Audit Committee – 27 June 2025

Payment Card Industry Data Security Standard (PCI DSS) Update

Purpose	For information
Classification	Public
Executive Summary	This report sets out the status of Payment Card Industry Data Security Standard (PCI DSS) at New Forest District Council.
Recommendation(s)	**It is recommended that Audit Committee:** **1. Note the update provided in the report.**
Reasons for recommendation(s)	To update committee members on the current position regarding full PCI DSS compliance and the next steps.
Ward(s)	All
Portfolio Holder(s)	Councillor Jeremy Heron – Finance and Corporate
Strategic Director(s)	Alan Bethune – Strategic Director Corporate Resources and Transformation (Section 151 Officer)
Officer Contact	Paul Whittles Assistant Director – Finance 02380 285766 paul.whittles@nfdc.gov.uk

Introduction and background

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. There are 4 PCI DSS compliance levels. New Forest District Council (NFDC) falls into Level 3: for merchants that process between 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.

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.

Progress made towards full PCI DSS Compliance

4. 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.

5. 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	Now taken via ARP

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

7. Guidance has been provided to officers involved in card payment processes outlining their roles and responsibilities regarding PCI DSS compliance and a training module is being developed within the council's Learning Management System.

Difficulties encountered with PCI Compliance

8. 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 to be PCI compliant.

9. The current Agent Referred Payments (ARP) system allows customers' calls to be 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.

10. 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.

11. When the "end call" solution was introduced, 20% of payments failed. The main reasons for the payment failure are due to the customer entering invalid card details or not entering # to proceed with their payment.

12. 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 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.

13. The "end call" failure rate has reduced to 14%, partly as a consequence of this action.

14. Officers have been issued with guidance advising them that the assisted payment form is only to be used in exceptional circumstances 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 significant majority of telephone payments continue to be taken using the PCI compliant ARP system.

15. Previously Keyhaven River were unable to use the ARP system for telephone payments as their telephone line did not allow for call forwarding. Last winter they were moved over to Teams for calls which allows for this functionality, however a decision was made for ARP payments to taken by the Environmental Enforcement and Amenities team instead. Telephone payment volumes at Keyhaven are very low and the current process is considered appropriate.

Next Steps

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

17. Complete the setup of a PCI DSS training module on the Learning Management System.

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

Financial and resource implications

19. The development of an alternative ARP solution (such as mid-call) will incur project delivery costs. These would need to form part of the ICT work programme with resources made available and approved in line with financial regulations.

Legal implications

20. There are no legal implications arising as a result of the recommendations in this report.

Risk assessment

21. With an element of manual intervention there remains a risk of data misuse. However, due to the existing controls in place, no significant risks have been identified at this time.

Environmental / Climate and nature implications

22. There are no environmental or climate and nature implications as a result of this report.

Equalities implications

23. There are no equality matters arising as a result of this report.

Crime and disorder implications

24. Ensuring the council is compliant reduces the risk of fraud.

Data protection / Information governance / ICT implications

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

Appendices:

None

Background Papers:

None