



Fairfax County Internal Audit Office

Department of Tax Administration
Electronic Payments Audit
Final Report

February 2009

"promoting efficient & effective local government"

Background

County citizens can pay their taxes by using various electronic payment methods, such as credit cards, electronic checks and automatic installments. The county has an IT project in process to have a single provider, Govolution, for electronic bill presentment as well as payments. The Department of Tax Administration (DTA) utilizes a third party processor, Govolution, to process all the personal property tax payments and real estate tax payments that are paid by the credit card and e-check through the DTA Internet Web site. DTA uses the Velocity Payment System (VPS) to monitor, track and reconcile all the online payments that are processed by the Govolution. The personal property tax payments are stored in the Assessment and Licensing Information System (ALIS), and the real estate tax payments are stored in the Integrated Assessment System (IAS). DTA implemented an electronic fund transfer (EFT) program, which is a payment plan that allows taxpayers to prepay taxes or pay delinquent taxes through automatic installments debited electronically from their bank accounts. The county utilizes a third party processor, Metavante, to process all EFT program payments.

Executive Summary

Our audit found that controls over the processing of electronic payments and the manual and automatic updates to county systems were adequate and operating effectively. There was also proper segregation of duties between electronic payments processing and electronic payments accounting/reconciliation functions. We also determined that the posting of transactions and reconciliations of payment activity were accurate and timely. However, compliance with the county's Information Technology Security Policy 70-05.01 related to data transmission, account management, password and privacy, needs to be strengthened. The primary issues noted were:

- Data containing taxpayers' social security numbers and sensitive bank information, i.e. bank account number, was not encrypted during the transmission from the county to the Metanvente system.
- No formal access request form was in place for adding, changing and removing users in VPS and IAS.
- For the VPS, segregation of duties control was weakened by the system administrator also serving as an end-user.
- Both the IAS Oracle database and IAS application did not enforce users to create strong passwords, i.e. password must adhere to a minimum length and must be changed routinely.

Scope and Objectives

This audit was performed as part of our Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those standards

require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit covered the period of February through July 2008, and our audit objectives were to:

- Review the contract, service level agreement between vendor and Fairfax County departments (Department of Information Technology and Department of Tax Administration) and independent security control review reports to determine whether the vendor has controls in place to ensure electronic transactions processing are current, accurate, complete and indisputable.
- Determine whether the data transmission between vendor and county department is secure and reconciliations are performed to verify data completeness.
- Determine whether the electronic payments are processed timely, accurately and completely by the county financial systems.
- Determine whether transactions are protected from unauthorized modification and not to be fraudulent; and customers' information is protected from being disclosed without their consent.

Methodology

Our audit approach included a review and analysis of internal controls over electronic payments processed by the Govolution and Metanvente, as well as the contract and service level agreement between vendor and Department of Tax Administration. We interviewed appropriate employees to understand the electronic payment process, observed employees' work functions, determined if controls were in place to prevent data from unauthorized modification, and tested electronic payment transactions on a sample basis. Information was obtained from various systems and databases including the IAS, ALIS, Financial and Accounting Management Information System (FAMIS), VPS and DTA Access Database for sampling and verification to source documentation during the audit.

Our audit did not examine the general and application controls over IAS, ALIS, FAMIS and VPS applications. Our transaction testing did rely on those controls; therefore, this was a scope limitation. The potential impact of this circumstance on our findings was that some portion of transaction data may be erroneous.

The Fairfax County Internal Audit Office is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the county executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the county executive and the Board of Supervisors, and reports are available to the public.

Findings, Recommendations, and Management Response

1. Data Transmission

The electronic fund transfer (EFT) program is a payment plan that allows taxpayers to prepay personal property and real estate taxes, or pay delinquent personal property and real estate taxes through automatic installments debited electronically from their bank accounts.

Bank of America utilizes Metavante, a third party processor, to collect all payments under the EFT program. DTA staff was entering the taxpayer's bank information including bank name, routing number and account number, into the Metavante system via modem connection. DTA used an analog modem which was a device that allowed a computer or terminal to transmit data over a standard dial-up telephone line. Data containing taxpayer's social security number and sensitive bank information, i.e. bank account number, was not encrypted during the transmission. Potentially this data can be intercepted when transmitted in this manner.

Fairfax County Information Technology Security Policy 70-05.01, 2.10.3 Transferring and Downloading Data states: "The owner shall ensure that the authorized user has implemented appropriate security measures before any Confidential or Sensitive data is transferred to the destination system. Security measures on the destination system shall be commensurate with physical and logical security measures on the originating system."

Taxpayer's bank information is sent to Metavante via analog modem without encryption. This transmission mechanism exposes Fairfax County and its customers to significant risk and liability over unauthorized interception or modification of data.

Recommendation: We recommend that DTA use Secure File Transfer Protocol (FTP) and encrypt the transmission of taxpayer social security numbers and sensitive bank information.

Management Response: DIT recommends use of Secure File Transfer Protocol (FTP) for transmission. DTA will create an Infra ticket requesting DIT implement the secure FTP process. The anticipated completion date is January 31, 2009.

2. User Access Control

The Velocity Payment System (VPS) is a web-based application that allows the Department of Tax Administration (DTA) to monitor, track and reconcile all the personal property tax payments and real estate tax payments that are paid by credit card and e-check through the DTA Web site. The Integrated Assessment System (IAS) stores county citizen's real estate tax assessment and tax payment information. VPS had about forty users and IAS had over a hundred users. All requests for adding, changing and removing VPS and IAS users were made through e-mails. The VPS system administrator removed three users during this audit. DTA could not provide

access authorization documentation evidencing that user access rights were reviewed and approved by the supervisor. DTA did not use a formal access request form to document user access authorization.

Fairfax County Information Technology Security Policy 70-05.01, states: “All accounts created should have an associated request and approval that is appropriate for the Fairfax County system or service. System administrators or other designated staff:

- Are responsible for removing the accounts of individuals who change roles within Fairfax County or are separated from their relationship with Fairfax County.
- Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
- Shall have a documented process for periodically reviewing existing accounts for validity.”

The lack of a standardized access request form creates risks of granting users excessive access rights to perform their duties, adding new users or changing users’ access rights without manager’s approval, and keeping transferred or terminated users active in the system.

Recommendation: We recommend that DTA establish standard access request forms for both VPS and IAS to document authorization and modification of access privileges approved by the manager, and maintain the completed forms on file.

During this audit, DTA had developed standard access request forms for both VPS and IAS; therefore no management response is required for this finding.

3. Segregation of Duties

The Velocity Payment System (VPS) is a Web-based application that allows DTA to accept credit card and check payments over the Internet. We obtained the list of system administrators for the VPS and noted that each system administrator not only had the system administrator privileges, i.e. create/delete user, change user password/permission and etc., but they also had user update rights to update production data, i.e. void sales, return sales and etc. In this case, an audit trail is created by the system and the audit trail can not be modified by the system administrators or users.

Industry best practices recommend that work responsibilities be segregated so that one individual does not control all critical stages of a process. In addition, Fairfax County Information Technology Security Policy 70-05.01, states: “Access control shall be implemented along with procedures that stipulate and safeguard access to county information only to those with privileges necessary to perform their job function. The concept of “least privilege” should be followed.”

DTA has not identified incompatible duties and assigned these duties to different individuals. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions may be processed.

Recommendation: We recommend that DTA implement segregation of duties control between system administrator and end-user duties. System administrators should not perform end-user tasks to update production data.

Management Response: DTA has implemented this recommendation. The IT project manager and business analyst IV staff is now responsible for system administration tasks. Security roles for end users no longer include system administration privileges.

4. Application Password Requirements

The Integrated Assessment System is a commercial off-the-shelf application that DTA utilizes to store county citizen's real estate tax assessment and tax payment information. Separate Oracle database logins and application logins were required to access IAS. Both the IAS Oracle database and IAS application did not enforce the creation of strong passwords, i.e. password must adhere to a minimum length and must be changed routinely.

DTA had planned to upgrade IAS to the new version, which was called iasWorld. The iasWorld will allow users to access both the IAS application and Oracle database through a single login. The iasWorld accommodated the county's strong password policy. However, the iasWorld strong password requirement was optional, which meant that the system administrator must manually implement the strong password requirements. It is our understanding that DTA will implement iasWorld within eight months.

Fairfax County Information Technology Security Policy 70-05.01, states: "All passwords, including initial passwords, shall be constructed and implemented according to the following complexity rules:

- It shall be routinely changed (at minimum, not longer than every 90 days).
- It shall adhere to a minimum length as established by DIT.
- It shall be a strong password as defined by DIT.
- It shall not be anything that can be easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
- It shall not be dictionary words or acronyms.
- Password history will be retained by systems to prevent the reuse of a password."

The IAS is a commercial off-the-shelf product developed by Tyler Technologies. The old version of the application does not have the built-in functions to enforce strong passwords and periodic password changes. Password identification and authentication is critical to every computer system. There is a potential risk for an unauthorized user to access the system by breaking unsophisticated passwords, undermining the available audit trail. Therefore, weak passwords cannot adequately

protect property tax assessment and payment data from unauthorized modification, disclosure, loss, or impairment.

Recommendation: We recommend that DTA coordinate with the system vendor to set up password requirements in the iasWorld that require a minimum of at least six alpha/numeric characters, enforce password change at least every 90 days, disallow the use of the five previous passwords, and establish a lockout mechanism after three consecutive logon failures to preclude unauthorized access to the system.

In the interim, DTA should request the IAS system users to change their passwords to no less than six alpha/numeric characters in compliance with the strong password requirements outlined in the county's Information Technology Security Policy 70-05.01.

Management Response: This interim recommendation has been implemented. IAS users will be periodically reminded via e-mail to change passwords and to use strong passwording protection. The iasWorld Web-based application accommodates the provisions in IT Policy 70-05-01. The iasWorld application is scheduled to be implemented this fiscal year. The anticipated completion date is June 30, 2009.