REDW LLC

The Rogoff Firm

CERTIFIED PUBLIC ACCOUNTANTS | BUSINESS & FINANCIAL ADVISORS

BERNALILLO COUNTY

NEW MEXICO

Internal Audit

Online Payment System

May 2011

REDW LLC
The Rogoff Firm
CERTIFIED PUBLIC ACCOUNTANTS | BUSINESS & FINANCIAL ADVISORS

Bernalillo County Internal Audit
Online Payment System

Executive Summary

SUMMARY OF PROCEDURES

REDW performed an internal audit of the Bernalillo County Online Payment System. Bernalillo County accepts online payments for property taxes in the Treasurer's Department, document fees in the Clerk's Office, and vendor registration fees in the Purchasing Department. Our internal audit focused on evaluating policies and procedures over online payments and establishing whether internal controls over the online payment system are adequate and operating as designed.

In order to determine whether policies and procedures are followed and if adequate controls are in place over the online payment system at Bernalillo County, we performed the following:

- Read the policies and procedures for the online payment system;
- Read the policies and procedures for daily cash reconciliation and cash drawer balancing;
- Interviewed relevant department personnel;
- Performed walk-through procedures of the online payment process, including daily cash reconciliations, for the Treasurer's Department, Clerk's Office, and Purchasing Department;
- Requested the Access Security Matrix to view employee access and verify compliance with policies and procedures;
- Performed the following security tests on the Online Payment System;
    - Ensured any pages requiring customer input or displaying any sensitive information were secure hypertext language pages (https);
    - Accessed the properties of the secure web pages to evaluate the SSL Certificate for valid certificate authority, name accuracy, adequate level of encryption (128 bit), and current date;
    - Determined if any information entered into online forms was cached or if the system used the "disable content on submit" function;
    - Determined if the system used a session idle-timeout on the transaction pages and if it did how long the idle-timeout was;

  - Evaluated the content of the credit card receipt webpage to determine whether it contained any sensitive information and if the credit card number was masked out except for the last 4 digits;
  - Evaluated the content of an automatic email receipt sent to a customer to determine if it contained sensitive information.
- Selected a sample of daily cash reconciliations and performed the following procedures;
  - Verified the amount of payment for the day's online payments reconciled to the bank statement;
  - Verified the amount deposited to the vendor agreed to the bank statement.

SUMMARY OF OBSERVATIONS AND RECOMMENDATIONS

We noted the following:

- **Access security matrix**—We were unable to obtain an access security matrix for Global Basket system. Access controls are vital to the security of the system and should be documented and actively maintained and monitored.
- **Session time out**— The session time out for Global Basket of three hours is too long. The purpose of an idle-time out is for security reasons, such as not leaving sensitive information up on the computer screen for other people to see. Three hours is too long and we recommend shortening the session time out to 60 minutes or less.
- **Data availability**— Information purchased online is emailed to the purchaser via a link. The email states that the link is only valid for seven days, but the link we received was valid for months after the date of purchase. We recommend the schedule time-outs be initially verified and periodically verified during routine system maintenance.

* * * * * * *

Further detail of our purpose, objectives, scope, procedures, observations, and recommendations is included in the internal audit report. In that report, management describes the corrective action being taken for each observation.

REDW LLC

May 11, 2011

Bernalillo County Internal Audit
Online Payment System

Table of Contents

REDW LLC
The Rogoff Firm
CERTIFIED PUBLIC ACCOUNTANTS | BUSINESS & FINANCIAL ADVISORS

Bernalillo County Internal Audit
Online Payment System

Report

Introduction

We performed the internal audit services described below solely to assist Bernalillo County in evaluating and testing compliance with online payment policies and procedures to ensure the accuracy, security, and integrity of credit card and eCheck payments to the County. Bernalillo County accepts online payments for three of the County's departments. The Bernalillo County Treasurer's Office, the property tax collector for the County of Bernalillo, accepts online payments for property taxes. The Bernalillo County Clerk's Office accepts online payments for the purchase of Public records. The County Purchasing Department accepts online payments from vendors who wish to bid on goods and services. Our services were conducted in accordance with the *Consulting Standards* issued by the American Institute of Certified Public Accountants, generally accepted government auditing standards, and the terms of our contract agreement for internal audit services. Since our procedures were applied to samples of transactions and processes, it is possible that significant issues related to the areas tested may not have been identified.

Although we have included management's responses in our report, we do not take responsibility for the sufficiency of these responses or the effective implementation of any corrective action.

Purpose and Objectives

Our internal audit focused on evaluating policies and procedures over the online payment system and testing compliance with online payment system policies and procedures.

Scope and Procedures Performed

Interviews: In order to gain an understanding of the processes and controls over the online payment system, we interviewed the following personnel:

- Lisa Sedillo-White, Purchasing Director
- Fidel Bernal, Deputy County Treasurer
- David Salas, Clerk's Office, IT Project Management Consultant
- Carol Thomas, Clerk's Office, Administrative Officer III
- Nader Kahlil, IT Web Support
- David Martell, Acting Application Manager

In order to understand online payment system policies and procedures:

- We read policies and procedures for the online payment system.
- We read policies and procedures for daily cash reconciliation and cash drawer balancing.

We performed the following testwork:

- Performed walk-through procedures of the online payment process, including daily cash reconciliations and end of day bank balancing, at each of the three departments utilizing the online payment systems; the Treasurer's Department, Clerk's Office, and Purchasing Department;
- Requested the Access Security Matrix to view employee access, assess the employee access controls, and verify compliance with policies and procedures;
- Performed the following security tests on the Online Payment System;
  - Ensured any pages requiring customer input or displaying any sensitive information were secure hypertext language pages (https);
  - Accessed the properties of the secure web pages to evaluate the SSL Certificate for valid certificate authority, name accuracy, adequate level of encryption (128 bit), and current date;
  - Determined if any information entered into online forms was cached or if the system used the "disable content on submit" function;
  - Determined if the system used a session idle-timeout on the transaction pages and if it did how long the idle-timeout was;
  - Evaluated the content of the credit card receipt webpage to determine whether it contained any sensitive information and if the credit card number was masked out except for the last 4 digits;
  - Evaluated the content of an automatic email receipt sent to a customer to determine if it contained sensitive information.
- Selected a sample of daily cash reconciliations and performed the following procedures;
  - Verified the amount of payments for the day's online payments reconciled to the bank statement;
  - Verified the amount deposited to the vendor agreed to the amount deposited on the bank statement.

OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

We identified the following weaknesses relating to the Bernalillo County online payment system.

1) Access security matrix

Employee access controls are helpful in preventing unauthorized system use. We were unable to obtain a list, or spreadsheet of who has what level of access to Global Basket servers, systems and applications. The IT Department should use this list as a tool to ensure the employee access controls are effective and performing as designed.

Recommendation

We recommend access controls be documented, maintained and monitored by the IT Department.

Management Response

The IT Department has created an Online Payment System (Global Basket) Access Security Matrix that identifies “Group Access” by Employee Name, Type of Permission, and Server Type. The IT Department will ensure that access controls are documented, maintained, and monitored by the IT Department.

2) Session time out

Session time outs are a system control used to protect data. Most default session time outs are 30 minutes, but the Online Payment System session times out after three hours. The purpose of an idle-time out is for security reasons, such as not leaving sensitive information up on the computer screen for other people to see.

Recommendation

We recommend that shortening the session time out period to 60 minutes or less.

Management Response

Our resolution in moving forward is to have an authorized administrator from IT change the “Basket Timeout” parameter to reduce the session time from 180 minutes to 60 minutes for all Product Types. This reduction in session time reduces any risk of sensitive information displayed on the User’s screen for too long, and reduces the vulnerability of data.

3) Data availability

Information purchased online is emailed to the purchaser via a link. The policy states that the link is only valid for seven days. The link we received was valid for months after the date of purchase.

Recommendation

We recommend that scheduled time-outs are initially and periodically verified to ensure they are operating effectively.

Management Response

As of April 29, 2011, the Recording and Filing manager now has access via the front end Interface of EagleRecorder to change the duration (in hours) for the link to be available to the customer for 168 hours (7 days). This will be verified on a monthly basis by the Recording and Filing Manager and also be periodically verified by Tyler Technologies as well. In addition, Tyler Technologies is writing a script, which will go into effect on May 6, to expire all links that are currently available to customers that are beyond the original 7 day link expiration period from their purchase date by invalidating the links stored in the database.

* * * * * * *

This report is intended for the information and use of Bernalillo County management, the audit committee, members of the board of commissioners of Bernalillo County and others within the organization. However, this report is a matter of public record, and once accepted its distribution is not limited.

REDW LLC

May 11, 2011