AUDIT COMMITTEE – 31 MAY 2022

PCI DSS UPDATE

1. RECOMMENDATIONS

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

2. INTRODUCTION

2.1 The payment card industry data security standards (PCI DSS) are a set of technical and operational requirements designed to ensure that all organisations that store, process or transmit cardholder data maintain payment security.

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 Non-compliance can lead to termination of the relationship with the bank or an increase in the transaction fees. It can also lead to large fines and penalties.

3. BACKGROUND

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

3.2 Payment Service Providers (PSP's) are companies that store, process or transmit cardholder data on behalf of another entity.

3.3 Third Party Service Providers (TPSP) are organisations that provide a service that has access to the Cardholder Data Environment. As a result, the third party needs to be PCI compliant and provide evidence of this compliance.

3.4 The following table details the payment channels, PSP's and TPSP's currently utilised at NFDC;

Payment Channel	PSP	TPSP
Card-present (CP) payments taken using Pin Entry Devices (PEDs) at: • Information offices • Keyhaven river • Car parking machines	• Information offices – Stripe • Keyhaven river – Worldpay • Car parking machines – Till Payments and AIB	• Information offices – Heycentric • Car parking machines – Parkeon
Telephone Payments (MOTO) CNP payments taken over the telephone: • By NFDC personnel • Automated telephone payments (ATP) system	• TNS (Mastercard) and Worldpay	• NFDC personnel - Business World • ATP - CivicaPay
E-commerce Card-not-present (CNP) payments over the internet	• TNS (Mastercard) and Worldpay	• Business World

4. DIFFICULTIES ENCOUNTERED WITH PCI COMPLIANCE

4.1 A project team, including Finance and ICT representatives was set up during 2021/22, with progress being made on the criteria outlined at 2.2.

4.2 In January 2022 Mastercard gave notice that they were retiring their payment gateway and therefore withdrawing their services as PSP for NFDC with the following deadlines:

i. CP transactions – 30th April 2022.

- NFDC has moved from Mastercard/Worldpay and Business World to Stripe and Heycentric for information office payments. This went live on 26th April 2022.

ii. MOTO – October 2022

iii. E-commerce – January 2023

4.3 The changes detailed in 4.1 and 4.2 will change NFDC's cardholder data environment (CDE) and therefore once again changes the scope for PCI compliance.

5. NEXT STEPS

5.1 A strategic review of financial systems, which will include payment systems for CP and CNP transactions is currently underway. PCI compliance will be considered as part of this review and during any procurement process for new PSP's and TPSP's. To work towards compliance, we will ensure that any system we procure is Point to Point Encrypted (P2PE) and listed as a PCI DSS validated solution.

5.2 The project team (which had to be reassigned to deliver the new payment gateway services at relatively short notice) will engage with our bank and third party service providers, as we will require appropriate evidence of PCI compliance from these services.

5.3 We will update our own policy and processes to ensure our practices are in keeping with PCI compliance. This will include a training package for officers who are involved in the taking of payments to give clarity on the do's and don'ts when it comes to taking payments.

6. FINANCIAL IMPLICATIONS

6.1 There are likely to be implementation costs associated with switching suppliers because of Mastercard's decision to retire their payment gateway. It is envisaged these costs will be met within existing budgets.

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
Executive Head Financial and Corporate Services
Section 151 Officer
023 8028 5001
Alan.bethune@nfdc.gov.uk

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