Tempe
Internal Audit

Memorandum

TO: Mark Wittenburg, Information Technology Director
Tom Duensing, Financial Services Director
FROM: Bill Greene, City Auditor
CC: Andrew Ching, City Manager
Ken Jones, Deputy City Manager – Chief Financial Officer
Steven Methvin, Deputy City Manager – Chief Operating Officer
Rosa Inchausti, Deputy City Manager

DATE: August 17, 2021

SUBJECT: PCI Compliance

Purpose

The purpose of this consulting engagement was to update an existing document that captures information regarding the City's credit card environment to support the City's Payment Card Industry Data Security Standard (PCI DSS) compliance efforts.

Background

In June 2019, the City hired an external consultant to identify City business units processing credit card payments. This information (captured in an Excel document) was used to define the City's card data environment and address PCI DSS compliance requirements. The following table provides a high-level overview of the PCI DSS. This review focused on requirement #12 which are the standards addressing maintenance of an information security policy including vendor management.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS 3.2	Requirement 12	12.8.4	Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: (12.8) Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
PCI DSS 3.2	Requirement 12	12.8.5	Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: (12.8) Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

We selected these two areas since they provide the foundation for maintaining and implementing policies and procedures to manage merchant service providers.

Scope and Methods

The objective of this consulting engagement was to provide information as described in the purpose statement above. The work performed does not constitute an audit in accordance with *Government Auditing Standards*.

To achieve our stated objectives, we conducted the following review steps:

- Verified the card-processing status and obtained additional information about how they facilitate card transactions in areas that were identified as either "unknown" or "unverifiable" in 2019.
- When necessary, conducted follow-up phone calls with business units who required assistance responding to the survey or identified currently responsible party.
- Obtained from procurement staff a copy of the contracts with the vendors responsible for processing credit card transactions.
- Obtained from Cash Management Supervisor merchant identification numbers assigned to the areas that process credit card payments to ensure all new locations were included since the last review in 2019.

Results

We updated the external consultant's PCI credit card environment spreadsheet and provided the results to Information Technology and Finance management. Overall, we noted only a small change in the number of locations processing credit cards and 70% of department responses remained consistent. However, there was a significant reduction in the number of questions previously answered "unknown", which yielded additional information for PCI DSS compliance efforts.

Since 2019, 3 locations processing credit cards closed, and 4 new locations were identified. In 2019, 4 locations did not respond. In 2021, 3 locations did not respond. Only one location did not respond in either 2019 or 2020. There were 29 survey questions asked for each location identified. The number of questions with the answer of "unknown" decreased from 193 to 60. Specific changes to previous answers for the 29 questions ranged from 1 – 13 and are identified in Appendix A.

Our research into vendors used by the City to process credit card transactions demonstrated that additional follow up is needed. There is no centralized system to identify and manage which vendors are used, which contracts are active, and the unique PCI DSS requirements specific to each vendor. Contracts and a management process are needed to monitor which PCI DSS requirements are managed by the service provider and the City as specified in vendor contract terms.

We requested copies of all contracts from the Procurement Section for vendors processing City credit card transactions. Vendor names were initially provided by the primary contacts in their survey responses. The primary contacts identified 11 vendors responsible for processing credit card payments for the City of Tempe. However, based on internet research and our review of contracts, we noted multiple name changes of the credit card processing companies and several of the contracts provided were unrelated to the processing of credit cards. As a result, it appears the City may only be using 4 credit card processing vendors. We located contracts for two of these vendors, but they appeared to be expired. For the other two vendors, we were provided solicitation and award documents for one, but could not locate executed contract documents specifying PCI DSS requirements and the other vendor had no records.

The following table shows the number of departments each vendor is responsible for. The Fiserv contract had a provision entitled "Standards of Compliance" and stated, First Data will comply with PCIDSS and focus on the six areas outlined in the background section of this report.

Vendor Name (other names)	Number of Departments	Contract
Fiserv/First Data*	18 (45%)	2010 – PCI provision page 4 Section 10.4
ActiveNetwork (ActiveNet)	16 (40%)	2016 – PCI provision page 9 paragraph 13
Paymentus	3 (7.5%)	Solicitation and Award documents – PCI provision pgs. 96 and 110
Mercury/Global Payment Direct/WorldPay (penciled in)	2 (5%)	2010 – PCI provision page 11 Paragraph 31
Unknown/lack of Response	1 (2.5%)	Not identified

*According to Cash Management and Procurement staff, Fiserv was formerly Banc of America Merchant Services (BAMS). The contract provided for Fiserv was AccessNet Services Agreement dated – October 7, 2010 which specifies First Data Government Solutions ("First Data"). According to Procurement staff, RFP 14-14 which references PCI language and compliance requirements, was awarded to Bank of America which changed to FDS Holdings. PayPoint Addendum to AccessNet Services Agreement had RFP 14-14 penciled in on document. It appears the contract is expired and references another name.

During fieldwork, we noted that staff assigned to different areas (e.g. Procurement, Finance, IT and operating departments) were not clear on their roles and responsibilities.
This directly contributed to inefficiencies when gathering information and documents necessary for us to update the spreadsheet detailing the City's credit card environment. There are also no written policies and procedures addressing the topic areas reviewed (12.8.4 and 12.8.5).

Recommendations

1. Develop a policies and procedures detailing PCI DSS responsibilities and schedule regular working meetings to ensure task identification and assignment necessary for compliance with requirements 12.8.4 and 12.8.5.

2. Based on our review, the following tasks should be assigned:
    a. Consider centralizing and consolidating all credit card payments with one vendor to ensure continuity and understanding of the contracts and possibly negotiate cost savings.
    b. For locations that did not respond, follow up to obtain answers and update the spreadsheet. Assign someone the responsibility of keeping information current.
    c. Follow up and update all responses for questions with a data field populated with "unknown."
    d. Document and perform site surveys necessary to verify assets, interconnected switching, servers, network architecture and the data flow review/diagram to help ensure compliance with PCI DSS requirements.

Appendix A

				Resp Recvd?		Resp "unknown"		# of Answers Changed	Area of Change
	Department	**Vendor Name**	**Contract ?**	**2019**	**2021**	**2019**	**2021**	**#**	
1	Fire Department – Budget & Finance	Fiserv	Yes	Yes	Yes	0	0	0	
2	Customer Services – Utility Billing & Backup (General)	Fiserv	Yes	Yes	Yes	13	1	2	Remote card processing
3	Customer Services – Utility Billing (Legacy Water)	Paymentus	Yes	Yes	Yes	12	0	3	Imprint machines
4	Customer Services – Non-Utility Transactions	Fiserv	Yes	Yes	Yes	12	3	6	Remote/imprint machines
5	PD – Lobby/Records	Fiserv	Yes	No	No	N/A	N/A	N/A	
6	PD – Alarms	Fiserv	Yes	No	Yes	N/A	0	N/A	
7	PD – Front Desks	Fiserv	Yes	Yes	No	4	N/A	N/A	
8	PD – Leads Online	Fiserv	Yes	Yes	Yes	0	0	0	
9	PD – PIO Record Requests	Fiserv	Yes	Yes	Yes	0	0	0	
10	Tempe Center for the Arts – Concessions	N/A	N/A	Yes	Yes - Closed	2	N/A	N/A	
11	Tempe Community Services – Tempe Public Library – Accounts Window	ActiveNet	Yes	Yes	Yes	2	0	3	Face-to-face/mail/phone, manual and internet connected
12	Tempe Community Services – Tempe Public Library – Self-Checkout	Fiserv	Yes	Yes	Yes	2	0	0	
13	Tempe Community Services – Tempe Public Library – Online	Fiserv	Yes	N/A	Yes-new	N/A	0	N/A	
14	Parks & Recreation – Kiwanis Park	ActiveNet	Yes	Yes	Yes	8	1	5	Maill, e-mail, face-to-face mail/phone
15	Human Services – Cahill Senior Center	ActiveNet	Yes	Yes	Yes	0	0	13	Email, Remote, mail, phone
16	Rolling Hills Golf Course	WorldPay	Yes	No	Yes	N/A	3	N/A	
17	Ken McDonald Golf Course	WorldPay	Yes	No	Yes	N/A	3	N/A	
18	Pyle Adult Recreation Center	ActiveNet	Yes	Yes	Yes	0	0	0	
19	Community Development – Code Compliance	Fiserv	Yes	Yes	Yes	10	2	5	Face-to-face/ mail/phone, imprint machines, dial-out terminals

20	Internal Services – Tax and License Division	Fiserv	Yes	Yes	Yes	4	0	11	Face-to-face/mail/phone, internet connected
21	Public Works Department – Transportation Division	Fiserv	Yes	Yes	Yes	0	0	0	
22	Tempe History Museum Store	ActiveNet	Yes	Yes	Yes	1	1	12	Mail, e-mail, one-line, face-to-face/mail/phone
23	Tempe Municipal Court – Financial Services	Fiserv	Yes	Yes	Yes	1	0	8	Face-to-face/mail/phone, manual, standalone
24	Engineering	Fiserv	Yes	Yes	Yes	10	0	6	Remote card
25	City Clerk's Office	Fiserv	Yes	Yes	Yes	0	0	1	Electronic storage
26	Tempe Center for the Arts - Box Office	Fiserv	Yes	Yes	Yes	0	0	0	
27	McClintock Pool	ActiveNet	Yes	Yes	Yes	10	0	5	Mail, phone, e-mail
28	Kid Zone Enrichment Program	Paymentus	Yes	Yes	Yes	8	2	0	
29	Human Services – Diversion	N/A	N/A	Yes	Yes – closed	13	N/A	N/A	
30	Parks & Recreation - Front Desk (Note: Combined with Admin Office below)	ActiveNet	Yes	Yes	Yes - closed	9	N/A	N/A	
31	Community Development – Bldg Safety	No Response	No Response	Yes	No	3	N/A	N/A	
32	Parks & Recreation Services – Admin Office	ActiveNet	Yes	Yes	Yes	2	0	6	Face-to-Face mail/phone, Standalone, manual entry
33	Parks & Recreation – Escalante Comm Ctr	ActiveNet	Yes	Yes	Yes	9	0	4	Imprint, standalone
34	Parks & Recreation – West Side Multi-Generational Ctr	ActiveNet	Yes	Yes	Yes	9	0	8	Electronic storage, mail, e-mail, imprint machines, manual entry, 3rd party hosted terminal
35	Parks & Recreation – North Side Multi Gen Ctr	ActiveNet	Yes	Yes	Yes	19	0	2	Mail, e-mail
36	Fin Services – Acctg	N/A	N/A	Yes	Yes	0	0	0	
37	Human Services – Social Services	Paymentus	Yes	Yes	Yes	0	6	10	Electronic storage, internet, mail, paper form, online, standalone wall jack
38	Tempe Center for the Arts	Fiserv	Yes	Yes	Yes	3	0	1	Electronic storage
39	Edna Vihel Arts Center	ActiveNet	Yes	Yes	Yes	15	1	3	Mail, paper form

40	Tempe Transit Store	ActiveNet	Yes	Yes	Yes	12	1	3	3rd party hosted terminal; internet connected
41	Special Events	ActiveNet	Yes	No	Yes	N/A	12	N/A	
42	Tempe 311	ActiveNet	Yes	No	Yes	N/A	12	N/A	
43	On Line Recreation	ActiveNet	Yes	No	Yes	N/A	12	N/A	