to reduce the likelihood and impact of, will also be a breach of the Data Protection Act 2018. Fines levied by the PCI for a data breach affecting a non-compliant organisation may be escalated by intervention to the Information Commissioner's Office, who may in turn impose further penalties.
-

2. Planning for PCI DSS Compliance

PCI DSS Compliance Requirements

- 2.1 PCI DSS was set up to help businesses process card payment securely and reduce fraud. This is achieved through enforcing a number of tight controls surrounding storage, transmission and processing of cardholder data.
- 2.2 The standard has 12 high level requirements which fall into the six categories below:
- Build and Maintain a Secure Network
 - Protect Cardholder Data
 - Maintain a Vulnerability Management Program
 - Implement Strong Access Control Measures
 - Regularly Monitor and Test Networks
 - Maintain a policy that addresses Information Security
- 2.3 Compliance itself is demonstrated through submitting a self-assessment questionnaire (SAQ) to an organisation's acquiring bank. Four SAQs (SAQ-A through SAQ-D) exist; the SAQ to be submitted depends upon factors such as the channel through which card payments are taken, the data being processed, and the volume of transactions.
- 2.4 The council presently enables members of the public to make payments through the following channels:
- Payments in person;
 - Payments via telephone (known as 'cardholder not present' or 'Mail Order / Telephone Order' – MOTO – transactions);
 - Electronic payments through an on-line portal.
- 2.5 On initial examination it appears that the Council will need to submit SAQ-D. This is the most onerous of the four and requires approximately 300 questions to be answered.

Temporary Corrective Actions

- 2.6 There is a program of work planned to update the chip & pin devices and systems used to take card payments at multiple locations throughout the organisation and supported by the Capita Pay360 card payment system. This is an Internet-hosted system which validates both telephone and in-person payments. This had originally been intended to be complete by the end of June but has been rescheduled for September 2020.
- 2.7 There are 3 modules within Capita Pay360 which are being upgraded:
- AIM: Income Management;
 - ACR: Cash receipting system with chip & pin;
 - Paye.net: Browser based payment processing for both face to face (chip & pin) and telephone payments. This system is in operation in contact centres and across council offices.
- 2.8 The chip & pin devices themselves are being upgraded to point-to-point encryption (P2PE) which reduces the scope of PCI compliance. Encrypting card and cardholder data at the point it is taken effectively means it is no longer readable, at least until it reaches the acquiring bank. Any computer networks which that data touches en-route to the acquiring bank have less of a compliance requirement than those where the data remains unencrypted.

- 2.9 Ongoing security testing of computer networks must be performed to comply with PCI DSS, which requires a minimum of quarterly checks of computer networks to be performed by an Approved Scanning Vendor. This is in place using HackerGuardian, a PCI SSC approved scanning vendor. An additional process has been added to review quarterly, or when a significant configuration change takes place, the computer addresses being scanned to ensure that they are always relevant. This process further checks whether any new addresses are considered for scanning.
- 2.10 The council has contracted with Lloyds Cardnet to assist in the submission of the SAQ. Their PCI DSS Compliance Team engage with NLC over the phone regarding the reporting & validation process and pro-active monitoring of merchant ID accounts. Monthly tasks to be completed are agreed as and if required, with quarterly scans referenced above scheduled to ensure ongoing compliance.
- 2.11 A further requirement of PCI DSS is to maintain an information security policy that addresses information security for all personnel. A new Information Security Policy, forming part of the council's Information Governance Framework, was approved by the Policy & Strategy Committee in June 2020.
- 2.12 In respect of the current Covid-19 crisis additional guidance for homeworking was issued to management and staff outlining individual responsibilities of staff while processing card data.

Future Actions and Recommendations

- 2.13 The PCI project group is seeking to make recommendations on the way forward to achieve PCI DSS compliance, balancing effectiveness and value. These shall include issuing internal guidance relating to card payments (particularly with regards Card-Holder-Not-Present) that the organisation must reference when designing business processes.
- 2.14 The Council's current ICT payment channels are complex, and by their nature potentially bring all of the council's ICT network and associated processes into scope for PCI DSS compliance. De-scoping environments and processes reduces risk, and a balanced approach to service flexibility and risk management is advisable. Acceptance of risk to gain benefit must be an informed action and recorded as such. Engaging with a Qualified Security Assessor (QSA) (someone approved by the PCI SSC to guide organisations towards compliance) may offer good value, despite a cost overhead, in assuring that current and future card payment processes can comply with card security requirements. The PCI project group will examine options in this regard.
- 2.14 Good design of technology and processes, as well as training individuals in how to handle card payments, are fundamental building blocks for PCI compliance. By ensuring that the minimum amount of cardholder data touches the Council's network, the need for compliance can be de-scoped. Payments made through telephone channels, however, currently make the practice of data minimisation difficult.
- 2.15 The telephone payments' channel relays cardholder data as voice traffic across the council's ICT network. The PCI project group will look into how this volume of traffic can be reduced, and ideally removed all together from the council network.
- 2.16 As part of the DigitalNL program the Council have been looking into a new payment handling process for telephone/Cardholder Not Present transactions and this is currently in discussion with Capita Pay360.

- 2.17 In terms of training, a module on PCI DSS is available as part of the council's new online staff training suite. The PCI project group is looking to assess the value of this module in making appropriate staff aware of the need to handle cardholder details appropriately.
- 2.18 It is necessary to maintain a controlled record of merchant identifiers and payment locations and devices. The PCI project group will develop a process flow for continual review and revision of this record, such as when a configuration status change takes place or new device is enrolled into the environment.
- 2.19 The impact of Covid-19 has meant that several offices where payments would have been taken are now closed, and remote working practices implemented. This has hampered the review of merchant identifiers however highlights the increased necessity of such a task.
- 2.20 For assurance the project group will consider the value of using software to identify where cardholder data may be inadvertently stored.
- 2.21 The PCI project group is looking to approach vendors to demonstrate services for telephone transactions that would reduce the scope and impact of PCI compliance on the council. This activity would also take into consideration the integration of leisure services into the council portfolio and their need for a similar system.

Risks to Delivering and Maintaining PCI DSS Compliance

- 2.22 The complexity of council technologies and the processes involved in processing payments, together with the complexity of PCI DSS compliance and the lack of internal expertise in achieving compliance, create a risk that compliance is not achieved or maintainable. This could be addressed through employing a QSA to advise, if not lead, on pursuing compliance, the value of which will be regularly examined as the PCI DSS assurance programme progresses.
- 2.23 There is a risk that a lack of appropriate governance will lead to an ineffective compliance programme. This will be countered through ensuring effective ongoing ownership and schedule review is made available to ensure continued compliance.
- 2.24 There is a risk of over engineering PCI DSS compliance and it becoming a burden on the council and the ability to provision services. With the current infrastructure of the organisation and the large number of compliance requirements that must be addressed there is the risk of forcing security checks and procedures onto a service that has little or no links to the PCI DSS. Appropriate and informed service design coupled with recognised architectural infrastructure models, will manage this, however regular engagement with compliance expertise in the form of a QSA can mitigate risk.
- 2.24 Under the current directive for staff to work from home due to the Covid-19 crisis, senior management, after taking advice and considering the risk factors involved, made the decision to allow staff to continue to process telephone payments from home. Guidance for homeworking was issued to management and staff outlining the individual responsibilities of staff while processing card payments over the telephone. There is a risk to the council as staff are working in a home environment unsupervised.

Next Steps

- 2.25 Following review of the range of information presented to the Panel, Members are asked to be aware of the complexity of obtaining PCI DSS compliance and to note that continued

compliance can only be obtained through good governance, informed risk management and appropriate service engagement to ensure progress.

- 2.26 The PCI project group is finalising options for system changes which will manage the risk associated with PCI DSS compliance. As highlighted in the previous section there will be a cost and benefit to each option that presents itself, and effective risk governance will be needed to ensure the correct balance is struck.

3. Equality and Diversity

3.1 Fairer Scotland Duty

There is no requirement to carry out a Fairer Scotland Duty assessment on this report.

3.2 Equality Impact Assessment

There is no requirement to carry out an equality impact assessment on this report.

4. Implications

4.1 Financial Impact

There is no immediate financial impact arising from this report, but possible future costs associated with this compliance programme should be noted.

4.2 HR/Policy/Legislative Impact

The council will be able to demonstrate effective security around the taking of card payments and meet requirements levied by the PCI SSC and through the Data Protection Act 2018.

4.3 Environmental Impact

There is no environmental impact arising from this report.

4.4 Risk Impact

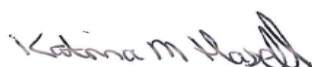
Risks have been noted in the body of this report.

5. Measures of success

- 5.1 The council continues to efficiently and effectively handle card payments to provide benefit to users of North Lanarkshire Council services.
-

6. Supporting documents

- 6.1 None



Head of Business Solutions