North Lanarkshire Council
Report

Audit and Scrutiny Panel

☒approval ☒noting **Ref** KH/RL/GL **Date** 09/12/21

PCI-DSS compliance – Progress Report

From Katrina Hassell, Head of Business Solutions

E-mail HassellK@northlan.gov.uk **Telephone** 01698 302235

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

Panel members are aware from the June 2021 update that the Council had targeted March 2022 to achieve full PCI DSS compliance, but that such was heavily dependent upon completing the significant change programme required to ensure MOTO (telephony payments) compliance.

This report summarises the positive actions completed to date on achieving compliance, updates on progress and challenges remaining in respect of MOTO compliance, and finally highlights the further activities which are necessary for the Council to achieve PCI DSS compliance.

Recommendations

The Panel is invited to:

1) Note the content of the report, and significant developments completed to date in progressing the Council towards compliance.
2) Note that a substantial level of work remains, particularly regarding MOTO transactions, to achieve compliance with relatively complex requirements. This work must be managed against a backdrop of competing high-priority programmes.
3) Note that the revised timeframe of March 2022 to achieve full compliance with all strands of the PCI DSS requirements is dependent upon the support of stakeholders. These are each faced with progressing competing programmes of work as outlined in (2) above.

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, and that acquiring banks require all organisations who accept card payments to be compliant with the Payment Card Industry Data Security Standards (PCI DSS).

1.2 The '*PCI-DSS Compliance – Progress Report'* to the Panel of 3 September 2020 highlighted the council has a complex array of payment systems and supporting processes and is therefore subject to equally complex and onerous compliance requirements. Non-compliance could ultimately lead to the Council being unable to process card transactions for goods and services. This report advised the Panel of the priority actions undertaken with Lloyds Cardnet PCI DSS Compliance team to enable the Council to continue to accept card payments. At the same time, the Council would be developing and deploying the longer-term actions and governance necessary to maintain compliance.

1.3 Through discussion of this earlier report at the Panel meeting of 3 September 2020, Business Solutions set an initial target date for achieving compliance with PCI DSS requirements of September 2021. Business Solutions thereafter identified the key milestones necessary to achieve compliance within that timeframe.

1.4 At the Panel meeting of June 2021, it was agreed that due to the additional complexities of MOTO transactions and the requirements to secure these payments, that a longer timeframe was required to examine and deploy solutions capable of securing MOTO payment channels. To this end, the target date for achieving full compliance was revised to March 2022.

1.5 This report illustrates progress against the planned activity, with a summary of compliance levels as of October 2021 provided for Panel consideration within paragraphs below.

2. Report

2.1 As noted in a previous Panel report, the Council is working towards a no 'Cardholder Data Environment' (CDE). In tackling this challenge, the approach has been to seek compliance on a channel-by-channel basis, thereby attesting to each individually. The channel break downs are as follows:

- Ecomm – Ecommerce (transactions conducted electronically on the Internet)
- EPOS – Electronic Point of Sale (face-2-face transactions using chip and pin devices.)
- MOTO – Mail Order / Telephone Order (card not present transactions over a telephone)

2.2 The Council has now successfully achieved compliance for the Ecomm channel.

2.3 Compliance against the following EPOS channels is well in hand and can be summarised as:

- The EPOS channel for the Corporate payment systems
- The EPOS channel covering Active and Creative Communities' (formerly Culture North Lanarkshire) use of the Spektrix booking system
- EPOS supported by standalone mobile chip and pin devices

2.4 The documentation to meet PCI requirements for these channels has been received from the relevant 3rd party providers and collated with the Council's policy documentation. Submissions will be made once final logistical issues have been resolved. These are:

2.4.1 EPOS compliance is supported through use of encrypted chip and pin devices. To appropriately provision encrypted devices for the Capita Pay360 solution, several technical constraints had to be addressed relating to the use of legacy applications within the Council. These legacy issues have now been remediated and the small number of non-compliant chip and pin devices will be replaced in the coming weeks.

2.4.2 Spektrix is used to manage and take payment for concert hall bookings. The Council had previously been informed that chip and pin devices taking Spektrix

payments were secured with encryption. However, upon further examination of these devices, encryption is confirmed as End-2-End Encrypted (E2EE) rather than Point-2-Point Encrypted (P2PE). It is the latter (P2PE) which PCI SSC consider as the standard required to ensure encryption throughout the transaction. To achieve this, a small number of devices therefore have to be updated and replaced. A pilot rollout of these replacements is underway, and once fully tested and evaluated, a full device deployment will follow.

2.5 The Council also takes EPOS payments through a Gladstone MRM system. Compliance against this particular combination is presently proving more challenging than those EPOS transactions outlined above because the Gladstone EPOS system is largely entwined with its MOTO transactions. The Panel are aware from previous reports that the MOTO channel for both the Spektrix and Gladstone systems (both previously used within the former Culture and Leisure North Lanarkshire entity) require further work to become PCI DSS compliant. These EPOS payments therefore cannot be attested alongside the other EPOS devices as initially planned.

2.6 When the Council initially set up payment card services, advice from the acquiring bank was to group associated Merchant ID's (MID's) together, as such was considered at that time to be the least complicated means of achieving PCI DSS compliance. This means however, that with compliance submissions based on MID groupings, non-compliance of even one channel within a grouping results in all other channels within that grouping also failing to achieve full compliance. There are presently four MID groupings, with the compliance status of each illustrated in figure 1 below.

NLC	Capita	Ecomm
Culture	Spektrix	Ecomm
Automated Call	Capita	Moto
NLC	Paye.net	Moto
Culture	Spektrix	Moto
Culture	Paye.net	Moto
NLC	Paye.net	EPOS
NLC	Gladstone	EPOS
Culture	Paye.net	EPOS
Leisure	Gladstone	EPOS/MOTO
Culture	Spektrix	EPOS
Culture	GPRS/IP	IP

Figure 1 - Current MID Grouping

Key: Green = compliant, Red = non-compliant

2.7 Compliance becomes further complicated due to the Leisure aspect of Active and Creative Communities having MID's associated with individual leisure sites, rather than a single MID for all sites managed. Given each Active and Creative Communities (Leisure) MID takes a combination of cardholder present (EPOS) and card holder **not** present (MOTO) transactions, the Council cannot achieve full compliance for the grouped EPOS channel, even though the majority of that grouping is technically compliant. In this situation two options are available

- Obtain separate MIDs for each channel, OR
- Accept that formal compliance for grouped MIDs is unachievable until MOTO payment processes become PCI DSS compliant.

2.8 A survey of transactions undertaken at individual leisure sites has been completed to identify those with scope to cease MOTO transactional activity, which subsequently allows the Council to certify compliance for the MID's associated with these centres on an EPOS only channel. Risks associated with further separating out MOTO and EPOS centres are detailed under the risk factors.

2.9 In parallel, there is progress underway to reduce the number of MOTO transactions that are taken by Active and Creative Communities. Presently each individual leisure centre has the functionality for taking MOTO payments, and actively does so. A new process is gradually being introduced across Active and Creative Communities for MOTO transactions to only be taken at a centralised headquarters. This will remove the need for both the EPOS and MOTO option at each individual leisure centre.

2.10 A request had been submitted to Lloyds Cardnet to change the current groupings layout from those shown in figure one above to those illustrated within figure two below. Doing so, allows an EPOS only grouping to be validated as there is no MOTO transactions grouped along with it. Delays in implementing this change have unfortunately arisen because Lloyds Cardnet are experiencing staffing issues, and in particular the departure of the Council's previous relationship manager. Pending assignation of our new customer manager, an interim manager has completed the requested changes to our MID grouping. These revisions, which are represented within figure 2, will allow the Council to complete compliance for the EPOS only grouping once the new Council EPOS devices referenced in paragraph 2.4.2 above have been deployed.

NLC	Capita	Ecomm
Culture	Spektrix	Ecomm
Automated Call	Capita	Moto
NLC	Paye.net	Moto
Culture	Spektrix	Moto
Culture	Paye.net	Moto
NLC	Paye.net	EPOS
NLC	Gladstone	EPOS
Culture	Paye.net	EPOS
Culture	Spektrix	EPOS
Culture	GPRS/IP	IP
Leisure	Gladstone	EPOS/MOTO

Figure 2 - Proposed MID Grouping

Key: Green = compliant, Red = non-compliant

2.11 The Panel will note that the automated call IVR (interactive voice response) system, which could be considered MOTO as it handles telephone calls, is now also in a separate grouping. Whilst this does handle telephone payments, such are completely outsourced and automated, with no card details therefore transmitted, processed, or stored on the Council network. This allows for SAQ completion as per the Ecomm profile.

2.12 The Council is continuing to work on reducing the number of MOTO transactions across the estate including Active and Creative Communities, where possible directing customers towards the automated call line or the fully compliant ecommerce channel. The complexity of the MOTO channel makes this difficult for all scenarios and systems employed by the Council. There is no obvious one-size-fits-all solution, and several different mechanisms are therefore being investigated.

2.13 The next Capita upgrade is scheduled for deployment in the coming months. This revised version will provide multiple options including:

2.13.1 Sending a digital link during a telephone call to a customer who can then make a payment, via that secure link, whilst still in the call. With this option, the customer can choose to remain with the agent, or complete the transaction later.

2.13.2 During a telephone call, when a customer is required to provide card details, they enter the card details, using a keypad into a touchtone phone with this then being processed securely with or without agent interaction.

2.14 There is unfortunately no equivalent solution for the Gladstone or Spektrix systems. Options are presently being examined to achieve PCI DSS compliance for these MOTO transactions but there is as yet no straightforward or clear solutions.

Additional Considerations

2.15 A PCI DSS awareness training program hosted within LearnNL has been implemented. Tamper check training documentation has been produced and is being introduced for those staff handling card payments. This will provide the appropriate awareness and training to identify security issues with the chip and pin terminal devices.

2.16 Consideration is on-going for a program of work to ensure that compliance, once achieved, is maintained annually. There will be several annual review tasks involved in this assurance program, including a requirement for any further card payment solution procurements to ensure appropriate PCI DSS certifications are identified and received from 3rd parties before contracts are agreed.

2.17 Awareness of the imminent version update of PCI DSS v4.0 should be noted by the panel. The PCI SSC are now targeting an introductory date of Q1 2022 for the next instalment of PCI DSS. There will be an 18-month transition period available once v4.0 materials are released so no immediate impact on the Council's position. Notwithstanding this though, the panel should understand that there may be further requirements for change by the time v4.0 is mandated in Q1 2024.

2.18 The introduction of the Second Payment Services Directive (PSD2) will bring further necessities and may have a big impact on the way merchants take payments from customers. Its introduction date has been pushed back from March 2022 to September 2022. As the Council is using a 3rd party hosted environment for Ecomm, this change should bring limited additional impacts, but the Panel should be aware of the change.

2.19 The introduction of 'open banking' in the UK may completely transform banking. It is presently unknown how this may affect the Council but is likely to be a consideration for 3rd party service providers. Such may introduce new opportunities for PCI DSS compliance in the future.

Risk Factors

2.20 There is the risk that separating Active and Creative Communities EPOS and MOTO Merchant IDs will double the number of MID's associated with Leisure. There are currently 19 Merchant ID's, so a potential increase to 38 would incur further costs and potentially double the workload of officers currently tasked with reconciling banking activity.

---

3. Public Sector Equality Duty and Fairer Scotland Duty

3.1 **Equality Impact Assessment**

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

3.2 **Fairer Scotland Duty**

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

4. Impact

4.1 **Financial impact**

4.1.1 There may be a small financial impact arising from changing the merchant ID groupings from those illustrated in figure one to those illustrated within figure two, but this is expected to be within the range of £10 - £15 charge.

4.1.2 Higher costs will arise from moving from 19 joint leisure EPOS / MOTO MID's to separate MID's for each. This is estimated at an increase of around £15 per month for each MID. Further work is required to assess any ongoing costs likely to arise in respect of a potentially increased workload for officers tasked with reconciling banking activity.

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 and the UK GDPR.

4.3 **Technology / Digital impact**

This report references relevant interdependencies with other transformation, service redesign and business change projects, with Enterprise Architecture Governance Group (EAGG) approval of any replacement technologies also acknowledged as a known requirement.

4.4 **Environmental impact**

There is no environmental impact arising from this report.

4.5 **Communications impact**

There is no immediate communication requirement or impact arising from this report.

4.6 **Risk impact**

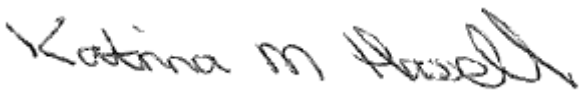
Risks are documented within paragraph 2.20 of this report.

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 There is no supporting documentation.



Katrina M Hassell
Head of Business Solutions