AUDIT COMMITTEE – 22 MARCH 2024

PCI DSS UPDATE

1. RECOMMENDATIONS

1.1 It is recommended that the Audit committee note the contents of this report.

2. INTRODUCTION

2.1 Payment card industry data security standard (PCI DSS) is the global security standard for all organisations that store, process or transmit cardholder data and/or sensitive authentication data.

2.2 There are 4 PCI DSS compliance levels. New Forest District Council (NFDC) falls into Level 3: for merchants that process 20,000 to 1 million transactions annually. As a Level 3 Merchant NFDC has a requirement to submit a self-assessment questionnaire (SAQ) annually, conduct approved scanning vendor (ASV) scans quarterly and complete the attestation of compliance (AOC) form.

2.3 Organisations that handle cardholder data, even if only momentarily, are required to comply with over 300 security protocols under PCI DSS. However, by outsourcing handling cardholder data to PCI DSS accredited third party service providers this is reduced to just over 20 security controls.

2.4 Payment card industry data security standards (PCI DSS) accreditation at NFDC has previously received high priority recommendations through the internal audit plan.

3. PROGRESS MADE TOWARDS PCI DSS COMPLIANCE

3.1 NFDC has been working towards outsourcing handling cardholder data to PCI DSS accredited third party service providers. These solutions work in a way such that no cardholder data ever enters NFDC systems.

3.2 The table below details the current progress.

Payment Channel	**Status**
Information Offices Pin Entry Devices (PEDs)	Outsourced
Car Park Terminal Payments	Outsourced
Automated Telephone Payments (ATP)	Outsourced
Web Payments	Outsourced
Keyhaven River Pin Entry Devices (PEDs)	Outsourced
Agent Referred Payments (ARP)	Work in Progress
Keyhaven River Telephone Payments	Work in Progress

3.3 The project team continues to engage with third party service providers to obtain confirmation of PCI DSS accreditation annually.

3.4 Guidance has been provided to officers involved in card payment processes outlining their roles and responsibilities regarding PCI DSS compliance.

4. DIFFICULTIES ENCOUNTERED WITH PCI COMPLIANCE

4.1 Historically, when taking telephone payments customers verbally provided their card details over the phone for agents to enter manually into the payment system. This

practice meant that cardholder data entered NFDC systems and increased the security protocols required to be PCI compliant.

4.2 In January 2023 a new Agent Referred Payments (ARP) system was implemented whereby customers calls are transferred/forwarded to a secure payment line where the customer enters their card details using their telephone keypad. The secure payment line is hosted and owned by a PCI compliant third-party service provider and cardholder data never enters NFDC systems.

4.3 This system operates as an “end call” solution. Once the call is transferred to the payment line it cannot be retrieved if the customer is struggling with their payment.

4.4 Since going live there has consistently been around a 20% failure rate for this type of payment. The main reason for the payment failure is due to the customer entering invalid card details or not entering # to proceed with their payment.

4.5 To support vulnerable customers the Executive Management Team (EMT) approved the use of an assisted payment form to complete telephone payments, with customers providing their card details verbally. This has been implemented as a temporary solution whilst alternative PCI compliant options are investigated, such as a “mid-call” solution that would allow the NFDC officer to retrieve calls where the customer is struggling to help guide them through the process.

4.6 Officers have been issued with guidance advising them that the assisted payment form is only to be used for vulnerable customers who are not able to use an alternative payment channel. Managers are able to monitor the use of the assisted payment form and track usage at an individual call agent level. No card details entered into the assisted payment form are retained by the Council. The majority of telephone payments continue to be taken using the PCI compliant ARP system.

4.7 Keyhaven River are unable to use the ARP system for telephone payments as their telephone line does not allow for call forwarding. ICT are in the process of moving Keyhaven River over to Teams for calls, which would offer this functionality. Telephone payment volumes at Keyhaven are very low.

5. NEXT STEPS

5.1 Continue to engage with NFDC officers involved in the payment process regarding their roles and responsibilities in ensuring PCI DSS compliance.

5.2 Continue investigations into alternative solutions for telephone payments for vulnerable customers.

5.3 Implement the ARP system for telephone payments at Keyhaven River once they have successfully migrated to teams.

6. FINANCIAL IMPLICATIONS

6.1 The development of an alternative ARP solution (such as mid-call) will incur project delivery costs. These costs will need to form the part of the ICT work programme.

7. CRIME & DISORDER / EQUALITY & DIVERSITY / ENVIRONMENTAL IMPLICATIONS

7.1 There are none.

8. DATA PROTECTION IMPLICATIONS

8.1 Any exposure of cardholder data without authorisation is considered a breach for both PCI and GDPR.

For further information contact:

Alan Bethune
Strategic Director Corporate Resources & Transformation
Section 151 Officer
023 8028 5001
Alan.bethune@nfdc.gov.uk

Naomi Baxter
Accountant
023 8028 5033
Naomi.baxter@nfdc.gov.uk