# North Lanarkshire Council Report

## Audit and Scrutiny Panel

☒approval ☒noting **Ref** KH/RL/GL **Date** 30/06/21

## PCI-DSS compliance – Progress Report

**From** Katrina Hassell, Head of Business Solutions

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

### Executive Summary

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) by the indicative date of September 2021.

Following on from the detailed report to the Panel in September 2020, this report summarises the positive actions completed to date to achieve iterative compliance, outlines the complexities of achieving compliance for MOTO (mail order/telephone order) transactions in particular, and illustrates further activity necessary for the Council to achieve PCI DSS compliance.

The complexities surrounding MOTO transactions when considered alongside the requirement for Business Solutions to procure replacement technologies and resource other priority council programmes illustrate the Council is unlikely to achieve full compliance by the targeted date of September 2021. A revised completion date of March 2022 is now targeted, with progress against this monitored through the Panel and the Transformation & Digitisation Committee.

### 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 these complex requirements, but such needs to be considered alongside the procurement and resourcing requirements of several other high-priority programmes, and
3) Note the revised timeframe of March 2022 to achieve full compliance with all strands of the PCI DSS security requirements.

### 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. Given non-compliance can ultimately lead to the council being unable to process card transactions for goods and services, this earlier 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 whilst it developed and deployed 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 a target date for achieving compliance with PCI DSS requirements of September 2021, and thereafter identified the key milestones necessary to achieve compliance within that timeframe.

1.4 This report illustrates progress against the planned activity, with a summary of estimated compliance levels as at September 2021 provided for Panel consideration within paragraph 2.20 below.

## 2. Report

2.1 Given the complexity of the Council's payment arrangements and supporting processes, a PCI DSS Governance Board was formed to provide oversight of project activities. The Board meets quarterly and will oversee development of the policies and processes required to achieve compliance.

2.2 Following through on the recommendation to engage a Qualified Security Assessor (QSA) to guide us towards compliance , the Council contracted the services of Compliance 3 (C3). C3 personnel have a background both in advising on and implementing PCI DSS compliance programmes, and operating PCI DSS compliance assurance programmes within the UK banking sector.

2.3 C3 facilitated an initial consultation session/workshop with senior stakeholders in February of this year. At this stakeholder session C3 provided an overview of the threat landscape, highlighted that payment data is personal data, and recommended we seek to limit exposure of payment data when designing our longer-term compliance arrangements. This is often referred to as minimising the Cardholder Data Environment (CDE).

2.4 With payment data assessed as personal data, and the Council legally required to protect such data, it is clear that actions taken to secure card payment systems and appropriate handling of cardholder data will not only address PCI DSS compliance, but will also support the Council in meeting the statutory requirements laid out in the UK GDPR and the Data Protection Act 2018. To this end, the project is now supported by the Council's Data Protection Officer and data protection team.

2.5 C3 confirmed that PCI DSS certification could be undertaken iteratively, and with this in mind, the C3 roadmap seeks to obtain compliance using a channel by channel approach. Our roadmap has therefore been constructed to reflect the three payment streams previously advised to the Panel of eCommerce, mail order/telephone order (MOTO), and cardholder present transactions, with compliance being sought separately for each.

2.6 Completion of the relevant self-assessment questionnaire (SAQ) for each payment system and channel forms a cornerstone of PCI DSS compliance. This requires the gathering of appropriate evidence to complete the appropriate SAQs, referring to documentation and contract clauses where appropriate. Using a red, amber green assessment rating (RAG), Table 1 below summarises the SAQs which need to be completed for each system and channel, and the relative complexity of each.

| Business Unit | Type | Questionnaire | Difficulty Level |
|---|---|---|---|
| **North Lanarkshire Council (Corporate)** | ECOMMERCE | SAQ – A | Easy (24 Questions) |
| | EPOS (Face2Face) | SAQ – P2PE | Easy (34 Questions) |
| | MOTO | SAQ D | Extreme (328 Questions) |
| **Culture** | ECOMMERCE | SAQ – EP | Difficult (192 Questions) |
| | EPOS (Face2Face) | SAQ - P2PE | Easy (34 Questions) |
| | MOTO | SAQ D | Extreme (328 Questions) |
| **Leisure** | ECOMMERCE | SAQ – A | Easy (24 Questions) |
| | EPOS (Face2Face) | SAQ – P2PE | Easy (34 Questions) |
| | MOTO | SAQ - D | Extreme (328 Questions) |

*Table 1- SAQ (Self-assessment Questionnaire) Complexity Levels*

2.7 With the former CultureNL and NL Leisure organisations operating independent arrangements, but the Council ultimately responsible for achieving compliance for all, table 1 above illustrates we have a complex card payment landscape to address with multiple systems taking payments across each of these channels as follows:

- A ‘Capita 360’ system is used by several Council services, and accommodates in person card payments, web-hosted ecommerce and both automated and non-automated telephone payments;
- NL Leisure offered eCommerce facilities to customers through a separate card provider WorldPay, but also use a ‘Gladstone’ system to accommodate MOTO and in person card payments;
- Culture NL also operate a ‘Gladstone’ system, but it is entirely separate to that used by NL Leisure and is primarily used to accept in person card payments for cultural activities;
- Finally, CultureNL also used a Spektrix hosted system to accommodate all forms of card payments in respect of concert hall bookings.

2.8 Following the initial meeting with C3, further workshops were held to examine the processes and payment card journeys associated with eCommerce and MOTO payments, with the data flows for these channels subsequently mapped. Members will wish to note these fully reflect the complicated payment structure of the newly in-sourced Active and Creative Communities.

2.9 Use cases for the MOTO and eCommerce payment channels have been developed, with payment volumes per channel currently being analysed.

2.10 The September 2020 report to the Panel highlighted the desire to minimise the amount of cardholder data routed through our card payment systems, and further outlined options to progress this via a range of planned upgrades to the Capita Pay360 card payment system. Work in this area has progressed well with the upgrade to the cardholder present payment channel now complete, and early assessments indicating our Cardholder Data

Environment (CDE) is moving to a security level which may allow a reduction in PCI scope. Work is under way towards achievement of a zero, or very low, CDE for this channel.

2.11 The '*Programme Progress Update on Insourcing of Culture, Sport and Leisure Services'* report to the Policy and Strategy Committee in December 2020 advised that integrating the leisure network with the council's infrastructure was challenging, and would be undertaken in a planned and phased way, commencing with upgrades to critical business systems. From a PCI DSS viewpoint, the upgrade to the Leisure Management System (Gladstone) used by the Leisure side of Active and Creative Communities has seen them move to a cloud hosting solution, improving the security of their data and reducing the scope of cardholder data residing on the currently separate Leisure network.

2.12 There is an additional requirement to liaise with other organisations which may be acting as service providers to the Council, such as Glasgow City Council. These organisations store, process or transmit cardholder data on the Council's behalf. The scope and requirements differ for service providers, and we need these to be documented to demonstrate PCI DSS compliance

**Next Steps/Planned Actions**

2.13 Having completed workshops in respect of the cardholder present channel, high-level flow diagrams and use case mapping are being progressed to facilitate compliance for that channel. As outlined in paragraph 2.7 above, the Council processes cardholder present payments through both Gladstone systems, Spektrix and Capita 360.

2.14 There is a requirement to forecast payment volumes associated with the cardholder present channel, which for the moment has the added complication of locations which routinely offer cardholder present payments having been closed or partially reduced due to Covid19 pandemic restrictions. This will lead to assumptions being made on the payment volume data we are able to analyse.

2.15 Developments to payment systems are taking place at the same time as PCI DSS compliance is being progressed. New systems are being put in place to update or replace ageing ones. As well as impacting on the immediate PCI DSS compliance programme, ongoing annual accreditation will require any changes to existing systems or the uptake of new payment processing to be carefully evaluated in advance of implementation.

2.16 Recognising the volume and nature of card transactions currently being processed within the Council's ICT/telephony network, the entirety of the Council ICT network is within the scope of the PCI DSS compliance assessment of the MOTO channel. In line with the C3 advice outlined in paragraph 2.3 above, we are seeking to limit exposure of payment data when designing our longer-term compliance arrangements, and will therefore need to procure new telephony payment services to reduce the scope of the MOTO channel. Appropriate solutions are currently being evaluated, but competing pressures within Business Solutions mean these – and therefore MOTO PCI DSS compliance – are unlikely to be fully operational by the targeted September 2021 deadline.

2.17 In the context of MOTO, consideration must also be given to the changing landscape of digital technology payments where there has been a move away from traditional telephone-based payment channels to the use of digital technology such as smart devices and social media. This includes mechanisms such as SMS, web chat, email, and online direct messaging.

2.18 The use of digital technology, whilst not replacing telephone-based payment completely, will complement the MOTO payment channel and provide further protection more in line with an eCommerce transaction thus reducing cost and improving security.

2.19 There is a further requirement to review and audit point of sale chip and pin devices. Due to the pandemic many locations that deliver face to face transactions were closed, with some but not all now reopening. An audit of the devices currently in place must be undertaken to ensure assets are accounted for and configurations confirmed.

2.20 Although we set an ambitious target of September 2021 for achieving PCI DSS compliance, it is clear through the work progressed so far that this indicative date cannot be achieved across all payment channels, particularly MOTO. Again using a RAG assessment convention, Table 2 below summarises expected compliance status as at September 2021.

| | NLC | Culture | | | Leisure |
|---|---|---|---|---|---|
| | **Capita Pay360** | **Spektrix** | **Gladstone** | **Capita Pay360** | **Gladstone** |
| **ECOMMERCE** | 100% | 100% | N/A | N/A | 100% |
| **EPOS** | 100% | 100% | 100% | 100% | 100% |
| **MOTO** | 60% | 50% | N/A | 60% | 60% |

*Table 2 – Submission / Compliance Status as at 30 September 2021*

2.21 Included in Appendix 1 is a projected timeline for the compliance of the MOTO payment channel, and a revised completion date of March 2022. As this timeline is reliant on multiple systems integrating to a solution which has still to be procured, there is scope for further movement on this revised completion date. Steps are planned to ensure our acquiring bank remains aware of the status of our compliance with the MOTO channel.

### Risk Factors impacting project completion

2.21 A recent staff absence has slowed the de-scoping progress for the Culture side of Active and Creative Communities. Although colleagues are covering this absence and supporting this priority project, they do not have the same level or in-depth technical knowledge of the former CultureNL network and payment infrastructures as those former employees.

2.22 The requirement for system upgrades and reliance on several other areas of Business Solutions projects underway, for example work required to introduce robust digital technology (tendering, testing, piloting, phased rollout, and full deployment) significantly impacts achievement of PCI DSS compliance for the MOTO channel within the targeted September 2021 timescales.

2.23 The introduction of digital technology will be a new method of taking payments and will involve training and implementation of required changes to documented practice.

2.24 The use of payment service providers who are not PCI DSS compliant may incur delay.

2.25 The plan to separately achieve compliance for channels and systems mean that risks can be mitigated to some extent. By taking a compartmentalised approach to compliance, scope exists to take remedial action to prevent a risk or issue affecting the compliance of one system or channel impacting on the others.

2.26 Having taken the priority action with the Lloyds Cardnet PCI DSS Compliance team outlined in paragraph 1.2 above, we have maintained close working relationships and dialogue with our acquiring bank. They are fully aware of, and satisfied with, the status of our implementation and compliance plan, and have confirmed there is no threat of merchant IDs being disconnected whilst we continue to develop and deploy our longer-term arrangements, including that extended timescale requirement in respect of MOTO.

## 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

Engaging Compliance 3 (C3) to guide us towards compliance with the relevant security standards incurs one-off revenue costs of £5,000 and will be met from Business Solutions 2021-22 revenue budget. Procurement of the unified communications platform highlighted in Appendix 1 is included within the approved capital programme. Though independent of specific PCI DSS requirements, this project has scope to link with the required payment solution software and therefore the individual payment management systems, which may provide opportunity to reduce the overall integration costs. These have however not yet been identified, hence scope still exists for PCI DSS compliance to give rise to some additional costs.

### 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 paragraphs 2.21 to 2.26 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

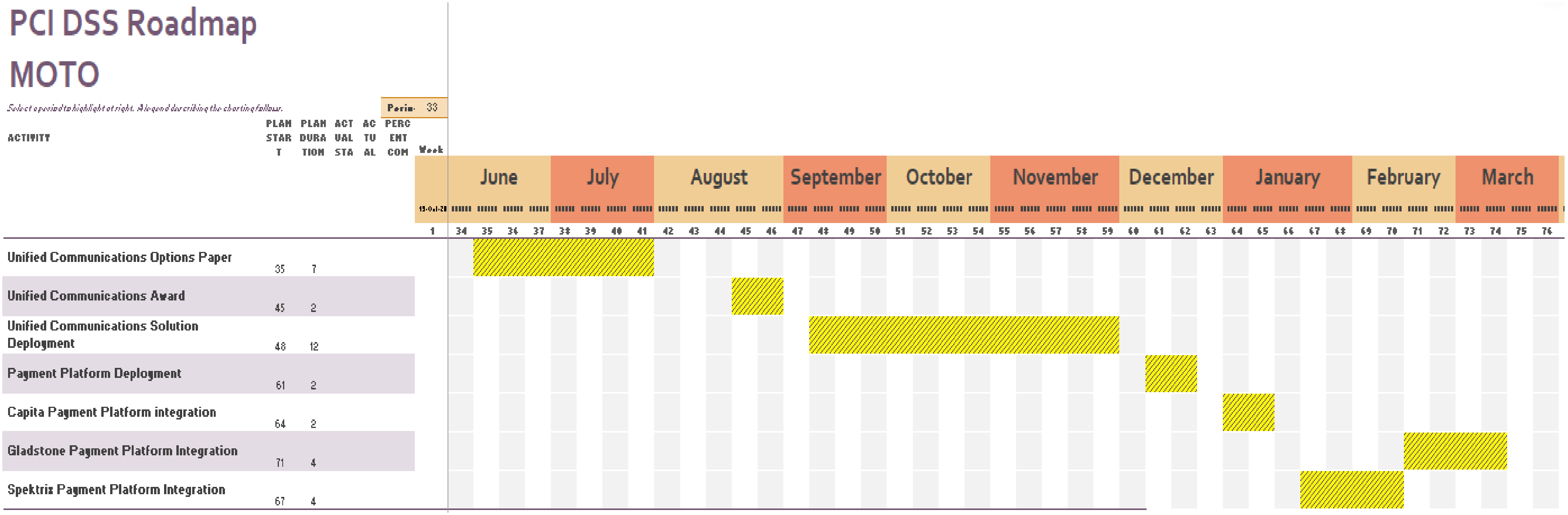
6.1 Appendix 1 – Moto Project Implementation Timeline

Katrina M Hassell

**Katrina M Hassell**
**Head of Business Solutions**

**Appendix 1**

## PCI DSS Roadmap for MOTO Implementation



PCI DSS Roadmap

MOTO

*Select a period to highlight at right. A legend describing the charting follows.*

Perio 33

| ACTIVITY | PLAN START | PLAN DURATION | ACTUAL STA | ACTUAL | PERCENT COM |
|---|---|---|---|---|---|
| Unified Communications Options Paper | 35 | 7 | | | |
| Unified Communications Award | 45 | 2 | | | |
| Unified Communications Solution Deployment | 48 | 12 | | | |
| Payment Platform Deployment | 61 | 2 | | | |
| Capita Payment Platform integration | 64 | 2 | | | |
| Gladstone Payment Platform Integration | 71 | 4 | | | |
| Spektrix Payment Platform Integration | 67 | 4 | | | |