DECISION

# RIBBLE VALLEY BOROUGH COUNCIL
# REPORT TO POLICY AND FINANCE COMMITTEE

Agenda Item No 8

|  |  |
|---|---|
| meeting date: | 6 SEPTEMBER 2016 |
| title: | CIVICA ICON SYSTEM UPGRADE |
| submitted by: | DIRECTOR OF RESOURCES |
| principal author: | MARK EDMONDSON |

## 1 PURPOSE

1.1 To inform Committee of the requirement to upgrade our Civica Icon Payments System, in order to continue to meet the Payment Card Industry Data Security Standards (PCI DSS), and seek approval to complete the upgrade in early 2017.

1.2 Relevance to the Council's ambitions and priorities:

- ***Council Ambitions/Community Objectives/Corporate Priorities***

  Without the revenue collected from rates, council tax and sundry debtors we would be unable to meet the Council's ambitions, objectives and priorities.

## 2 BACKGROUND

2.1 The Council uses the Civica Icon Payments System to process income e.g. cash, card and internet payments.

2.2 The number of transactions made electronically and using payments cards continues to substantially increase each year.

2.3 Industry rules regarding security i.e. PCI DSS continues to develop and become more onerous each year.

2.4 Civica informed its customers that they would only support customers operating versions of their software that are less than two years older than the current version. (See Appendix A - Civica Icon – Bulletin June 2016).

2.5 We upgraded to version 14 (v14) of that software in March 2015 and the deadline for their support for that version is to end 31 October 2017.

2.6 Civica have informed all customers that they must upgrade to version 16 (v16) of the software by 31 March 2018 to maintain PCI DSS compliance.

2.7 The payment card industry has recently introduced contactless payments and all new point of sales devices must accept payments by this method as of 1 January 2016. Full implementation for contactless payments is due by 1 January 2020.

## 3 ISSUES

3.1 Civica has announced a discount for customers that place an order before 30 September 2016 and a copy of our quote is attached at Appendix B.

3.2 To ensure that we remain PCI DSS complaint and supported by Civica we must upgrade to version 16 by 30 October 2017.

3.3 Orders placed after 30 September 2016 will incur an additional £1,000 in implementation costs for the upgrade from v14 to v16, an additional £1,500 for the initial licence for P2P encryption and an additional £840 per annum in annual charges.

## 4 RISK ASSESSMENT

4.1 The approval of this report may have the following implications:

- Resources – The cost of upgrading the payment system and chip and pin devices is £13,957. This could be funded from the new burdens Council Tax Support earmarked reserve. There would be additional annual charges of £1,700 per annum which would need to be added to our revenue budget for software maintenance. Failure to place an order before 30 September 2016 will result in these charges increasing by £2,500 and an additional £840.00 per annum.

- Technical, Environmental and Legal – In order to maintain our PCI DSS compliance we must upgrade to v16 before 31 March 2018. Furthermore v14 of the software will no longer be supported from 31 October 2017.

- Political - None

- Reputation – Taxpayers and residents expect to be able to make payments electronically both safely and securely. Failure to maintain our PCI DSS compliance would risk sever reputational damage if a breach was to occur.

- Equality and Diversity – Giving taxpayers and residents multiple ways to make payments to the Council helps to meet our Equality and Diversity requirements.

## 5 RECOMMENDED THAT COMMITTEE

5.1 Approve the upgrade of the Civica Icon Payments System from v14 to v16 at the discounted rate for orders placed before 30 September 2016.

HEAD OF REVENUES AND BENEFITS DIRECTOR OF RESOURCES

PF42-16/ME/AC
24 August 2016

For further information please ask for Mark Edmondson

Appendix A

# Civica ICON – Bulletin June 2016

Welcome to this ICON bulletin which provides several key updates which will impact your organisation over the coming months.   Contained within is important information on:

- PCI DSS Version 3 – changes and impacts to your organisation.
- Software lifecycle and end of support dates for current and future ICON releases
- Contactless payments
- Non geographic number pricing

Should you have any queries, please contact our Support team in the first instance on 0300 456 0540.

## PCI DSS

### Key points

- All customers will need to upgrade to ICON version 16 in order to maintain PCI compliance. PCI deadlines are in place such that any client or Hosted systems which have not been upgraded will not be PCI compliant and as such will not be able to process payments.
- For PCI compliance, all Chip and Pin terminals will require TNSPay payment client to be upgraded to Version 5
- Timescales for the above are determined by your current ICON release but all customers should note there is an absolute and immoveable deadline of 31st March 2018 where all production systems must be at Version 16 for PCI compliance.
- The Hosted environment will move to PCI defined strong cryptographic protocols only in October 2017.  Support for TLS1.0 and 1.1 will not be available. TLS1.2 only will be supported.

### Background

PCI DSS has determined that SSLv3 and TLS1.0 are not considered strong cryptographic protocols.

Full details can be found at https://www.pcisecuritystandards.org/pdfs/Migrating_from_SSL_and_Early_TLS_-v12.pdf

### What is a cryptographic protocol?

In the broadest sense these are means to ensure the security of communication channels using encryption methods.  In the context of ICON, this concerns inbound and outbound web (browser) connections to and from your ICON environment.   It will also include Chip and Pin transactions using TNSPay payment client.

The PCI Security Council determined that vulnerabilities such as ‘Poodle’, ‘Heartbleed’ and ‘Freak’ were due to weaknesses within the protocols.    Organisations were encouraged to move to secure protocols by mid-2016. However, following industry feedback – the PCI SSC issued updated and revised sunset dates of June 2018.

The cryptographic protocols used during a web payment session will be determined by the browser and the server.   Simply disabling ‘insecure’ protocols without adequate customer communication would lead to website access being blocked and payments unable to be processed. Finding the balance between security and payment provision has been the challenge of the industry, PCI DSS and specifically Civica ICON.

Where is SSL or early TLS used within the ICON solution?

### Inbound from the Internet

If you are a Non Hosted customer, you are likely to allow inbound insecure protocols to your web payment environments via customer Internet access to Webpaypublic, Estore or Paylink.

If you are a Hosted customer, SSLv3 Internet traffic into the Hosted environment was disabled in October 2014 (removing the most 'at risk' factors). TLS1.0 is currently allowed into the data centre as to deny this would block a significant proportion of customer payment traffic.

### Outbound to TNS

Currently both TNS's client software and their data centre gateway use SSL as the cryptographic protocol. Migration to a new Mastercard Gateway is required for all payments – including MOTO, E-commerce and Cardholder present.

What does my organisation need to do to obtain PCI DSS compliance?

- For Hosted customers, Civica will manage the process of disabling all inbound 'insecure' browser traffic – no changes will be required by our customers (though note that you will need to inform your end customers/citizens) – Civica intends to undertake this in October 2017.
- Customers must upgrade to version 16 where support for a new Mastercard Gateway is provided (and only secure protocols are supported). Civica has revised its roadmap to ensure all customers can migrate to a PCI DSS compliant environment for all payment types by the required deadline.
- Customers must upgrade to version 5 of TPPC for all chip and pin devices (only PCI defined secure protocols are supported at this release).
- If you are Non Hosted – contact your ICON Account Manager

What are the benefits to my organisation to upgrading?

- PCI DSS compliance
- Options for Point to Point encryption (P2PE) and tokenisation are available at V16. This provides opportunity to descope your cardholder present environment.
- Opportunity to reduce your SAQ requirement

What impact is there on the Civica ICON Roadmap?

Civica has revised its roadmap to ensure all customers can migrate to a PCI DSS compliant environment for all payment types by the required deadline. The timescales for release of our Hosted distribution offering have been moved to accommodate this PCI requirement, a summary is provided below:

| Release | Date | Contents |
|---|---|---|
| 16.1 | 01/09/2016 | PCI compliance via Mastercard Gateway and TNSPay payment client V5 support.<br>Point to Point encryption<br>Tokenisation |
| 16.2 | 29/12/2016 | Hosted distribution – also includes Hosted e-returns and full browser workstation replacement<br>PEG enhancements |
| 17.1 | 10/04/2017 | Hosted Bank Reconciliation |

### Next steps

Civica will issue a further detailed bulletin on all aspects concerning deprecation of Hosted support for TLS1.0/TLS1.1 in October 2017.

Customers should plan to upgrade to ICON Version 16 for ongoing PCI compliance. Timescales for upgrade are documented in the following section 'software lifecycle and end of support'. Costs are provided below.

### Upgrade from Release 12 to 16.1

For orders prior to 30th September 2016 - £12,000
For orders after 30th September 2016 – £14,000

### Upgrade from Release 14 or higher to 16.1

For orders prior to 30th September 2016 - £8,000
For orders after 30th September 2016 - £9,000

## Software lifecycle and end of support dates

For transparency and to enable customer planning, Civica has published its software lifecycle including 'end of support' dates.

| Software Version | Release Date | Security Updates end | End of support/Deadline to upgrade to supported release |
|---|---|---|---|
| 11 | 01/03/2012 | Ended | Ended |
| 12 | 01/10/2013 | Ended | 31/03/2017 |
| 14 | 01/03/2015 | 31/03/2017 | 31/10/2017 |
| 15 | 04/01/2016 | 31/12/2017 | 31/03/2018 |
| 16 | 01/09/2016 | 31/08/2018 | 28/02/2019 |
| 17 | 10/04/2017 | 31/03/2019 | 30/09/2019 |

## Contactless payments

### When do I need to move to contactless devices?

As of **1st January 2016**, all **new** POS deployments must accept contactless payments. This applies to newly acquired merchants, or merchants replacing their current POS devices.

Customers are not required to immediately replace their existing devices. However any new or replacement devices must accept contactless payments. The deadline for full contactless implementation is 1st January 2020.

What do I require to implement contactless?

Contactless payments are available on the Verifone VX820, these devices may be ordered via your ICON Account Manager. Please note that contactless requires an electrical power supply.

Civica has sought further clarification concerning the required version of TNSPay Payment client (TPPC). To ensure support for the Mastercard Paypass contactless scheme, **customers must run a minimum version of TPPC 2.1.12. This is a correction to a previous communication. Customers should not operate contactless on any lower version of TPPC software. A minimum version of Verifone's integrated payment architecture (VIPA) 4.0.4.7 is also required.**

Customers wishing to implement contactless on existing VX820 devices should contact the ICON Support team. A power supply will be required in addition to a software upgrade to TPPC 2.1.12 and possible VIPA update. A small charge will be applicable for the power supply.

Please note that merchants using POS devices with contactless must support high-value payments (£30). Any TNS Pay payment client configuration requirements will be provided by Civica upon device order.

PCI and PCI PTS Considerations

Contactless is available at your current ICON version and version 2.1.12 of TPPC. However PCI DSS Version 3.1 compliance may only be achieved at ICON version 16 and version 5 of TNSPay payment client.

The VX820 version 3 (as provided by Civica) is PCI PTS approved until April 2020.

Contactless and Kiosk

A separate communication will be issued to Kiosk customers.

Apple pay

Civica will support Apple pay at Version 16 and TPPC Version 5.

**Non Geographic Numbers**

Further to Ofcom changes in July 2015, organisations are required to publish the access and service charge to customers for use of telephony services to 084x numbers. After consultation with our supplier, Civica published rates to all customers. Unfortunately our supplier has recently communicated that the information provided to Civica for some customers was incorrect.

A further communication will follow.

Civica apologises for this error which was communicated in good faith

Appendix B

**Civica UK Ltd**
Second Floor
Garden Place
Victoria Street
Altrincham
Cheshire
WA14 1ET

Tel 0161 929 1810
Fax 0161 929 7322
e-mail icon@cvica.co.uk
Web: www.civica.co.uk

Ribble Valley Council

## ICON V16 Upgrade Services
## Discounted (for orders placed before 30th September)

| Description | Initial License | Implementation Services | Annual Charges |
|---|---|---|---|
| Upgrade from V14 to V16 (discounted for orders placed before 30th September) | | £8,000 | |
| P2Pencryption for under 10 Chip & Pin Devices | £2,500 | £2,500 | £650 |
| Tokenisation of up to 15,000 CHP transactions | | | £1,050 |
| **Total project cost (excl VAT)** | **£2,500** | **£10,500** | **£1,700** |

| | Set Up Cost (One Off) | Annual Subscription |
|---|---|---|
| 2 VX820 Chip and Pin Device (per device)<br>*Note that where VX810's are being replaced, the existing annual charge will continue and the Annual Subscription in this quotation will not apply.* | £960.00 | £0.00 |
| Chip & Pin Delivery Charge (per delivery) | £15.00 | £0.00 |
| **Total** | **£975.00** | **£0.00** |

### NOTES

- This quotation is subject to Civica's standard terms and conditions and is valid for 30 days.
- Payment of 'implementation services will be billed 'On Order' (an invoice will be issued payment within 14 days of receipt of the P/O)
- Civica's payment terms are 28 days from receipt of an invoice.
- Fees for the Implementation Services exclude expenses.
- All services to be taken within 12 months of receipt of a purchase order.
- ALL quotations are subject to final business approval within Civica, any issues or changes identified with the quotation you will be notified within 5 days.
- All prices exclude VAT.