Payment Card Industry Data Security Standard and Tender in respect of Payment Services

Report of Cllr Richard Wenham, Executive Member for Corporate Resources (richard.wenham@centralbedfordshire.gov.uk)

Advising Officers: Chief Information Officer (stephan.conaway@centralbedfordshire.gov.uk), Chief Finance Officer, (charles.warboys@centralbedfordshire.gov.uk), Director of Improvement and Corporate Services, (deb.broadbent-clarke@centralbedfordshire.gov.uk); and Ralph Gould, Head of Financial Control, ralph.gould@centralbedfordshire.gov.uk, Tel: 0300 300 6779

This report relates to a Key Decision

Purpose of this report

1. To explain the actions proposed to achieve practical compliance with the Payment Card Industry – Data Security Standard (PCI-DSS).

2. Ensure best value is obtained from the suppliers of systems that enable the Council to obtain and process electronic payments from local taxpayers, tenants and other service users.

RECOMMENDATIONS

The Executive is asked to:

1. authorise the Chief Information Officer and Chief Finance Officer, in consultation with the Executive Member for Corporate Resources, to make contract awards in respect of the tender for payment services.
Overview and Scrutiny Comments/Recommendations

3. The implementation of the Council’s IT strategy to deliver digital transformation across the Council’s services was reviewed at the 15 December 2015 meeting of the Corporate Resources Overview and Scrutiny Committee. Members commented on the need to ensure that all customers should have a range of choices to transact with the Council. Members also expressed a desire to ensure security and cost savings remained a focus for the Council. The financial impact of increases in the costs associated with taking payments by debit and credit cards were detailed in the draft Budget 2016/17 and Medium Term Financial plan which were considered by the Corporate Resources O&S Committee on 2 February 2016 and subsequently approved by the Council.

4. The security requirements relating to the PCI-DSS are one element of the overall Council’s IT security and transformation activity and as such it is not proposed to take this report to the Corporate Resources O&S. However, the overall IT Strategy is subject to ongoing review by the Corporate Resources O&S and a report on digital transformation, with a focus on IT security and cost saving measures, is to be made to the 28 June 2016 meeting of that Committee.

Background information

5. Taxpayers and service users expect to be able to make payments to the Council by credit or debit card. Various systems from external suppliers are needed to capture and process card payments. Where any organisation takes payment by debit and credit cards, the companies issuing the cards require the organisation to comply with the Payment Card Industry – Data Security Standard (PCI-DSS).

6. Annually the Council collects 140,000 payments paid by either credit or debit cards. In line with the national picture the vast majority of transactions relate to Visa Debit cards (83%). A similar number of transactions, made predominantly by Housing tenants and Council taxpayers, are processed at Post Offices and other retail outlets using customer payment cards which are issued by a service provider on behalf of the Council. Whilst the processes for credit and debit card transaction are subject to PCI-DSS requirements the customer payment cards are not within the scope of the card industry requirements.

7. The compliance and operational issues related to modern payment methods apply to varying extents across the Council. Any changes in processes and suppliers will impact to some extent on all Council Directorates. Facilitating convenient and modern ways to collect income is important for service users, tenants and taxpayers.
The provision of the various payment options involves back office support and expenditure on service providers as well as external and internal assurance and compliance activities. New payment methods are continually being implemented, such as mobile banking applications for smart phones, and Council services aspire to provide a wider range of payment options, such as collecting mobile payments in the Housing service.

**PCI – DSS Compliance**

8. The PCI-DSS, currently comprising 12 requirements and over 200 controls, is intended to ensure that any Card Holder Data obtained to effect a payment is secure. The card companies can impose fines for non compliance with the PCI-DSS and can prevent an organisation accepting cards. The Council, supported by an independent security assessor, carries out an annual self assessment of PCI –DSS compliance.

9. The IT and Finance services have been identifying options to de scope as much of the payment processes as is reasonably practical from the Council's obligations under PCI-DSS. The approach identified is judged to be the most cost effective way to address PCI –DSS compliance. The objective is to ensure that, reflecting service requirements, as much as possible of the Council’s payment transactions are processed by systems and third parties that are assessed as fully compliant with the current PCI-DSS.

10. The table overleaf identifies the current position by payment channel (internet, telephone etc.) and indicates the options to either work towards full PCI-DSS compliance for the specific channel or de scope from the requirements by processing on third party systems. The majority of credit and debit card transactions (76%) are processed through payment services provided by a third party that are currently assessed as fully PCI-DSS compliant, specifically via the internet and touch tone telephone.

11. The other two payment channels involve either officers taking payment details over the telephone and accessing a third party system to progress the payment or the use of Chip and Pin card reading devices. To achieve and maintain full PCI-DSS compliance in respect of telephone transactions would require significant expenditure. Chip and Pin readers process a small number of transactions but are important payment options within specific services such as Registrars. The Chip and Pin machines currently in operation are not assessed as fully PCI-DSS compliant.
12. **Payment Transactions 2015**

<table>
<thead>
<tr>
<th>Type</th>
<th>2015 volume %</th>
<th>Processed within a fully compliant PCI-DSS environment</th>
<th>Options to de-scope PCI-DSS / achieve compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet via the Council Website</td>
<td>47</td>
<td>Yes</td>
<td>Currently de-scoped</td>
</tr>
<tr>
<td>IVR (Interactive Voice Response) telephone transaction touch tone</td>
<td>29</td>
<td>Yes</td>
<td>Currently de-scoped</td>
</tr>
<tr>
<td>MOTO (Mail Order Telephone Order) transactions where the cardholder is not present</td>
<td>22</td>
<td>No</td>
<td>Seek to Identify a cost effective and timely solution through a tender process. Any solution should meet both service and PCI-DSS requirements.</td>
</tr>
<tr>
<td>Chip and Pin Machine</td>
<td>2</td>
<td>No</td>
<td>Point-To-Point Encryption (P2PE) solution via upgrade with current supplier or source alternative provision</td>
</tr>
</tbody>
</table>

**Transaction Costs for Debit and Credit Cards**

13. The largest cost element of the card processing activity relates to transaction costs associated with the different types of cards. The transaction costs are currently charged monthly by the supplier of the payment service system and reflect a bundle of related costs. The bundled transaction costs include charges from the card scheme providers (e.g. VISA and MasterCard), the company processing the transactions (the Merchant Acquirer -e.g. Worldpay) and the Payment Service Provider (Capita). The most significant element of the overall transaction cost is the ‘interchange fee’ which is levied by the Card Company on the Acquirer.

14. In March 2015 Visa changed the interchange charge in respect of Non-Commercial Debit cards from a flat rate per transaction to a percentage of each transaction, subject to various caps. The overall impact of the changes increased the total annual transaction costs paid by the Council from £50k to £95k and the financial pressure of £45k was reflected in the 2016/17 Budget and MTFP.

**Procurement Requirements**
15. Contracts with the relevant service providers were entered into on the creation of the Council and have not been subject to any market testing since the original five year contract periods expired. The contracts have been extended on an annual basis.

16. Subjecting the current contracts to competition will present an opportunity to prove best value and allow suppliers to reflect pricing to the Council in line with a 4 to 5 year contractual commitment.

**Reason for decision**

17. The overall value of potential contracts arising from the Payment Services tender could exceed the £200,000 criteria for a Key decision. The Executives’ approval to delegate authority to award any relevant contracts arising from the tender is requested to ensure that Council officers can progress any new arrangements in a timely manner.

**Council Priorities**

18. The proposed actions will contribute to the development of a more efficient and responsive Council that operates systems and processes that meet customer requirements are secure and comply with external (PCI-DSS) requirements.

**Corporate Implications**

**Legal Implications**

19. In line with the Council’s Procurement rules participation in the payment service framework tender will market test existing service providers and facilitate compliance with PCI-DSS requirements. Whilst none of the individual existing service suppliers are paid in excess of the £200,000 annual criteria for a Key Decision, the overall annual tender value given the number of Lots could exceed £200,000. This report requests that the Committee authorise the Chief Information Officer and Chief Finance Officer to make any contract awards in respect of the tender for payment services.

**Financial and Risk Implications**

20. In total the annual cost of providing the various payment methods outlined above is approximately £250,000 per annum which reflects a number of suppliers’ transactions costs, system licences and system upgrades.

21. The cost of achieving full PCI –DSS compliance is difficult to quantify, particularly as the technology and compliance requirements continue to change. The cost to the Council, relative to the small number of
payment transactions involved, of achieving full PCI-DSS compliance under the current service arrangements is judged as being prohibitively expensive. As outlined above the IT and Finance service have been identifying options to ideally de-scope payment channels from the PCI-DSS or where this is not practical, work towards compliance within existing budgets.

22. This area is subject to significant and rapid changes in technology, compliance requirements, transaction charges and payment methods. The Council’s preferred payment method for taxes, rents and other services is Direct Debit and this option is promoted extensively. Overall payments by card comprise less than 10% of all payments received by the Council but are important methods for services to collect income, particularly in respect of often hard to collect amounts. Withdrawing any of the card payment methods from the Council’s services would potentially impact on reputation, cash flow and cost especially if other methods of payment were used, such as cheques.

23. The issues outlined above are common to all local authorities and there are many options available to provide payments services. Shropshire Council has arranged a payment services tender framework which will invite tenders under an OJEU procedure for a series of Lots intended to elicit solutions for the varying requirements of local authorities. By participating in the initial tender with Shropshire Council all the Council’s existing contracts will be market tested and it is anticipated that a range of alternative payment service options can be considered that could progress the PCI-DSS strategy and the overall Digital Transformation plan.

24. Eight Lots will be included in the Invitation To Tender of which responses to the six Lots as listed in the table overleaf could in some combination, subject to evaluation, meet the Council's various requirements.

25. **Payment Services Tender - Relevant Lots**

<table>
<thead>
<tr>
<th>Lot</th>
<th>Payment Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Merchant Accounts</td>
</tr>
<tr>
<td>2</td>
<td>Payment Gateway Service</td>
</tr>
<tr>
<td>3</td>
<td>Maximum de-scope card acceptance service</td>
</tr>
<tr>
<td>5</td>
<td>Customer Payment Cards</td>
</tr>
<tr>
<td>7</td>
<td>IVR – Telephone Touch tone</td>
</tr>
<tr>
<td>8</td>
<td>Intelligent automated payment systems</td>
</tr>
</tbody>
</table>

26. A Payment Services procurement framework has been developed by Shropshire Council and a specialist card processing advisory service
with the initial set up costs met by Shropshire Council. Authorities participating in the initial Invitation to Tender contribute a participation fee of £500 and 20% of any actual savings achieved over current arrangements during the life of any contracts awarded. The invitation to tender was published in May 2016 and it is anticipated that results will be available during July 2016.

27. The Council’s business requirements are to both progress PCI-DSS compliance and to offer a cost effective up to date range of ways to make payments to the Council. The framework as developed is the only current payment services framework that could meet the Council’s requirements. The anticipated savings on existing arrangements are estimated by the Finance service to be in the order of 15% which under the framework would mean gross savings of approximately £30k p.a. before payment of £6k p.a. under the terms of the framework.

28. Identifying suitable opportunities to de scope PCI-DSS obligations as far as is practically possible would reduce the risks of financial penalties or withdrawal of services by card companies. The requirements for internal IT and Finance resource and specialist advice to complete ongoing PCI-DSS compliance assessments would also be reduced in line with the extent of the PCI-DSS de-scoping achieved.

**Equalities Implications**

29. The Council has a statutory duty to promote equality of opportunity, eliminate unlawful discrimination, harassment and victimisation and foster good relations in respect of the nine protected characteristics; age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

30. The Council currently offers a wide range of ways for taxpayers, tenants, customers and other service users to make payments. The proposed actions are intended to improve efficiency without reducing the number of payment options.

**Implications for Work Programming**

31. There are no implications on the work programme of the Overview and Scrutiny Committee or further reports which might be considered by Members.

**Conclusion and next Steps**
32. It is recommended that the Executive Committee delegate authority to the Chief Finance Officer and Chief Information Officer in consultation with the Executive Member for Corporate Resources to make contract awards in respect of payment services following the completion of the payment services tender.

Appendices

None

Background Papers

None