



# Fairfax County Internal Audit Office

**Fairfax County Park Authority  
Electronic Payments Audit  
Final Report**

**December 2005**

*"promoting efficient & effective local government"*

## Executive Summary

We 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. However, compliance with the County's Information Technology Security Policy 70-05.01 related to account management, password and privacy, needs to be strengthened.

The primary issues noted were:

- Users' passwords for the ParkNet application are assigned by the system administrator. The system neither requires the users to change their passwords after first time logon, nor requires the users to change their password periodically.
- The ParkNet applications cannot time-out or sign-off a user when no activity has occurred for a certain period.
- Audit log reports generated by the ParkNet application disclose customer's complete credit card number.
- No formal access request form for adding, changing and removing users in the Govolution V-POS and V-Clerk web applications.
- No adequate controls or procedures are in place to ensure that assigned personnel review the audit log reports and file them properly.

## 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. The audit covered the period of May 2004 through September 2004, and our audit objectives were to determine that all electronic payment processes have effective internal controls:

- Reviewed the contract, service level agreement between the vendor and Fairfax County departments (Department of Information Technology and Fairfax County Park Authority), and vendor SAS 70 report or other independent security control review reports to determine whether the vendor had controls in place to ensure electronic transaction processes were current, accurate, complete and indisputable.
- Determined whether the data transmission between vendor and the Park Authority was secure and reconciliations were performed to verify data completeness.
- Determined whether the electronic payments were processed timely, accurately and completely by the County financial systems, and reflected accurately on the County Internet Website.

- Determined whether protections were in place to prevent unauthorized modification, and to prevent personal information about customers from being disclosed without their consent.

## Methodology

Our audit approach included a review and analysis of internal controls over the electronic payment process, as well as the contract and service level agreement between vendor and Fairfax County Park Authority. 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 ParkNet application, Financial and Accounting Management Information System (FAMIS), V-Clerk application, VPOS application, Secured Communication Tool, and Credit Card Tracking Access Database for sampling and verification to source documentation during the audit. However, we limited our review of the system controls to those controls necessary to achieve these audit objectives.

The Fairfax County Internal Audit Office is free from organizational impairments to independence in our reporting as defined by generally accepted 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. Park Authority ParkNet Application Password

Users' passwords for the ParkNet application were being assigned by the system administrator. The system neither required the user to change their password after first time logon, nor required the user to change their password periodically.

Fairfax County Information Technology Security Policy 70-05.01 states that all passwords, including initial passwords, must be constructed and implemented according to the following Fairfax County Information Resource rules:

- it must be routinely changed
- it must adhere to a minimum length
- it must be a combination of alpha and numeric characters
- it must 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 must not be dictionary words or acronyms
- password history must be kept to prevent the reuse of a password

The ParkNet application is a commercial off-the-shelf product developed by BetaData System, Inc. The application was being modified to enforce strong passwords and periodic password changes, but this had not been implemented yet. The ParkNet application contained customers' personal information such as name, address, and home phone number. This information was available to virtually all ParkNet users. Credit card information was stored but viewable only by system administrators.

Password identification and authentication is critical to every computer system. Weak passwords cannot adequately protect ParkNet data from unauthorized modification, disclosure, loss, or impairment.

**Recommendation:** We recommend that the Park Authority coordinate with the vendor to develop password features in ParkNet application 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 meantime, the Park Authority should require ParkNet application users to change their passwords to no less than six alpha/numeric characters in compliance with the strong password requirements based on the County's Information Technology Security Policy 70-05.01.

**Management Response:** Password changes will be implemented in accordance with the recommendation for a minimum of at least six alpha/numeric characters, an enforced password change at least every 90 days (disallowing the five previous passwords), and a lockout after 3 consecutive logon failures. These ParkNet updates will be completed by February 15, 2006.

## 2. Park Authority ParkNet Application Authentication Period

The ParkNet application did not have an "authentication period" to protect the application from security breaches. In other words, ParkNet applications could not time-out or sign-off a user when no activity had occurred for a certain period. An authentication period is the maximum acceptable period between an initial authentication process (sign-on) and subsequent re-authentication process during a single terminal session or during the period data is being accessed.

Based on the National Institute of Standards and Technology Federal Information Processing Standard (FIPS), Publication (PUB) 112 *Password Usage*, the ParkNet application falls under the "Password System for Medium Protection Requirements" category. FIPS PUB 112 recommends that applications which process data leading to, or directly related to monetary payments or process data that fall under the Privacy Act of 1974 should implement the "Password System for Medium Protection." The authentication period requirement is, "Login and after ten (10) minutes of terminal inactivity."

The ParkNet application contains customers' confidential and personal information such as name, home phone number, and credit card information. This application did not have a "session time-out" function to time-out or sign-off a user when no activity had occurred for a certain period. If a user left his/her computer unattended without exiting the ParkNet application, someone else could access ParkNet without password authentication.

**Recommendation:** We recommend that the Park Authority employ the session time-out features available in the operating systems of the ParkNet application users' workstations to secure the ParkNet application from access by unauthorized users. The time-out feature should activate after a short time, e.g., ten to fifteen minutes.

**Management Response:** As recommended, the time-out features of the Windows operating system is being activated as units are replaced. All units running ParkNet will have the Windows operating system by December 2006.

### 3. **Disclose Customer's Complete Credit Card Number**

Customers can register for classes and make payments through the ParkNet Interactive Voice Response (IVR) system or Parktakes Online. The ParkNet application can generate different credit card audit log reports. The IVR Audit Log Report and the Web Credit Card Audit Log Report show detailed credit card information, including complete credit card numbers. The Park Authority utilizes these two reports to perform error transaction investigation and resolve customer disputes.

Only the system administrator and the two backups had access to the online audit log reports. The reports were being printed and filed with the problem documentation under lock and key, separate from the Daily Cash Report files. These were accessible to those involved with problem resolution/analysis during normal business hours. From a security view point, full credit card numbers should not be stored in the system and only prefix and suffix should be retained.

The IVR Audit Log Reports were designed by the vendor, BetaData System, Inc. An unauthorized person could gain access to the reports containing private and sensitive information such as customer credit card numbers. This increases the risk of credit card abuse.

**Recommendation:** We recommend that the Park Authority coordinate with the vendor to modify the design of the IVR Audit Log Report and Web Credit Card Audit Log Report to limit the disclosure of full credit card numbers to only those transactions which did not result in an authorized payment. This will enable the Park Authority to continue to investigate errors and resolve customer account issues while eliminating disclosure of full credit card numbers on completed, correct transactions.

**Management Response:** The ParkNet vendor is redesigning the IVR Audit Log and Web Credit Card Audit Log reports so that for all transactions, only the credit card number prefix and suffix will appear on the reports. These will be completed by January 16, 2006.

#### 4. Access Control

The V-POS and V-Clerk applications are web-based applications that enable the Park Authority to monitor, track and reconcile all the credit card payments processed by Govolution. All requests for adding, changing and removing V-POS and V-Clerk users were being made through emails or phone conversations. There was no formal access request form. In addition, the system administrator did not keep all the email communications for the requests of authorizing access to V-POS and V-Clerk applications.

Fairfax County Information Technology Security Policy 70-05.01 states: "All accounts created must have an associated request and approval that is appropriate for the Fairfax County system or service."

There are only four users from the Park Authority using V-POS and V-Clerk. However, the lack of a standardized access request form creates risks of mishandlings, alterations, and misunderstandings.

**Recommendation:** We recommend that the Park Authority establish a standard access request form to document authorization and modification of access privileges approved by the manager and maintain the completed forms on file.

**Management Response:** As recommended, a standard access request form to document authorization and modification of access privileges has been developed and is in use.

#### 5. ParkNet Application Audit Log Report

All incomplete credit card payment transactions were being automatically caught by the ParkNet application and reported in the IVR Error Log Report if the payment was made through the IVR system and Web Unfinished Cart Report if the payment was made through the Internet.

Park Authority personnel stated that the audit log reports should be reviewed by the assigned staff and the error transactions should be investigated and resolved. However, the Park Authority was unable to provide the reviewed audit logs during our examination.

Output reports should be reviewed and control information should be reconciled to determine whether errors occurred during processing. The user department has ultimate responsibility for maintaining data quality, and shall review output reports for data accuracy, validity, and completeness.

The Park Authority did not have adequate controls and procedures in place to ensure that assigned personnel were reviewing the audit log reports and filing them properly. Without prompt review of the IVR Error Log Report and Web Unfinished Cart Report, incomplete or erroneous transactions may not be caught and corrected.

The corresponding IVR Error Log Report and Web Unfinished Cart Report were not kept in the ParkNet application after the incomplete or erroneous transactions were corrected. The reports were not archived by the application. Without properly saving the output reports, it was difficult to determine whether all incomplete or erroneous transactions were investigated and corrected.

**Recommendation:** We recommend that the Park Authority develop controls and procedures to ensure that the assigned personnel review the audit log reports timely, resolve incomplete or erroneous transactions, and file them promptly.

**Management Response:** As recommended, a procedure has been developed and implemented to ensure that assigned personnel review the audit log reports on a timely basis, and resolve incomplete or erroneous transactions and file them promptly.