OFFICE OF THE CITY AUDITOR
COLORADO SPRINGS, COLORADO

13-23
Colorado Springs Utilities E-Commerce Review

December 2013

OFFICE OF THE CITY AUDITOR
COLORADO SPRINGS, COLORADO

13-23
Colorado Springs Utilities E-Commerce Review

December 2013

Purpose

The purpose of this audit was to evaluate the adequacy and effectiveness of controls surrounding several areas of e-commerce activities within Colorado Springs Utilities. These areas included relevant Automated Clearing House (ACH) services, customer interfaces, and vendor interfaces. This audit also included a review of Colorado Springs Utilities interpretation of the Fair and Accurate Credit Transactions Act (FACTA) and the Colorado Open Records Act (CORA).

Highlights

We concluded that the majority of the controls tested were adequate and effective. We identified one observation and two opportunities for improvement.

To accomplish our audit objectives, we reviewed policies and procedures as well as interviewed management and staff to obtain an understanding of the internal control structure around e-commerce activities. The controls identified were reviewed against the Control Objectives for Information and related Technology (COBIT) 4.1 information technology (IT) industry best practices standard for adequacy.

It was noted that management's implementations of the processes reviewed in this audit were strongly influenced by customer need. It was obvious during the course of this review that the customers' best interest was heavily considered when making process decisions. Management frequently expressed concern for the customer's experience. Additionally, Colorado Springs Utilities was exceptional with regards to documenting their policies and procedures. In general, well documented policies and procedures reduce employee confusion allowing for more consistent and efficient operations.

Management Response

Colorado Springs Utilities management generally agreed with the observations presented. See detailed responses in the attached report.

Recommendations

1. Management should develop and document a process to monitor for fraudulent activities by individuals accessing files containing customer bank account information generated during the processing of physical checks.

Opportunity for Improvement

1. Management should consider providing the option for customers to create more complex passwords using special characters if cost effective.
2. Management should consider conducting a detailed analysis of the necessity of ongoing production data access granted to application developers and other IT staff.

City Council's
Office of the City Auditor
City Hall
107 North Nevada Ave. Suite 200
Mail Code 1542
Colorado Springs CO 80901-1575
Tel 719-385-5991
Fax 719-385-5699
Reporting Hotline 719-385-2387
www.SpringsGov.com/OCA

Office of the City Auditor
Public Report

Date: December 13, 2013

To: President King, President Pro-Tem Bennett, and Members of City Council

Re: 13-23 Colorado Springs Utilities E-Commerce Audit

We conducted an audit of the e-commerce services at Colorado Springs Utilities. The purpose of this audit was to evaluate the adequacy and effectiveness of controls surrounding several areas of e-commerce activities. These areas included relevant Automated Clearing House (ACH) services, customer interfaces, and vendor interfaces. The audit also included a review of Colorado Springs Utilities interpretation of the Fair and Accurate Credit Transactions Act (FACTA) and the Colorado Open Records Act (CORA).

We concluded that the majority of the controls tested were adequate and effective. We identified one observation and two opportunities for improvement and have listed the recommendations for each in the attached report.

As always, feel free to contact me if you have any questions.

Sincerely,

Denny L. Nester, MBA CPA CIA CGFM CFE CGAP

Cc: Jerry Forte, Chief Executive Officer
Bill Cherrier, Chief Planning and Financial Officer
Carl Cruz, Chief Customer and Corporate Services Officer
Kathleen Solano, General Manager, Customer Revenue and Service Department
Kim Girling, Manager, Customer Solutions
Joe Hickert, Interim General Manager, Information Technology Services Department
Charise Swanson, Manager, Compliance and Risk Mitigation Services
David Maier, Manager, Enterprise Risk Management Services
Patricia Van Meter, Lead Analyst, Enterprise Risk Management Services

City Council's Office of the City Auditor
City Hall ◆ 107 North Nevada Avenue ◆ Suite 200 ◆ Mail Code 1542
Colorado Springs CO 80901-1575
Tel 719-385-5991 ◆ Fax 719-385-5699 ◆ Reporting Hotline ◆ 719-385-2387
www.SpringsGov.com/OCA

Office of the City Auditor

Colorado Springs Utilities
E-Commerce Audit

Office of the City Auditor

Colorado Springs Utilities
E-Commerce Audit

REPORT DETAILS

PURPOSE AND SCOPE

The purpose of this e-commerce services audit was to evaluate the adequacy and effectiveness of:

- Application controls concerning ACH services
- Password and access controls on customer facing interfaces
- Controls relevant to the integrity, confidentiality, and compliance with internal policies concerning data transmitted to and from vendors

This audit also included an evaluation of how personally identifiable information (PII) protections as indicated in FACTA and CORA are implemented.

BACKGROUND

Colorado Springs Utilities focused on providing high quality customer service. Customers were able to access their account information online as well as to view and pay their bills online. Credit card and direct bank withdrawal payments were processed by third party partners.

In general, electronic commerce, or e-commerce, is the buying and selling of goods via an electronic medium. Customers paying bills online is a form of e-commerce as well as the interactions between Colorado Springs Utilities and the third parties to process such payments.

The Control Objectives for Information and related Technology (COBIT) is an overarching business and management framework for governance and management of enterprise IT developed by the IT Governance Institute. COBIT provides IT professionals with a guide of globally accepted industry control best practices. The practices outlined in the COBIT framework were used in this audit to evaluate the adequacy of the controls reviewed.

COMMENDABLE PRACTICES

Management's implementations of the e-commerce processes were strongly influenced by customer satisfaction. During the discussions with the auditor, management frequently expressed concern for the customer's experience. Additionally, Colorado Springs Utilities was exceptional with regards to documenting their policies and procedures. In general, well documented policies and procedures reduce employee confusion allowing for more consistent and efficient operations.

CONCLUSION

We concluded that the majority of the controls tested were adequate and effective. We identified one observation and two opportunities for improvement, which are detailed in the body of the report.

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

OBSERVATION 1 – LACK OF MONITORING OF ACCESS TO FILES CONTAINING CUSTOMER BANK ACCOUNT INFORMATION

Access to stored customer bank account information generated during processing of physical checks was not being monitored.

Anytime sensitive data is stored, there is the possibility of it being misused. Sensitive data, such as customer bank account information, could be used in identity theft or for other fraudulent activities. To prevent the fraudulent use of sensitive data, access to the data is typically limited to personnel who need it to perform their job responsibilities. Additionally, the access to the sensitive data should be logged so that it can be monitored for suspicious activity and to provide accountability of the individuals who are accessing it.

Colorado Springs Utilities accepted checks via the mail and other sources from their customers as payment for services provided. To process these checks efficiently, they were scanned for electronic processing. The customers' banking information (bank routing number, bank account number, and name) was then compiled and stored in a file on Colorado Springs Utilities computer systems. Fourteen information technology personnel had direct access to these files. This access was approved by the data owners since it was understood that the IT personnel needed access to perform their routine job responsibilities. However, access to the files was not being monitored and there were no policies in place indicating that such access should be monitored.

AUDITOR'S RECOMMENDATION

Management should develop and document a process to monitor for fraudulent activities by individuals accessing files containing customer bank account information generated during the processing of physical checks.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with the recommendation. Access to such information is currently limited to personnel whose job responsibilities are to provide support within our Customer Information System (CIS). Information Technology Services (ITS) will implement system and database audit logging within the CIS to track ITS personnel access to customer banking information in order to minimize the risk of fraudulent activities and to ensure access is directly related to the performance of their job responsibilities. In addition, ITS will partner with Compliance & Risk Mitigation Services (CRM) to create a process to review these logs, conduct the required verification, document the results, and take appropriate action. ITS and CRM plan to have their respective solutions implemented no later than April 30, 2014.

OPPORTUNITIES FOR IMPROVEMENT

OPPORTUNITY FOR IMPROVEMENT 1 – UNABLE TO USE SPECIAL CHARACTERS FOR *MY ACCOUNT* PASSWORDS

Customers were unable to use special characters when creating passwords for their online account.

Customers utilized a web interface referred to as "My Account" to gain online access to their account information as well as to view and pay their bills online. In order to gain access, customers were required to create a username and password for their account. The password they would create was required to have at least one uppercase letter, one lowercase letter, one number, be 6-12 characters in length, and not contain any special characters. It was a common industry practice to allow or require passwords to contain special characters to increase the complexity of a user's password. While the password complexity requirements being enforced appeared to be sufficient, not allowing the use of special characters reduced the maximum potential strength of the password.

AUDITOR'S RECOMMENDATION

Management should consider providing the option for customers to create more complex passwords using special characters if cost effective.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with the recommendation. As of October 3, 2013, customers have the option to create a more complex password by using six special characters (!, @, #, $, %, ^) when changing or creating their password for My Account.

OPPORTUNITY FOR IMPROVEMENT 2 – DEVELOPERS AND OTHER IT STAFF HAD ONGOING ACCESS TO PRODUCTION DATA

Application developers and other IT staff had ongoing access to production data used for e-commerce activities.

Application developers are not commonly provided ongoing access to production data due to their intimate knowledge of the application system's functionality. Such knowledge increases the risk of them exploiting the data. While general IT staff may not have this level of understanding, they may still be able to exploit the data. However, there are special circumstances where application developers and other IT staff need to have temporary access to production data. An example of such a situation is when an emergency change needs to be made to the system or data.

It was determined that application developers and other IT staff had ongoing access to production data. Management had previously approved this ongoing access to ensure timely support of e-commerce activities. Management was concerned that implementing a temporary access process would unacceptably increase support response time.

AUDITOR'S RECOMMENDATION

Management should consider conducting a detailed analysis of the necessity of ongoing production data access granted to application developers and other IT staff.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with the recommendation and has completed the analysis to confirm only required support personnel have access. As a result of the analysis, two IT staff members had their access removed leaving twelve who require on-going access per their job responsibilities.

CITY COUNCIL'S OFFICE OF THE CITY AUDITOR

COLORADO SPRINGS, COLORADO

About our Office

The mission of the Office of the City Auditor is to provide City Council with an independent, objective and comprehensive auditing program for operations of the City. Our auditing program includes:

- Evaluating the adequacy of financial controls, records and operations
- Evaluating the effectiveness and efficiency of organizational operations
- Providing Council, management and employees objective analysis, appraisals, and recommendations for improving systems and activities

The Office of the City Auditor is responsible for auditing the systems used by the City of Colorado Springs and its enterprises, including Colorado Springs Utilities. We perform a variety of audits for these entities, including financial audits, performance audits, contract audits, construction audits, and information system audits. We also perform follow-up on a periodic basis to monitor and ensure management actions have been effectively implemented.

Authorization and Organizational Placement

Our audits are conducted under the authority of Chapter 1, Article 2, Part 7 of the Colorado Springs City Code, and more specifically parts 703, 705 and 706 of the Code. The Office of the City Auditor is structured in a manner to provide organizational independence from the entities it audits. This independence is accomplished by the City Auditor being appointed by and reporting directly to the City Council.

Audit Standards

The audit was conducted in a manner that meets or exceeds the International Standards for the Professional Practice of Internal Auditing, a part of the Professional Practices Framework promulgated by the Institute of Internal Auditors, with the exception of the requirements under standards 1312 and 1321 to obtain an external quality assurance review once every five years. We do not believe this non-compliance impacted the quality of our audit.

The audit included interviews with appropriate personnel and such tests of records and other supporting documentation as deemed necessary in the circumstances. We reviewed the internal control structure and compliance tests . Sufficient competent evidential matter was gathered to support our conclusions.

City Hall ◆ 107 North Nevada Avenue ◆ Suite 200 ◆ Mail Code 1542
Colorado Springs CO 80901-1575
Tel 719-385-5991 ◆ Fax 719-385-5699 ◆ Reporting Hotline ◆ 719-385-2387
www.SpringsGov.com/OCA